Deutscher Bundestag **Drucksache 14/5555**
14. Wahlperiode 13. 03. 2001

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz

Tätigkeitsbericht 1999 und 2000 des Bundesbeauftragten für den Datenschutz
– 18. Tätigkeitsbericht –

Inhaltsverzeichnis

Zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz vom 13. März 2001 gemäß § 26 Abs. 1 des Bundesdatenschutzgesetzes.

Seite

Abbildungsverzeichnis

1 Einführung – Überblick und Ausblick –

Mit dem 18. Tätigkeitsbericht, den ich dem Deutschen Bundestag vorlege, gebe ich einen Überblick über meine Arbeit in den Jahren 1999 und 2000. Dieser Bericht, der vierte in meiner Amtszeit als Bundesbeauftragter für den Datenschutz, gibt zugleich einen Ausblick auf anstehende wichtige Fragen und Probleme beim Umgang mit dem Persönlichkeitsrecht, die in der nahen Zukunft dringenden, zum Teil auch politischen Handlungsbedarf erfordern.

Den Mitgliedern des Deutschen Bundestages danke ich vor allem für die vielfache Unterstützung und Aufgeschlossenheit. Den Mitarbeiterinnen und Mitarbeitern meiner Dienststelle danke ich für ihr besonderes Engagement; für ihren hohen Einsatz und Sachverstand ist auch dieser 18. Tätigkeitsbericht ein nachhaltiger Beleg.

Wie der Tätigkeitsbericht an vielen Stellen aufzeigt, heißt Datenschutzaufsicht im Zeitalter des Internet nicht mehr nur, die klassische Kontrollaufgabe wahrzunehmen und Datenschutzverstöße aufzudecken und zu beseitigen. Viel stärker noch als früher sind heute die partnerschaftliche Beratung und die Mitgestaltung von datenschutzfreundlichen Verfahren gefragt. Erfreulicherweise wird diese Dienstleistung meines Hauses von Behörden und Unternehmen, für die ich zuständig bin, aber auch von Bürgerinnen und Bürgern intensiv in Anspruch genommen.

Auch in Zukunft wird ein Schwerpunkt meiner Arbeit in dieser Art von Vorsorge liegen. Deshalb enthält dieser Bericht insbesondere für die Nutzung von Telediensten praktische Ratschläge, wie man selber etwas für den eigenen Datenschutz tun kann (s. Nr. 8.5, Nr. 34 dort Nr. 8).

1.1 Datenschutz zu Beginn des 21. Jahrhunderts: Eine Bestandsaufnahme

Nach rund einem Vierteljahrhundert seines Bestehens steht der Datenschutz in Deutschland vor neuen Herausforderungen. Wurde er einstmals eher als Stiefkind betrachtet, hat er sich heute zu einem allseits akzeptierten hohen Rechtsgut gewandelt. Der Weg dahin war allerdings von Vorurteilen und Skepsis begleitet. Datenschutz begann als Abwehrrecht des selbstbestimmten Bürgers gegenüber einem mächtigen, informationshungrigen Staat. Inzwischen schützt er die Bürger auch mehr und mehr vor einer ebenso informationshungrigen Wirtschaft.

Immens gestiegene Informationssammlungen und -verarbeitungen in privater Hand in Gestalt der neuen Technologien kennzeichnen die datenschutzrechtlichen Probleme der heutigen Zeit. Die weltweit vernetzten Systeme auf dem Informations- und Telekommunikationssektor schaffen völlig neue Möglichkeiten im Umgang mit personenbezogenen Daten. Nicht nur die Menge der Daten, sondern auch deren Kombinierbarkeit und Nutzbarkeit sind die neuen Gefahrenpotenziale für den Datenschutz der Bürger. Ohne Frage haben die Technologien der Informations- und Kommunikationsgesellschaft unseren privaten und beruflichen Alltag erleichtert und bereichert, zugleich liefern sie aber eine Vielzahl von Daten über unser Verhalten.

Während staatliche Datenerhebung und -verarbeitung einem relativ strengen Datenschutzregime unterworfen sind, entwickeln sich die privatwirtschaftlich betriebenen personenbezogenen Datenbanken beinahe unreglementiert. Bei Informations-, Finanz- oder sonstigen Dienstleistungsunternehmen oder bei großen Versandhändlern werden Daten über Konsumgewohnheiten, über Bonität oder sonstige, teilweise sehr private Sachverhalte systematisch gesammelt und unter verschiedenen Gesichtspunkten ausgewertet und genutzt. Nicht anonyme Kunden- und Haushaltsbefragungen gehören heute zum Alltag. Der Gewinn des bei Beteiligung in Aussicht gestellten Preises ist hierbei ziemlich unwahrscheinlich, das Abbild des Konsumverhaltens jedoch sicher. Seine Privatheit kann man gewissermaßen zum Preise eines Rabatts auch verkaufen, wie im Falle der „PAYBACK-Karte“, mit deren Hilfe alle Käufe des Karteninhabers ausgewertet werden können (s. Nr. 31.7.4).

Mit der komplexer gewordenen Datenverarbeitung in der Wirtschaft ist das Datenschutzrecht der Betroffenen nicht ausreichend gewachsen. Um mit diesen Entwicklungen Schritt zu halten, geht es für den Datenschutz darum, die immer undurchsichtiger werdende Informationsverarbeitung für die Betroffenen, die Bürger und Kunden, transparenter zu machen und ihnen so die Wahrnehmung ihrer Rechte zu erleichtern oder gar erst zu ermöglichen. Dazu muss auch die Wirtschaft ihren Beitrag leisten. Viele Unternehmen in der IT- und Telekommunikationsbranche haben inzwischen bereits unter Beweis gestellt, dass ein Produkt bei gleicher Qualität und gleichem Preis allein Wettbewerbsvorteile dadurch hat, dass es datenschutzgerechter ist als andere, dass es anderen vorgezogen wird, weil es mit möglichst wenig personenbezogenen Daten seiner Benutzer auskommt und nicht jegliche Datenspuren aufzeichnet.

Auch dem Medieninteresse ist es zu verdanken, dass die Sensibilität der Bürger für ihr Persönlichkeitsrecht gewachsen ist. Mehr und mehr ist festzustellen, dass der Bürger in seiner Eigenschaft als Nutzer z. B. des Internet, eines Handys oder einer Kredit- oder anderen Wertkarte die Frage nach seinem persönlichen Datenschutz stellt und gesteigertes Interesse daran hat, was aus seinen Daten wird, wo sie möglicherweise zwischengespeichert werden, wer auf sie zugreifen kann und welche Missbrauchsmöglichkeiten bestehen.

Die Informationsgesellschaft hat den Datenschutz vor etliche neue Herausforderungen gestellt. Es ist jedoch nicht ausschließlich eine Frage von neuen Gesetzen und Regelungen; vielmehr muss das Verständnis für die Notwendigkeit von Datensicherheit und Datenschutz in den Köpfen aller, die damit zu tun haben, wachsen. Ein entsprechendes Verantwortungsbewusstsein muss geweckt und gestärkt werden – eine wichtige Aufgabe von allen zum Schutze jedes Einzelnen.

1.2 Bundesdatenschutzgesetz: Für die neuen Aufgaben gerüstet?

Mehr als fünf Jahre nach Verabschiedung der EG-Datenschutzrichtlinie steht deren Umsetzung in das deutsche

Recht endlich bald bevor. Angesichts der versäumten termingerechten Umsetzung der Richtlinie hat sich die Bundesregierung dazu entschlossen, in zwei Stufen vorzugehen. In einer ersten Stufe sollen so rasch wie möglich alle unumgänglichen gesetzgeberischen Anpassungen an die Richtlinie und verschiedene darüber hinausgehende Regelungen erfolgen. Hierzu zählen auch die von meinen Länderkollegen und mir geforderten Modernisierungsbestrebungen, wie die Regelungen zur Videoüberwachung und Chipkarte, die Einführung eines Datenschutzaudits, die Verpflichtung auf Datensparsamkeit bis hin zur Datenvermeidung auch durch Anonymisierung und Pseudonymisierung. Der von der Bundesregierung beschlossene Gesetzentwurf stellt einen erfreulichen Fortschritt gegenüber den früheren Entwürfen dar. Insofern habe ich es nicht beklagt, dass der in der 13. Legislaturperiode erarbeitete Referentenentwurf, der über eine enge Umsetzung der EG-Datenschutzrichtlinie nicht hinausgegangen wäre, nicht in das Gesetzgebungsverfahren eingebracht wurde.

Die Fortentwicklung des Datenschutzes kann und soll mit dem Abschluss dieses Gesetzesvorhabens zum allgemeinen Datenschutz aber keinesfalls zum Stillstand kommen. Wegen des hohen Novellierungsbedarfs sollen über diesen ersten Teil der Reform hinaus in einer zweiten Stufe die Arbeiten an einer umfassenden Neukonzeption des Datenschutzrechts noch in der laufenden Legislaturperiode aufgegriffen und weitergeführt werden. Das Ziel, das Gesetz in der zweiten Stufe der Novellierung zu modernisieren, zu vereinfachen und seine Lesbarkeit zu erhöhen, begrüße ich sehr. Auch teile ich die Auffassung, dass noch im Laufe dieser Legislaturperiode das gesamte bereichsspezifische Datenschutzrecht daraufhin zu überprüfen sein wird, ob über die bereits vorgenommenen Änderungen hinaus weitere Anpassungen an die Richtlinie geboten sind, und zwar auch, soweit keine europarechtliche Anpassungspflicht besteht – also außerhalb der Gemeinschaftskompetenzen. Denn nur so kann vermieden werden, dass es auf Dauer zweierlei Datenschutzrecht mit unterschiedlich hohem Schutzniveau gibt (s. Nr. 2.1).

Wer heute das Datenschutzrecht modernisieren möchte, darf nicht die Augen davor verschließen, dass ein wirksamer Datenschutz nicht an den eigenen Grenzen Halt machen kann. Der elektronische Geschäftsverkehr und das Internet sind Stichworte hierfür. Ich halte es deshalb für einen Meilenstein in der Geschichte des Datenschutzes und für einen wichtigen Erfolg, dass die Charta der Grundrechte der Europäischen Union auch eine Grundlage für den Schutz personenbezogener Daten geschaffen hat. Der Rang des Datenschutzes als einer der Grundfreiheiten des Menschen wird damit auch international aufgewertet (s. Nr. 2.4).

Auch im internationalen Datenverkehr der Informationsgesellschaft wird es zunehmend auf einen effektiven Datenschutz ankommen. Dieser Prozess wird weiteren Aufschwung dadurch erhalten, dass die Europäische Kommission gegenüber immer weiteren Drittstaaten feststellt, dass diese ein angemessenes Datenschutzniveau im Sinne der Richtlinie gewährleisten. Auch gegenüber den USA konnten im vergangenen Jahr Fortschritte auf der Grundlage der EG-Datenschutzrichtlinie nach langwierigen Verhandlungen über die Zulässigkeit der Übermittlung personenbezogener Daten erzielt werden. Im Ergebnis konnte ein akzeptables Datenschutzniveau ausgehandelt werden. Es kommt jetzt darauf an, die in den „Safe-Harbor-Principles“ aufgeführten Grundsätze mit Leben zu füllen. Die EG-Datenschutzrichtlinie mit ihren tragenden Grundsätzen für den Schutz natürlicher Personen bei der Verarbeitung ihrer Daten kann damit auch in Drittstaaten Vorbildwirkung für den Datenschutz erlangen (s. Nr. 2.2.2).

Auch die Selbstregulierung wird künftig, insbesondere im Unternehmensbereich, eine wichtige Rolle spielen müssen. Vor dem Hintergrund gesetzlicher Vorgaben wird hierdurch die Möglichkeit eröffnet, branchenspezifische Regelungen zu treffen und ggf. weltweit für das jeweilige Unternehmen verbindlich zu machen.

1.3 Telefonüberwachung – Spirale ohne Ende? –

In den letzten Jahren ist die Zahl der Telefonüberwachungen in Deutschland alarmierend angestiegen. In den letzten fünf Jahren wurden folgende Überwachungsanordnungen erlassen: 4 674 (1995), 6 428 (1996), 7 776 (1997), 9 802 (1998), 12 651 (1999). Gegenüber 1995 sind damit die Anordnungen um über 170 % angestiegen, für 1999 ist eine Steigerung von fast 30 % gegenüber dem Vorjahr festzustellen.

Die Gründe hierfür liegen sicherlich auch darin, dass die Möglichkeiten, nach § 100 a StPO Überwachungsmaßnahmen anzuordnen, im Laufe der letzten Jahre immer weiter ausgedehnt worden sind, und dass die Anzahl der Handys stark gestiegen ist. Eingriffe in das Fernmeldegeheimnis im Rahmen der rechtsstaatlichen Ordnung sind grundsätzlich zu akzeptieren; es stellt sich jedoch die Frage, in welchem Umfang dies erfolgen soll und wie effektiv die damit betrauten Stellen mit diesem Instrument zur Gewährleistung des staatlichen Strafverfolgungsanspruchs umgehen. Empirische Untersuchungen hierzu oder gar Evaluierungen liegen bisher nicht vor.

Den Anstieg der Telefonüberwachung beobachte ich mit großer Sorge. Seit Jahren appelliere ich an die Strafverfolgungsbehörden, dieses Mittel sparsam einzusetzen.

Um sicherzustellen, dass Telefonüberwachungen nur durchgeführt werden, wenn sie dringend notwendig sind, und nicht als „Standardmaßnahme“ eingesetzt werden, ist der Gesetzgeber gefragt. Für die Fälle der akustischen Wohnraumüberwachung hat der Gesetzgeber erfreulicherweise Berichtspflichten der Staatsanwaltschaft gegenüber der obersten Justizbehörde und der Bundesregierung gegenüber dem Deutschen Bundestag auferlegt. Entsprechende Berichtspflichten halte ich auch für den Bereich der Telefonüberwachung für dringend erforderlich. Der Gesetzgeber sollte darüber informiert sein, wie die Telefonüberwachung in der Praxis wirkt, welche Erfolge sie gebracht hat und was mit den nicht mehr für das

laufende Ermittlungsverfahren benötigten Daten geschieht. Tief in das Persönlichkeitsrecht eindringende Eingriffsbefugnisse müssen hinsichtlich ihrer Wirkungen bewertet werden können, um sowohl ein Unter- als auch ein Übermaß zu vermeiden. Der Bürger muss nachvollziehen können, weshalb solche Eingriffe in seine Freiheit in einem Rechtsstaat gerechtfertigt sind. Vor diesem Hintergrund hat das Bundesministerium der Justiz ein Forschungsvorhaben zur Evaluierung der Telefonüberwachungsmaßnahmen in Auftrag gegeben, das ich als einen ersten Schritt für die Bewertung der Notwendigkeit und der Effektivität der Ermittlungsmaßnahmen begrüße.

Leider ist ein anderes wichtiges Vorhaben beim Bundeskriminalamt, das durch das Sammeln und Dokumentieren von Fallschilderungen Defizite und andere Schwachstellen in bestehenden gesetzlichen Regelungen erkennen und auf diese Weise rechtspolitischen Handlungsbedarf aufzeigen sollte, ins Stocken gekommen. Das Vorhaben einer Rechtstatsachensammelstelle steht quasi vor seinem Aus, wird es nicht auf politischer Ebene wiederbelebt und mit hohem Nachdruck neu in Gang gesetzt (s. Nrn. 6.4.2 und 11.9).

1.4 Verwendung der Stasi-Abhörprotokolle – Wie weit reicht der Opferschutz? –

Der Berichtszeitraum war besonders von dem rechtspolitischen Streit darüber geprägt, ob und in welchem Umfang Stasi-Abhörprotokolle in einem parlamentarischen Untersuchungsausschuss und von Medien verwendet werden können. Hierbei wurde leider auch behauptet, dass ost- und westdeutsche Personen der Zeitgeschichte unterschiedlich behandelt würden.

Ich habe in dieser Diskussion immer den Opferschutzgedanken des Stasi-Unterlagen-Gesetzes in den Vordergrund gestellt. Eine Unterscheidung der Stasiopfer nach ihrer Herkunft – Ost oder West – habe ich zu jeder Zeit abgelehnt. Die Stasi-Abhörprotokolle sind illegal entstandene Unterlagen, die nach den Grundsätzen unseres Rechtsstaates nicht hätten entstehen dürfen. Sie dürfen deshalb jetzt nicht zum Nachteil der Opfer der Praktiken des MfS genutzt werden.

Hinsichtlich der Verwendung der Stasi-Abhörprotokolle in einem parlamentarischen Untersuchungsausschuss war die Problematik nicht neu. Bereits 1995 hatte der sog. Schubladenausschuss des Kieler Landtages ebenfalls auf Stasi-Abhörprotokolle der BStU zugreifen wollen. Das Landgericht Kiel hatte seinerzeit festgestellt, dass Stasi-Abhörprotokolle nicht an den parlamentarischen Untersuchungsausschuss herausgegeben werden dürfen, weil die Rechte der Betroffenen aus Art. 10 Abs. 1 GG bezüglich der durch das Abhören des Fernmeldeverkehrs gewonnenen Stasi-Unterlagen Vorrang gegenüber dem Aufklärungsinteresse eines parlamentarischen Untersuchungsausschusses hätten. Das Urteil spiegelte somit meine Rechtsposition wider, wie auch in meinem 16. und 17. TB nachzulesen ist. Da sich die Bundesregierung in ihrer Stellungnahme zu meinem 16. TB meiner Auffassung angeschlossen hatte, und die BStU das Thema nicht weiter problematisiert hatte, kam die Heftigkeit der neuerlichen öffentlichen Diskussion einigermaßen überraschend. In der Zwischenzeit sind verschiedene juristische Gutachten erstellt worden, die allerdings wegen ihrer unterschiedlichen Ergebnisse zu keiner endgültigen Klärung der Rechtsfragen beigetragen haben.

Bis April 2000 bin ich davon ausgegangen, dass die BStU keine Stasi-Abhörprotokolle von Betroffenen (Opfern) ohne deren Einwilligung an Medien herausgibt. Über die Medien erfuhr ich erstmals im Fall Leisler Kiep, dass Stasi-Abhörprotokolle an die Medien herausgegeben wurden, obwohl der Betroffene nicht Täter oder Begünstigter, sondern Opfer des MfS war, weil er zielgerichtet ausgespäht wurde. Im Hinblick auf den für mich eindeutigen Gesetzestext habe ich in diesem Falle die Herausgabe der Stasi-Abhörprotokolle umgehend beanstandet.

Meine ausführliche Rechtsauffassung hierzu habe ich mehrfach in Parlament und Öffentlichkeit vorgetragen (s. Nr. 5.8.1). Zusammengefasst ist bei Herausgabe personenbezogener Informationen an Medien wie auch zur Forschung zu prüfen, ob die Person der Zeitgeschichte Betroffener oder Dritter ist. In diesem Fall ist eine Herausgabe unzulässig. Betroffene sind nach der maßgeblichen Legaldefinition des Stasi-Unterlagen-Gesetzes Personen, zu denen der Staatssicherheitsdienst aufgrund zielgerichteter Informationserhebung oder Ausspähung einschließlich heimlicher Informationserhebung Informationen gesammelt hat. Dies ist bei Opfern illegaler Abhörmaßnahmen eindeutig der Fall. Weiterhin ist für jede Information gesondert festzustellen, ob Personen Mitarbeiter des Staatssicherheitsdienstes, Begünstigte, Betroffene oder Dritte sind, wobei maßgebend ist, mit welcher Zielrichtung die Informationen in die Unterlagen aufgenommen worden sind. Nach diesen gesetzlichen Definitionen kann es keinen Zweifel geben, dass – für jedes Protokoll gesondert festzustellen – die Personen, die das Ziel von illegalen Abhörmaßnahmen waren, Betroffene im Sinne des StUG sind, wenn klar ist, dass sie weder Mitarbeiter noch Begünstigte der Stasi waren.

Zur Verwendung der Stasi-Abhörprotokolle differieren die zwischen und z. T. innerhalb der Bundestagsfraktionen vertretenen Auffassungen. Da auch innerhalb der Bundesregierung unterschiedliche Auffassungen vertreten werden, kommt die einzig zur Verfügung stehende Möglichkeit einer Rechtsaufsicht der Bundesregierung nicht zum Tragen. Sollte – was nicht zu hoffen ist – eine Einigung nicht möglich sein, wird wieder einmal mehr das Bundesverfassungsgericht oder der Bundesgesetzgeber das Sagen haben müssen.

1.5 Maß der Videobeobachtung nicht überziehen

Videobeobachtung und -überwachung haben in Deutschland erheblich zugenommen und nehmen weiter zu. Diese Entwicklung wird dadurch begünstigt, dass viele Bürger sich an die Kameras gewöhnt haben und nichts mehr dabei denken, wenn sie am Geldautomaten, an Tankstellen, auf Bahnhöfen oder in Kaufhäusern beobachtet bzw. überwacht werden. Hinzu kommt, dass die hierfür erfor-

derliche Technik immer leistungsfähiger, immer kleiner und billiger wird. Seitdem die Digitalisierung auch hier Einzug gehalten hat, scheinen die Möglichkeiten beim Einsatz der Videoüberwachung schier unbegrenzt. So werden bereits neben digitalen Gesichtserkennungssystemen auch Systeme entwickelt, die „normales“ von „verdächtigem“ Verhalten unterscheiden sollen.

Im Berichtszeitraum hat es eine sehr rege öffentliche Diskussion um die Videoüberwachung im öffentlichen Raum gegeben, bei der allerdings die Wogen der Auseinandersetzung zeitweise sehr hoch gingen – von der Videoüberwachung als eine Art Allheilmittel im Kampf gegen die Kriminalität bis hin zu ihrer Verteufelung. Wenn jetzt auch endlich Schluss ist mit dieser Polarisierung, so besteht doch noch kein Anlass für eine Entwarnung.

Tatsache ist, dass die Bürger aufgrund des zunehmenden Einsatzes von Videotechnik immer mehr damit rechnen müssen, dass sie offen oder heimlich von einer Videokamera aufgenommen werden. Da eine Videokamera alle Personen erfasst, die in ihren Bereich gelangen, werden von der Videoüberwachung in unvermeidbarer Weise auch völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen betroffen. Die daraus resultierende Ungewissheit, ob und von wem man beobachtet wird und zu welchen Zwecken dies geschieht, kann einen latenten Anpassungsdruck erzeugen. Damit sage ich nicht, dass Videobeobachtung und -überwachung grundsätzlich von Übel sind. Der Einsatz von Videotechnik an sog. Kriminalitätsschwerpunkten, an denen wiederholt Straftaten begangen wurden und Anhaltspunkte dafür bestehen, dass auch künftig dort Straftaten begangen werden, ist sicherlich gerechtfertigt, soweit mit der Beobachtung neben der Sicherung von Beweisen eine Präventionswirkung erreicht werden kann (s. Nr. 12.3). Die Grenzen von Videobeobachtung und -überwachung müssen aber möglichst genau festgelegt werden. Erfreulicherweise gibt es einen breiten Konsens in Politik und Gesellschaft darüber, dass die Schaffung flächendeckender Beobachtungsmöglichkeiten durch Videokameras zur Verhinderung bloßer Störungen der öffentlichen Ordnung mit dem Grundsatz der Verhältnismäßigkeit nicht zu vereinbaren ist. Da der Ausbau der Videotechnik im öffentlichen wie auch im privaten Bereich offenkundig deutlich fortschreitet, kommt es jetzt auf den genannten breiten Konsens in Politik und Gesellschaft an, die bisherige allgemeine Diskussion im Kleinen und vor Ort, z. B. auf der kommunalen Ebene fortzusetzen und dabei alle die Punkte einzufordern, die unabdingbar für die Gewährleistung des Persönlichkeitsrechts Unbeteiligter sind. Meine Länderkollegen und ich haben hierfür in einer Entschließung konkrete Forderungen gestellt (s. **Anlage 20**). Hierzu gehören insbesondere, ein Höchstmaß an Transparenz zu schaffen und die Verarbeitung personenbezogener Daten auf das Unvermeidliche zu reduzieren.

1.6 Veröffentlichung heimlicher Bildaufnahmen unter Strafe stellen

Im Strafgesetzbuch finden sich zahlreiche Straftatbestände, die die Verletzung des persönlichen Lebens- und Geheimbereichs sanktionieren. So wird in § 201 StGB die heimliche Aufnahme des nicht öffentlich gesprochenen Wortes und dessen Veröffentlichung unter Strafe gestellt. Vorschriften gegen das unbefugte Aufnehmen des Bildes von Menschen und die Veröffentlichung solcher Aufnahmen existieren jedoch nicht. Dabei ermöglichen es vor allem die technischen Entwicklungen in der Videotechnik und im Internet, Bilder von Menschen unbemerkt aufzunehmen und auch weltweit zu verbreiten, ohne dass der Einzelne dies je wahrnimmt, geschweige denn seine Zustimmung geben könnte.

Vor diesem Hintergrund habe ich in letzter Zeit mit großer Besorgnis immer öfter Eingriffe in die Persönlichkeitsrechte von Bürgern festgestellt. So werden im Internet Fotos von Personen veröffentlicht, die weder von der Aufnahme noch von deren Veröffentlichung Kenntnis haben. Dabei bewegen sich diese Personen nur zum Teil in der Öffentlichkeit, zum Teil aber in Bereichen, wo sie sich bewusst der Öffentlichkeit entziehen wollen und deshalb auch gar nicht mit der Aufnahme von Bildern rechnen können oder müssen. Dazu zählen z. B. eine Privatwohnung, Umkleidekabinen in Schwimmbädern oder Geschäften. Es kann nicht angehen, dass so etwas weiterhin straffrei ist. Dies bedarf aus meiner Sicht dringend einer gesetzlichen Regelung. Es ist äußerst unbefriedigend, wenn die Veröffentlichung von heimlichen Tonaufnahmen unter Strafe gestellt ist, während die mindestens einen ebenso tiefen Eingriff in die Persönlichkeitsrechte darstellende Nutzung oder Veröffentlichung von heimlichen Bildaufnahmen nur dann strafbar ist, wenn sie in Verbindung mit anderen Delikten steht. Für diese unterschiedliche Behandlung sehe ich gerade mit Blick auf die modernen technischen Möglichkeiten keinen sachlichen Grund.

Ich appelliere deshalb an den Gesetzgeber, im Strafgesetzbuch eine Regelung für die Fälle zu schaffen, in denen mittels Bildaufnahme bzw. -veröffentlichung unbefugt in den Kernbereich der Privatsphäre und in die Intimsphäre eingegriffen wird (s. Nr. 6.13).

1.7 Keine Entschlüsselung der Persönlichkeit

Bei der Entschlüsselung des menschlichen Genoms waren in den letzten Jahren bahnbrechende Fortschritte zu verzeichnen. Bereits heute sind für bestimmte vererbliche Krankheiten Gentests erhältlich, die eine Aussage darüber treffen, ob eine Erkrankung vorliegt oder in welchem Umfang ein Erkrankungsrisiko besteht. Noch sind solche Gentests lediglich Spezialisten mit besonderer Laborausstattung vorbehalten. Doch ist bereits in den USA der Prototyp eines handtellergroßen Minilabors vorgestellt worden, das innerhalb kürzester Zeit einen Gentest durchführen kann.

Gentechnische Untersuchungen beim Menschen enthalten höchst persönliche Informationen in einem Maße, das die Sensitivität bisheriger personenbezogener Informationen bei weitem übersteigt. Die Erkenntnisse der Genetik werfen schwierige medizinische, ethische und rechtliche Fragen auf.

Anders als beispielsweise das unbefugte Öffnen eines Briefes sind derart gravierende Eingriffe in das Persönlichkeitsrecht derzeit nicht strafbar, lediglich die Datenschutzgesetze ziehen in ihrem Anwendungsbereich gewisse Grenzen für die Erhebung und Verarbeitung solcher Daten. Diese Vorschriften sind aber in vielen realistischen Szenarien nicht anwendbar.

Ich halte deshalb ein gegen jedermann gerichtetes, ausdrückliches und strafbewehrtes Verbot für vordringlich, ohne besondere Befugnis die Analyse des Genoms eines Anderen durchzuführen oder durchführen zu lassen, oder Ergebnisse der Analyse des Genoms eines Anderen zu verarbeiten und zu nutzen.

Diese Schutzmaßnahmen für eines der wichtigsten Geheimnisse eines Menschen sollten getroffen werden, auch wenn das Risiko besteht, dass sie mangels international abgestimmter Regelungen nicht in allen Bereichen vollständig und zuverlässig greifen. Es ist besser, bald die internationale Diskussion damit anzustoßen, als auf ein sich irgendwann einmal einstellendes Ergebnis zu warten (s. Nr. 25.2.3).

1.8 Gesetzesinitiative zum Schutz der Arbeitnehmerdaten nicht länger verschleppen

Auch unsere Arbeitswelt wird zunehmend durch den Einsatz immer leistungsfähigerer Informations- und Kommunikationstechniken geprägt. Telearbeit und papierarmes Büro sind Stichworte dieser neueren Strukturen, die auch in der öffentlichen Verwaltung Einzug halten. Der PC gehört inzwischen zum Büroalltag; häufig ermöglicht er den Zugriff auf umfangreiche Datenbanken und erlaubt die Nutzung des Internet einschließlich des Empfangs und des Versands von elektronischer Post, der E-Mail. Immer mehr sollen Dokumente nur noch elektronisch verwaltet und jederzeit sofort eingesehen werden können. Immer häufiger werden Fragen zum Umgang mit Daten von Arbeitnehmern vor allem im Zusammenhang mit E-Mail und Internetnutzung gestellt. Ohne Zweifel führt der technische Komfort zu erleichterten Arbeitsbedingungen für die Mitarbeiter. Zugleich liegt er auch im Interesse der Arbeitgeber, die sich vom Einsatz dieser Techniken Wirtschaftlichkeits-, aber auch Rationalisierungseffekte versprechen. Auf der anderen Seite ist unbestreitbar, dass der zunehmende Einsatz von Informations- und Kommunikationstechniken auch Risiken für die Persönlichkeitsrechte der Mitarbeiter in sich birgt.

Das Bundesarbeitsgericht hat bereits 1984 – also zu einer Zeit, als die Informations- und Kommunikationstechnik noch in den Kinderschuhen steckte – auf die Risiken für das Persönlichkeitsrecht des Arbeitnehmers durch die technisierte Ermittlung von Verhaltens- und Leistungsdaten hingewiesen. Da gesetzliche Regelungen zum Arbeitnehmerdatenschutz nach wie vor weitgehend fehlen, ist die Rechtslage aufgrund einer notwendigerweise lückenhaften, aber auch schwer zu erschließenden Rechtsprechung vielfach nicht eindeutig. Darüber hinaus erscheint es äußerst problematisch, wenn Arbeitnehmer und Arbeitgeber ihre datenschutzrechtlichen Rechte und Pflichten nach geltendem Recht weitgehend nur aus dieser Rechtsprechung ableiten können.

Die Datenschutzbeauftragten des Bundes und der Länder fordern bereits seit 1984 bereichsspezifische gesetzliche Regelungen zum Arbeitnehmerdatenschutz. Der Deutsche Bundestag hat die Bundesregierung mehrfach aufgefordert, einen entsprechenden Gesetzentwurf vorzulegen, was dieser bereits auch mehrfach ausdrücklich zugesagt hat. Allerdings sind diesen Worten bislang keine Taten gefolgt. Auch in dieser Legislaturperiode hat die Bundesregierung neuerlich angekündigt, ein entsprechendes Gesetz vorzulegen, das die Entwicklung der Informations- und Kommunikationsgesellschaft arbeitsrechtlich flankieren soll.

Ich appelliere an die Bundesregierung, durch Vorlage eines Gesetzentwurfs die Gesetzesberatung nun endlich in Gang zu setzen, damit in der zunehmend technisierten Arbeitswelt Rechtsklarheit und Rechtssicherheit für alle Beteiligten geschaffen wird. Es ist nicht länger hinnehmbar, den Auftrag des Deutschen Bundestages nach Vorlage eines Arbeitnehmerdatenschutzgesetzes zu verschleppen (s. Nr. 18.1).

1.9 Internet – (k)ein rechtsfreier Raum

Im Internet steigt die Zahl der Nutzer weiter steil an, durch neue Anbieter von Informationen und neue Angebote wird die virtuelle Welt noch bunter und faszinierender. Ihr dynamisches Wachstum trifft auf eine unregulierte und etwas chaotische, noch längst nicht stabile Situation in der virtuellen Welt. Aber auch im Internet handeln Menschen, die Rechte und Pflichten haben (s. auch Nr. 18.7). Fraglich ist jedoch, was davon wie unter den Bedingungen eines an keine nationalen Grenzen gebundenen Netzes durchsetzbar ist.

In vielen nationalen Gesetzen und internationalen Deklarationen wird beispielsweise das Recht auf unbeobachtete Kommunikation bekräftigt. Die Technik des Internet, in dem Daten als Pakete von Knoten zu Knoten weitergereicht und dazu in jedem Knoten zunächst auch gespeichert werden, macht das Beobachten der Kommunikation allerdings besonders leicht, insbesondere weil sich der Weg der Daten nach der Topologie der beteiligten Datennetze und nach ihrer Belastung richtet, so dass die Partner in der Regel weder wissen noch gar bestimmen können, über welche Länder die Pakete laufen.

Für deutsche Anbieter im Internet schreibt das Teledienstedatenschutzgesetz insbesondere vor, dass Daten über Nutzer nur erhoben, verarbeitet und genutzt werden dürfen, wenn und solange es für das Erbringen oder das Abrechnen der Nutzung erforderlich ist oder soweit der Nutzer ausdrücklich seine Einwilligung erteilt hat. Der Nutzer ist außerdem über die Verarbeitung seiner Daten zu informieren. Ein besonderes Problem ist die Bekämpfung der auch im Internet vorhandenen Kriminalität. Die Strukturen des Internet lassen sich auch für die Verbreitung von extremistischer Hetze, von illegalen Raubkopien urheberrechtlich geschützter Werke oder von Kinderpornografie leicht nutzen. Obwohl das nur einen kleinen Teil

der Nutzung dieses Mediums ausmacht, kann man diesen Missbrauch nicht hinnehmen.

Weil aber in der Regel die Nutzung für den Nutzer entgeltfrei ist, werden Nutzungsdaten zur Abrechnung nicht benötigt. Sie sind deshalb zu löschen und sind dann für die Strafverfolgung nicht mehr verfügbar. Das ist unschädlich, wenn es zur Strafverfolgung genügt, den Anbieter zu kennen, der für die Straftat verantwortlich ist und dessen Angebot zumindest eine gewisse Zeit lang gerade dafür im Netz erreichbar sein muss. Für den Fall, dass man, etwa zu Beweiszwecken, auch Daten der Nutzer eines solchen Angebotes benötigt, ist zu klären, wie man diese Daten zuverlässig und gerichtsverwertbar erlangen kann. Das vorsorgliche Speichern aller personenbezogenen Daten aus allen Nutzungen des Internet wäre jedoch offensichtlich unverhältnismäßig. Es würde einen unzumutbaren Überwachungsdruck für jeden Nutzer erzeugen und damit nicht nur die Informationsfreiheit, sondern auch die Entwicklung dieses Mediums beeinträchtigen.

Das zwangsweise Speichern aller Daten aus der Nutzung des Internet sollten die Demokraten denen überlassen, die Gründe haben, die Informationsfreiheit zu fürchten.

1.10 Datenschutz in der Telekommunikation stärken

Fortentwicklung und Ausbreitung moderner Informationstechnologien erfolgen in schnellen, großen Schritten. Von den Bürgern werden die neuen Möglichkeiten in der Telekommunikation massenhaft als Fortschritt genutzt.

Demgegenüber erhalten die herkömmlichen Befugnisse der Strafverfolgungsbehörden eine neue Dimension. Nach § 12 FAG können Strafverfolgungsbehörden in strafgerichtlichen Verfahren von Telekommunikationsunternehmen Auskunft darüber verlangen, wer wann mit wem wie lange kommuniziert hat (sog. Verbindungsdaten). Mit Blick auf den Umfang der heute anfallenden Daten können mittels der Verbindungsdaten nahezu Verhaltensprofile mit hoher Aussagekraft erstellt werden. Eine Überwachung dieser Vorgänge greift daher tief in das Telekommunikationsgeheimnis der Betroffenen ein. Seit längerem steht eine Erneuerung dieser Vorschrift an. In diesem Zusammenhang appelliere ich an den Gesetzgeber, die Auskunftsanordnung von einem Katalog von Straftaten abhängig zu machen, bei denen die Verbindungsdaten mitgeteilt werden dürfen. Unabdingbar ist auch, eine Schutzklausel für Telefonate von Personen zu schaffen, die zur Wahrung von Berufsgeheimnissen verpflichtet sind, wie Priester, Ärzte, Rechtsanwälte oder Journalisten. Der vom Gesetzgeber durch die bestehenden Zeugnisverweigerungsrechte anerkannte Schutz des Vertrauensverhältnisses zwischen bestimmten Berufsangehörigen und Dritten, die deren Hilfe und Sachkunde in Anspruch nehmen, muss auch im modernen Telekommunikationszeitalter Bestand haben (s. Nr. 6.4.1).

Wegen der rasanten Entwicklung der modernen Kommunikationstechniken hat die Europäische Kommission im Juli 2000 einen Entwurf für eine EG-Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vorgelegt. Diese soll die bestehende Richtlinie vom Dezember 1997 ersetzen. Aus meiner Sicht sollte die neue Richtlinie zum Anlass genommen werden, auch im nationalen Recht den Datenschutz in der Telekommunikation und bei den Telediensten in einem einheitlichen Gesetz zu regeln. Dies würde der zusammenwachsenden Technik in beiden Bereichen entsprechen, den Anbietern von Komplettlösungen Rechtssicherheit und -klarheit verschaffen sowie den Nutzern dieser Dienste ein einheitliches und damit für sie durchschaubares Rechtssystem anbieten (s. Nr. 10.1.1).

Überhaupt scheint sich die Halbwertzeit von Datenschutzvorschriften im Bereich der Informations- und Kommunikationsmedien weiter zu reduzieren. Vor diesem Hintergrund appelliere ich an den Gesetz- und Verordnungsgeber, nicht nur reaktiv auf die Entwicklungen der Telekommunikationstechnik und Gegebenheiten des Telekommunikationsmarktes zu antworten, sondern diese im Vorfeld aufzugreifen und mitzugestalten.

1.11 Appell zu mehr eigenverantwortlichem Datenschutz

Immer wieder wenden sich Bürger mit Beschwerden an mich, Unternehmen seien im Besitz ihrer Adressdaten, die sie niemals dorthin weitergegeben hätten. Insbesondere was die freiwillige Weitergabe ureigener Daten an private Dritte betrifft, muss jeder Einzelne Verantwortung für den Schutz seiner Daten aktiv übernehmen. Hier appelliere ich an die Bürger zu mehr eigenverantwortlichem Datenschutz. Wer die Weitergabe seiner Daten nicht möchte, muss daher darauf achten, dass entsprechende Klauseln in Firmenunterlagen gestrichen werden. Dazu gehört auch, sich mit Kleingedrucktem auseinander zu setzen und bei Unklarheiten das Unternehmen zu fragen. Mehr Eigenvorsorge heißt auch, etwas mehr darauf zu achten, wem man welche Informationen und Auskünfte gibt. Für Informationen über den Datenschutz wie auch für die Durchsetzung ihrer Datenschutzrechte stehen den Bürgern die Datenschutzbeauftragten von Bund und Ländern wie auch die Aufsichtsbehörden der Länder zur Seite.

An die Nutzer der Informationstechnik appelliere ich insbesondere möglichst Angebote datenschutzfreundlicher, d. h. sicherer Technik zu nutzen und damit zum eigenen Datenschutz beizutragen. Im Bereich des technischen Datenschutzes wird vieles nicht durch Gesetze, sondern durch andere Normen und Standards geregelt werden müssen. Hierbei setze ich vor allem auch darauf, dass der Gesetzgeber im neuen Bundesdatenschutzgesetz die Rahmenbedingungen für das sog. Datenschutzaudit schaffen wird. Damit würde dem Konsumenten, der vielfach die technischen Fragen der Datensicherheit gar nicht abschätzen kann, ein Gütesiegel für datenschutzfreundliche Produkte an die Hand gegeben (s. Nr. 8.1.2).

1.12 Beratungen und Kontrollen, insbesondere Beanstandungen

Die Kenntnis der tatsächlichen Abläufe bei der Erfüllung von Aufgaben ist Grundlage für die Beratung des Deutschen Bundestages und der Bundesregierung. 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, von Telekommunikationsunternehmen, von Unternehmen, die Postdienstleistungen erbringen, und von privaten Unternehmen, die unter das SÜG fallen, ausgesprochen wichtig. Im Berichtszeitraum habe ich zu zahlreichen Gesetzesvorhaben und datenschutzrechtlichen Fragen Bundesbehörden und sonstige öffentliche Stellen des Bundes sowie die genannten Unternehmen beraten und kontrolliert (s. hierzu **Anlage 2**).

Nach dem Bundesdatenschutzgesetz in Verbindung mit spezialgesetzlichen Regelungen, wie dem TKG oder PostG, 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. Die Zahl der Beanstandungen in 1999 und 2000 ist gegenüber dem Berichtszeitraum des vorherigen Tätigkeitsberichtes (1997 und 1998) leicht gesunken. 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 Die notwendige Erneuerung des Datenschutzes

2.1 Die Umsetzung der europäischen Datenschutzrichtlinie

2.1.1 Verfahrensstand

Mehr als fünf Jahre nach Verabschiedung der europäischen Datenschutzrichtlinie 95/46/EG im Oktober 1995 steht deren Umsetzung in das deutsche Recht nun endlich unmittelbar bevor. Den Inhalt der Richtlinie, dessen Konsequenzen für das deutsche Datenschutzrecht und die Schwierigkeiten bei der Umsetzung habe ich bereits in meinem 16. und 17. TB (jeweils Nr. 2.1) ausführlich dargestellt. Nachdem in der 13. Legislaturperiode kein entsprechender Gesetzentwurf den parlamentarischen Gremien zugeleitet wurde, enthielt die Koalitionsvereinbarung vom 20. Oktober 1998 unter Nr. IX.13 wenigstens den Passus, das deutsche Datenschutzrecht an die Richtlinie kurzfristig anzupassen. Angesichts der versäumten termingerechten Umsetzung der Richtlinie hat sich die neue Bundesregierung dazu entschlossen, in zwei Stufen vorzugehen. In einer ersten Stufe sollen so rasch wie möglich alle unumgänglichen gesetzgeberischen Anpassungen an die Richtlinie und verschiedene darüber hinausgehende Regelungen erfolgen. Gestützt auf eine erfreuliche Aufgeschlossenheit der beteiligten Koalitionskreise und vor dem Hintergrund des Eckwerte-Papiers aus der SPD-Bundestagsfraktion (vgl. 17. TB Nr. 2.1.2.2) sowie eines Gesetzentwurfs der Fraktion Bündnis 90/Die Grünen vom November 1997 (vgl. 17. TB Nr. 2.1.2.2) hat das federführende BMI über 60 Änderungen an dem ursprünglichen Entwurf vom Dezember 1997 vorgenommen. Hierzu zählen auch die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in mehreren Entschließungen – zuletzt auf ihren Konferenzen vom 25./26. März 1999 und 12./13. Oktober 2000 (vgl. **Anlagen 9** und **24**) – vom Bundesgesetzgeber geforderten Modernisierungsbestrebungen wie die Regelungen zur Videoüberwachung und zu Chipkarten, die Einführung eines Datenschutzaudits, die Verpflichtung auf Datensparsamkeit bis hin zur Datenvermeidung durch Anonymisierung und Pseudonymisierung und noch einige weitere Punkte. Da der Novellierungsbedarf jedoch – aus Datenschutzsicht wie auch aus Sicht der Regierungskoalition – weitaus höher ist, sollen über diesen ersten Teil der Reform hinaus in einer zweiten Stufe die Arbeiten an einer umfassenden Neukonzeption des Datenschutzrechts noch in der laufenden Legislaturperiode aufgegriffen und weitergeführt werden. Trotz der erklärten Absicht, die erforderliche Anpassung an die Datenschutzrichtlinie zügig vorzunehmen, dauerte es noch bis zum 14. Juni 2000, bis das Bundeskabinett den Gesetzentwurf zur Änderung des BDSG beschlossen hat, nachdem bereits im Januar 2000 die Europäische Kommission die Einleitung der 3. Stufe des Vertragsverletzungsverfahrens wegen Nicht-Umsetzung der EG-Datenschutzrichtlinie u. a. gegen Deutschland bekannt gegeben hatte (s. u. Nr. 2.6). Der Bundesrat hat zu dem Gesetzesvorhaben am 29. September 2000 Stellung genommen und dabei eine Reihe von Änderungswünschen formuliert. Der Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze (BT-Drs. 14/4329) ist im Bundestag eingebracht; die Beratungen in den Ausschüssen hatten bei Redaktionsschluss noch nicht begonnen. Ich hoffe, dass die Novellierung des BDSG nun endlich Mitte 2001 in Kraft treten wird.

2.1.2 Vorgaben der europäischen Datenschutzrichtlinie 95/46/EG

Die europäische Datenschutzrichtlinie 95/46/EG enthält im wesentlichen folgende Regelungsansätze, die auch für das deutsche Datenschutzrecht bestimmend sind:

- Reduzierung der Verarbeitung personenbezogener Daten auf das Unvermeidliche:

Die Richtlinie schreibt eindeutig vor, dass der Verarbeitungsvorgang nur im Hinblick auf einen rechtlich zulässigen und präzise definierten Zweck festgelegt werden kann, womit etwa präventive Datensammlungen mit Blick auf künftige, noch nicht feststehende Aktivitäten ebenso ausscheiden wie die Bildung von Datendepots, die sich jederzeit für neue Ziele reaktivieren lassen.

- Schaffung eines Höchstmaßes an Transparenz:

  Um dieses Ziel zu erreichen, sieht die Richtlinie neben einer umfassenden Information des Betroffenen auch – fakultativ – eine Meldepflicht der verarbeitenden Stelle und damit eine Dokumentation der Verarbeitung vor.

- Möglichst effiziente Verarbeitungskontrolle:

  Zentrale Bedeutung kommt dabei dem Auskunftsrecht zu in Verbindung mit der Berechtigung, die Löschung, Sperrung oder Berichtigung unvollständiger oder unrichtiger Daten zu verlangen. Ergänzend treten in bestimmten Fällen Widerspruchsrechte sowie eine Regelung über automatisierte Einzelentscheidungen hinzu, die nur in bestimmten Fällen zulässig sind. Neben diesen Möglichkeiten einer individuellen Kontrolle sieht die Richtlinie – als Alternative zur Meldepflicht – interne Kontrollen durch betriebliche und behördliche Datenschutzbeauftragte sowie eine externe Kontrolle durch eine besondere Kontrollinstanz vor, der neben Untersuchungs- und Einwirkungsbefugnissen auch ein Klagerecht eingeräumt wird.

2.1.3 Neuregelungen im aktuellen Gesetzentwurf

Der von der Bundesregierung beschlossene Gesetzentwurf stellt einen begrüßenswerten Fortschritt gegenüber den früheren Entwürfen dar. Die wichtigsten in der laufenden Legislaturperiode neu in den Entwurf aufgenommenen Vorschriften sind folgende:

- Datenvermeidung und Datensparsamkeit (§ 3a)

  Die neu in das allgemeine Datenschutzrecht aufgenommene Vorschrift des § 3a enthält eine Zielvorgabe für die technische Gestaltung von Datenverarbeitungssystemen. Eine vergleichbare Regelung findet sich bereits in § 3 Abs. 4 des Teledienstedatenschutzgesetzes (TDDSG). Sie hat sich dort bewährt. Wie im TDDSG sollen durch die Einführung des Grundsatzes der Datenvermeidung und Datensparsamkeit schon durch die Gestaltung der Systemstrukturen die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten soweit wie möglich vermieden und dadurch Gefahren für das informationelle Selbstbestimmungsrecht des Betroffenen von vornherein so gering wie möglich gehalten werden. Die Regelung zielt auf den Vorrang anonymer und pseudonymer Formen der Datenverarbeitung als einer von mehreren Möglichkeiten der Ausgestaltung des Systemdatenschutzes ab, um auf diese Weise dem Grundsatz der Erforderlichkeit Rechnung zu tragen. Ergänzt wird die Vorschrift durch die in den Abs. 6 und 6a des § 3 enthaltenen Legaldefinitionen der Anonymisierung und der Pseudonymisierung.

- Vorabkontrolle (§ 4d Abs. 5 und 6)

  In Umsetzung von Art. 20 Abs. 1 der Richtlinie regelt § 4d Abs. 5 die automatisierten Verarbeitungen, die der Vorabkontrolle unterliegen. Die Vorabkontrolle stellt ein Verfahren zur Prüfung der materiellen Zulässigkeit der Datenverarbeitung dar. In dem hierfür einschlägigen Erwägungsgrund 53 heißt es: „Bestimmte Verarbeitungen können jedoch aufgrund ihrer Art, ihrer Tragweite oder ihrer Zweckbestimmung ... oder aufgrund der besonderen Verwendung einer neuen Technologie besondere Risiken im Hinblick auf die Rechte und Freiheiten der betroffenen Personen aufweisen."

  In der Vorabkontrolle sehe ich einen ersten Schritt in die richtige Richtung zu einem wirksamen Schutz gegen einen gebietsübergreifenden und grenzenlosen Einsatz beispielsweise von Videoüberwachung durch öffentliche Stellen und private Unternehmen. Ich denke dabei auch an die Gefahr durch groß angelegte Informationssysteme.

- Automatisierte Einzelentscheidung (§ 6a)

  Mit der Regelung des § 6a wird Art. 15 der Richtlinie umgesetzt. Das bereits oben angesprochene, in der Richtlinie zum Ausdruck gebrachte Prinzip einer möglichst effizienten Verarbeitungskontrolle durch wechselseitige Ergänzung von individueller und institutioneller Kontrolle soll hier eine weitere Ausprägung finden.

- Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen/Videoüberwachung (§ 6b)

  Die Vorschrift stellt die Videoüberwachung erstmals auf eine gesetzliche Grundlage, die der Wahrung des informationellen Selbstbestimmungsrechts durch einen angemessenen Interessenausgleich Rechnung trägt. In Abs. 1 wird schon die Beobachtung selbst von der Regelung erfasst, so dass es nicht auf das Erfordernis einer anschließenden Speicherung des Bildmaterials ankommt. Abs. 2 regelt die Transparenz des Vorgangs der Videoüberwachung, wonach der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen sind.

- Mobile personenbezogene Speicher- und Verarbeitungsmedien/Chipkarten (§ 6c; s. auch u. Nr. 9)

  Der von der Bundesregierung beschlossene Gesetzentwurf sah keine gesetzliche Regelung zu Chipkarten mehr vor. Im Zuge der parlamentarischen Beratungen soll aber wieder ein neu formulierter § 6c in das Gesetz aufgenommen werden. Im Vordergrund dieser Regelung steht die Sicherung der tatsächlichen und dabei insbesondere der informatorischen Voraussetzungen dafür, dass der Betroffene sein informationelles Verhalten kompetent steuern kann. Hierzu

muss er insbesondere erkennen können, welche Möglichkeiten ihm und den beteiligten Stellen eingeräumt werden, wenn er etwa eine Chipkarte benutzt. Dem dienen die Unterrichtungspflichten in Abs. 1 Nr. 1 bis 4. Die Vorschrift des Abs. 2 soll die Realisierung der Informationsrechte des Betroffenen ermöglichen, während Abs. 3 bestimmt, dass die Tatsache der Kommunikation des mobilen personenbezogenen Speicher- und Verarbeitungsmediums für den Betroffenen eindeutig erkennbar sein muss.

- Datenschutzaudit (§ 9a)

  Entsprechend einer bereits in § 17 des Mediendienste-Staatsvertrages enthaltenen Regelung verfolgt das Datenschutzaudit des BDSG-Entwurfs das Ziel, datenschutzfreundliche Produkte auf dem Markt zu fördern, indem deren Datenschutzkonzept geprüft und bewertet wird. Der Deutsche Bundesrat hat in seiner Stellungnahme vom 29. September 2000 angeregt, diese Vorschrift zu streichen. Die Bundesregierung hat sich in ihrer Gegenäußerung vom 30. Oktober 2000 dem nicht angeschlossen. Ich hoffe sehr, dass diese Vorschrift erhalten bleibt.

- Rechte des Bundesbeauftragten für den Datenschutz

  Die bei der Datenverarbeitung in Akten bisher bestehende Begrenzung auf die sog. Anlasskontrolle, bislang in § 24 Abs. 1 Satz 2 geregelt, soll aufgehoben werden. Damit kann ich ohne Anhaltspunkte für eine Rechtsverletzung auch in Akten kontrollieren. Der bisher im Zusammenhang mit dem alle zwei Jahre für den Bundestag zu erstellenden Tätigkeitsbericht in Form einer Sollvorschrift gekleidete Auftrag, „auch eine Darstellung der wesentlichen Entwicklung des Datenschutzes im nicht-öffentlichen Bereich“ zu liefern, wird um die ausdrückliche Befugnis erweitert, mich jederzeit – also unabhängig von dem Medium des Tätigkeitsberichts – an Parlament und Öffentlichkeit zu wenden.

Als weitere Ausprägungen der Regelungsansätze der Richtlinie im aktuellen Gesetzentwurf seien als die wesentlichsten noch genannt:

- Wegfall des Dateiregisters beim Bundesbeauftragten für den Datenschutz und gesetzliche Verpflichtung auch für öffentliche Stellen des Bundes, einen Beauftragten für den Datenschutz zu bestellen (§ 4d Abs. 1 und 2, § 4f Abs. 1, § 4g Abs. 2 und § 26),
- die entsprechende Anwendung der Regelungen über die Auftragsdatenverarbeitung auf Wartungsarbeiten und vergleichbare Unterstützungstätigkeiten an Datenverarbeitungsanlagen (§ 11 Abs. 5),
- die Ergänzung des Widerspruchsrechts gegen die Übermittlung und Nutzung zum Zweck der Werbung um die Pflicht zur Unterrichtung (§ 28 Abs. 4),
- die Modifizierung der Vorschriften zum nicht-öffentlichen Bereich im Hinblick auf die sog. sensitiven Daten (§ 28 Abs. 6 bis 8, § 29 Abs. 5, § 30 Abs. 5) und
- die Änderung der Vorschriften über die Auskunft und die Benachrichtigung (§ 33 Abs. 2, § 34 Abs. 1 bis 3).

Art. 9 der europäischen Datenschutzrichtlinie sieht für die Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt, Abweichungen und Ausnahmen von den einschlägigen Vorschriften der Richtlinie nur insofern vor, als dies notwendig ist, um das Recht auf Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen. Zur Umsetzung dieser Bestimmung in § 41 s. u. Nr. 31.5.

2.1.4 Überlegungen für die zweite Stufe der Datenschutzreform

Die Begründung des aktuellen Gesetzesentwurfs enthält eine begrüßenswerte Absichtserklärung der Bundesregierung zur zweiten Stufe der Novellierung. Darin bekräftigt sie ihr Vorhaben, noch im Laufe dieser Legislaturperiode eine umfassende Neukonzeption des BDSG zu verabschieden. Dem Ziel, das Gesetz in der zweiten Stufe der Novellierung zu modernisieren, zu vereinfachen und seine Lesbarkeit zu erhöhen, kann nur beigepflichtet werden. Auch teile ich die Auffassung, dass im Laufe noch dieser Legislaturperiode das gesamte bereichsspezifische Datenschutzrecht daraufhin zu überprüfen sein wird, ob über die bereits vorgenommenen Änderungen hinaus weitere Anpassungen an die Richtlinie geboten sind, und zwar auch, soweit keine europarechtliche Anpassungspflicht besteht – also außerhalb der Gemeinschaftskompetenzen –, da in der Tat nur so vermieden werden kann, dass es auf Dauer zweierlei Datenschutzrecht mit unterschiedlich hohem Schutzniveau gibt.

Die konkreten Überlegungen zu dieser zweiten Stufe haben gerade erst begonnen, so dass zu deren Regelungsinhalten noch nicht im Einzelnen Stellung genommen werden kann. Folgende Punkte werden aber u. a. anzugehen sein:

- Leichtere Handhabbarkeit und Lesbarkeit des BDSG
- Überprüfung des Verhältnisses von BDSG und bereichsspezifischen Datenschutzgesetzen
- Harmonisierung des Verarbeitungsbegriffs mit der Richtlinie
- Erweiterung und Präzisierung der Regelungen zur Ton- und Bildverarbeitung
- Materielle Stärkung der Befugnisse der Aufsichtsbehörden
- Technischer Datenschutz
- Verbesserung des Selbstschutzes
- Regelung der elektronischen Einwilligung als wichtiger Einzelaspekt mit zentraler Bedeutung
- Auftragsdatenverarbeitung/Outsourcing bei Berufs- oder besonderen Amtsgeheimnissen
- Regelung des Arbeitnehmerdatenschutzes (s. u. Nr. 18.1),
- Förderung und Unterstützung von datenschutzfreundlicher Software
- Selbstregulierung (codes of conduct).

Das ungewöhnliche Vorhaben, ein Gesetzgebungsverfahren in zwei Stufen zu bewältigen, muss zu seinem Abschluss ein ausgereiftes Gesetz erwarten lassen, das unter Einbeziehung der bisher geführten politischen und rechtlichen, wissenschaftlichen wie praxisorientierten Diskussion den Bedürfnissen aller Anwender – Datenverarbeitern wie Betroffenen – entspricht und das, so hoffe ich, anders als seine Vorgänger, nicht schon am Tag seiner Verkündung als reformbedürftig angesehen wird.

2.2 Die Brüsseler Datenschutzgruppe nach Artikel 29 der EG-Richtlinie

2.2.1 Arbeitsschwerpunkte und Ergebnisse

Nachdem ich im 17. TB (Nr. 2.2.1) über die konstituierende Sitzung der Artikel 29-Gruppe und die nachfolgenden Brüsseler Treffen informiert habe, sind für die vergangenen zwei Jahre die Ergebnisse von zwölf weiteren Gruppensitzungen anzuzeigen. Auch dieses Mal behandelte die Gruppe einen weitgespannten Themenbogen, der vom Stand der Umsetzung der EG-Datenschutzrichtlinie in den Mitgliedstaaten der EU (s. u. Nr. 2.6) über Probleme des Internet, der Überwachung des Fernmeldeverkehrs, des E-Commerce, der Telekommunikation und der Genomanalyse bis hin zur Aufnahme eines Grundrechts auf Datenschutz in die Europäische Grundrechtecharta (s. u. Nr. 2.4) reichte. Weitere Beratungsthemen waren der Konzeption von europäischen Verhaltenskodizes in den Bereichen Marketing (FEDMA) und Luftverkehr (IATA) sowie der Ausarbeitung von datenschutzrelevanten Standardvertragsklauseln im internationalen Handelsverkehr gewidmet.

Erneut hat die Gruppe der Öffentlichkeit ihre wesentlichen Beratungsergebnisse in Dokumenten (Working Papers – WP) zugänglich gemacht, die von der Arbeitsunterlage „Die Verarbeitung personenbezogener Daten im Internet“ (WP 16) bis zum Dokument „Privatsphäre im Internet“ (WP 37) reichen (Zusammenstellung der von der Arbeitsgruppe angenommenen Texte s. **Anlage 5**).

2.2.2 Drittstaatentransfer – Das Safe-Harbor-Arrangement

Der internationale Datenschutz im Hinblick auf den Datenverkehr mit Staaten außerhalb der EU bildete, ebenso wie im vorangegangenen Berichtszeitraum, auch dieses Mal den Schwerpunkt der Brüsseler Beratungen.

Rechtlicher Ausgangspunkt ist die in Kapitel IV der Richtlinie geregelte Übermittlung personenbezogener Daten in Drittländer. Nach Art. 25 ist der Datentransfer in Drittstaaten strikten Grundsätzen verpflichtet, die die Richtlinie – dem Adäquanzprinzip folgend – als Angemessenheit des Schutzniveaus definiert (Art. 25 Abs. 1 und 2). Art. 25 sieht in seinem Absatz 6 ferner vor, dass die Europäische Kommission die Angemessenheit des Datenschutzes in einem Drittland „feststellen“ kann, wenn dieses die in der Vorschrift näher genannten Anforderungen erfüllt.

Zunächst billigte die Gruppe in ihren Stellungnahmen vom 7. Juni und vom 7. September 1999 der **Schweiz** und **Ungarn** einen adäquaten Datenschutz zu. Die Europäische Kommission stellte per Entscheidung vom 26. Juli 2000 fest, dass beide Länder ein angemessenes Datenschutzniveau im Sinne von Art. 25 Abs. 2 der Richtlinie gewährleisten (s. u. Nr. 32.2.1 und Nr. 32.2.2).

Komplexer gestaltet sich dagegen das transatlantische Verhältnis der **EU** zu den **USA**. Über die kontroversen Ausgangspunkte der in den vergangenen Jahren geführten Debatte und die mit dem Ziel eines konstruktiven Dialogs von der Gruppe erarbeiteten und in vier Arbeitspapieren niedergelegten gemeinsamen Positionen habe ich bereits im 17. TB (Nr. 2.2.2) berichtet. Aber auch die in den USA einsetzende rechtspolitische Diskussion, die nach wie vor vom Vorrang der Selbstregulierung vor umfassender Gesetzgebung geprägt ist, war schließlich auf die Erarbeitung von Lösungsansätzen zur Überbrückung der Systemunterschiedlichkeiten gerichtet. Sie führte zur von der US-Seite initiierten Safe-Harbor-Diskussion, die seitdem auf der Tagesordnung aller Sitzungen der Brüsseler Artikel 29-Gruppe wie des Artikel 31-Ausschusses der Regierungsvertreter stand (zu diesem s. 17. TB Nr. 2.2.3).

Das Arrangement des „Sicheren Hafens“ sieht vor, dass das US-Handelsministerium ein Verzeichnis derjenigen Unternehmen führt, die sich, um die Vorteile des Systems zu erhalten, öffentlich auf die Grundsätze des Safe Harbor verpflichtet haben. Zu dieser Firmenliste gelangt man über meine Homepage mittels folgender URL: http://www.bfd.bund.de/europa/page3.html. Wer sich auf amerikanischer Seite dem System des Safe Harbor anschließt, ist vor der Sperrung des Datenverkehrs sicher, während im Gegenzug die europäischen Unternehmen wissen, an welche US-Firmen Daten übermittelt werden können, ohne dass zusätzliche Garantien verlangt werden müssen. Schließlich können die Unionsbürger sicher sein, dass ihre Daten vorschriftsmäßig geschützt werden.

Begleitet von fünfzehn „Häufig gestellten Fragen“ (Frequently Asked Questions, FAQs) stützt sich das Safe-Harbor-Konzept auf sieben Prinzipien (den vollständigen Text s. **Anlage 6)**:

- Informationspflichten über die Art der Daten und der Erhebung, den Zweck, die Art der Empfänger und die Wahlmöglichkeiten hinsichtlich der Begrenzung der Nutzung und Übermittlung
- Wahlrecht hinsichtlich der Nutzung der Daten
- Wahlrecht hinsichtlich der Weiterübermittlung der Daten an Dritte
- Angemessene Maßnahmen zur Sicherheit der Datenverarbeitung
- Erforderlichkeit, Richtigkeit, Vollständigkeit und Aktualität der Daten im Rahmen ihrer den Prinzipien entsprechenden Zweckbestimmung
- Recht auf Auskunft
- Effektive Durchsetzung der Prinzipien.

Die Gruppe, die sich zuvor allein im Berichtszeitraum in fünf weiteren Dokumenten mit dem Safe-Harbor-Arrangement befasst hatte (s. **Anlage 5**, WP 19, 21, 23, 27 und 31), verabschiedete anlässlich ihrer Sitzung am 16. Mai 2000 in Brüssel unter meiner Mitwirkung einstimmig die Stellungnahme 4/2000 (s. **Anlage 5**, WP 32). Diese verdeutlicht einerseits die in den zweijährigen Gesprächen mit dem US-Handelsministerium erzielten großen und bedeutsamen Fortschritte für einen verbesserten Schutz personenbezogener Daten, zeigt aber andererseits, dass bei einer begrenzten Zahl grundlegender Fragen noch einige letzte Schritte gesetzt werden müssten. Nach Ansicht der Gruppe enthält das Safe-Harbor-System noch eine Reihe von Schwachstellen, die sich insbesondere in den Punkten Auskunftsrecht, Zweckbindung und Rechtsmittel zeigen.

Auch das Europäische Parlament (EP) stellte in seiner Entschließung vom 5. Juli 2000 eine Reihe von Forderungen an Kommission und Mitgliedstaaten, indem es – wenn auch nicht unter wörtlicher Bezugnahme – die von der Gruppe angemahnten verbliebenen Schwachstellen benannte. Allerdings hielt das EP der Kommission nicht vor, für den Fall einer Entscheidung zugunsten des Safe-Harbor-Arrangements ihre Kompetenzen zu überschreiten. Ohne auf die o.g. Kritikpunkte noch einmal einzugehen, entschied die Kommission denn auch am 26. Juli 2000 (Amtsblatt der Europäischen Gemeinschaften Nr. L 215 vom 25. August 2000, S. 7 ff.).

Zur Genugtuung der Artikel 29-Gruppe enthält die Entscheidung der Kommission eine Überprüfungsklausel in Art. 4 Abs. 1, die es ermöglicht, dass Feststellungen der Angemessenheit im Zusammenhang mit dem Sicheren Hafen überprüft werden können, nachdem das EP Mitgliedstaaten und Kommission aufgefordert hatte, „die Entscheidung im Lichte der Erfahrungen und möglicher künftiger rechtlicher Entwicklungen unverzüglich zu überprüfen“. In diesem Zusammenhang könnten auch die o. g. Schwachstellen – von Seiten des EP wie seitens der Art. 29-Gruppe – wieder aufgegriffen werden.

Auch künftig werden Datenübermittlungen an Stellen in den USA möglich sein, die sich nicht auf Safe Harbor verpflichten. Allerdings muss für diese dann eine der in Art. 26 der Richtlinie vorgesehenen zulässigen Ausnahmen gelten, die beispielsweise in der Einwilligung des Betroffenen liegen könnte, oder es müssten alternative Absicherungen, wie etwa durch einen Vertrag, gegeben sein. Diesem Zweck dienen auch die oben (Nr. 2.2.1) erwähnten Standardklauseln für Musterverträge, die die Europäische Kommission derzeit im Zusammenwirken mit der Artikel 29-Gruppe, den Mitgliedstaaten und Vertretern der privaten Wirtschaft erarbeitet.

2.3 Neue Datenschutzregelungen für die Organe der EU sorgen auch für Einrichtung eines Europäischen Datenschutzbeauftragten

Zwar hat die Gemeinschaft mit der Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 einen beachtlichen Beitrag zur praktischen Umsetzung des Datenschutzes in Europa geleistet (s. Nrn. 2.1 und 2.6). Da die Richtlinie aber gemäß Art. 34 ausschließlich an die Mitgliedstaaten der EU gerichtet ist, konnte sich ihr Geltungsbereich bislang nicht auf die Organe und Einrichtungen von europäischer Gemeinschaft und Union erstrecken. Diese Lücke im europäischen Datenschutzgefüge habe ich immer wieder kritisiert (vgl. 12. TB S. 49, 13. TB S. 57f., 15. TB Nr. 33.6, 16. TB Nr. 2.2 und 17. TB Nr. 2.3). Daneben haben Entschließungen der Konferenz der Europäischen Datenschutzbeauftragten und der Datenschutzbeauftragten des Bundes und der Länder sowie zuletzt das Europäische Parlament das Problem aufgegriffen (s. 17. TB Nr. 2.3).

Einen ersten Schritt zur Behebung dieses Defizits bewirkte die Einfügung von Art. 286 in den am 2. Oktober 1997 als „Vertrag von Amsterdam“ verabschiedeten Unionsvertrag, wonach die Rechtsakte der Gemeinschaft auf Datenverarbeitungen der Organe und Einrichtungen der Gemeinschaft angewendet werden und der Rat aufgefordert wird, auf Vorschlag der Kommission eine Europäische Datenschutzaufsichtsbehörde zur Kontrolle der Gemeinschaftsstellen zu schaffen.

Der hierauf von der Kommission am 15. Juli 1999 vorgelegte Verordnungsvorschlag wurde am 30. November 2000 vom Binnenmarktrat verabschiedet. Nicht zuletzt aufgrund des großen Einsatzes der Bundesregierung für eine zügige Verabschiedung des seit Januar 1999 überfälligen Rechtsaktes konnte hinsichtlich der verbliebenen Änderungsvorschläge zwischen Europäischem Parlament und Rat Übereinstimmung erzielt werden. So beschloss das Europäische Parlament – in Abweichung von der üblichen Reihenfolge – seine Stellungnahme bereits vor dem Zusammentreten des Binnenmarktrates, der am 30. November 2000 die Verordnung in der endgültigen, bereits zuvor vom Parlament gebilligten Fassung verabschieden konnte.

Auf materiellrechtlicher Ebene enthält die Verordnung die „Umsetzung“ von Gemeinschaftsrechtsakten (hier der EG-Datenschutzrichtlinie und der EG-TK-Datenschutzrichtlinie 97/66/EG) mit der Folge, dass deren Bestimmungen – etwa betreffend die Zulässigkeitsvoraussetzungen der Datenverarbeitung, die Betroffenenrechte, die zwingende Einrichtung eines behördlichen Datenschutzbeauftragten oder den Datenschutz im Rahmen interner Telekommunikationsnetze – sich nunmehr in dem an die europäischen Organe und Einrichtungen gerichteten Regelwerk wiederfinden. In einigen Fällen werden Bestimmungen eingeführt, die datenschutzfreundlicher sind als diejenigen der Richtlinie. So ist beispielsweise nach Art. 13 der Zugang zu den von den Gemeinschaftsorganen verarbeiteten Daten immer unentgeltlich, während nach Art. 12 der Richtlinie lediglich die Zahlung „übermäßiger Kosten“ untersagt ist. Die Sicherheit der Verarbeitung ist – entgegen dem entsprechend knapp gehaltenen Art. 17 Abs. 1 der Richtlinie – in Art. 22 der Verordnung erfreulich detailliert geregelt.

Die Verordnung sieht in Art. 41ff. die Einsetzung eines Europäischen Datenschutzbeauftragten vor, dessen Befugnisse denen der Kontrollstelle nach Art. 28 der EG-Richtlinie nachgebildet sind und der nach Artikel 29 Abs. 2 der

Richtlinie künftig als Mitglied der Artikel 29-Gruppe (s. o. Nr. 2.2) angehören wird. Wenn Unionsbürger der Meinung sind, dass sie in ihren Rechten verletzt worden sind, die ihnen durch die Verordnung gewährt werden, können sie künftig ihre Beschwerden direkt an den Europäischen Datenschutzbeauftragten richten, der sein Amt gem. Art. 44 Abs. 1 in völliger Unabhängigkeit ausübt.

2.4 Europäische Charta der Grundrechte

Am 7. Dezember 2000 wurde anlässlich des Europäischen Rates von Nizza von den Staats- und Regierungschefs der Mitgliedstaaten der Europäischen Union, dem Präsidenten der Europäischen Kommission und der Präsidentin des Europäischen Parlaments feierlich die Europäische Charta der Grundrechte verkündet. Damit fand ein Vorhaben seinen Abschluss, zu dem der am 15./16. Oktober 1999 in Tampere tagende Europäische Rat den endgültigen Startschuss gegeben hatte, nachdem sich bereits der Europäische Rat in Köln im Juni 1999 auf Initiative der Bundesregierung in seinen Schlussfolgerungen dafür ausgesprochen hatte, dass „die auf der Ebene der Union geltenden Grundrechte in einer Charta zusammengefasst und dadurch sichtbar gemacht werden". Der Entwurf der Charta wurde seit Dezember 1999 von einem Konvent unter der Leitung des ehemaligen Bundespräsidenten Roman Herzog erarbeitet. Dem Konvent gehörten Vertreter der Regierungen und der Parlamente der Mitgliedstaaten der EU sowie des Europäischen Parlaments an.

Nachdem die Gemeinschaft mit der Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 einen beachtlichen Beitrag zur praktischen Umsetzung des Datenschutzes geleistet hat und der Datenschutz mit der an die Organe und Einrichtungen der Gemeinschaft gerichteten Vorschrift des Art. 286 bereits Eingang in den Vertrag über die Europäische Union gefunden hat (zu dem auf Art. 286 gegründeten Verordnungsvorschlag zum Datenschutz durch Organe und Einrichtungen der Gemeinschaft s. o. Nr. 2.3), bestand als nächste Zielvorgabe zu seiner Bekräftigung auf europäischer Ebene die Aufnahme eines Grundrechts auf Datenschutz in den neu zu schaffenden Katalog.

Aus diesem Grund haben die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und die Artikel 29-Gruppe (s. o. Nr. 2.2.1) die Ausarbeitung der Grundrechtecharta von Anfang an begleitet und sich bereits im Vorstadium der Konventsberatungen geäußert. So forderte die 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 in Rostock Bundesregierung, Bundestag und Bundesrat auf, sich für die Einfügung eines Grundrechts auf Datenschutz in den zu schaffenden Katalog europäischer Grundrechte einzusetzen **(s. Anlage 13).** Auch die Brüsseler Datenschutzgruppe wandte sich mit ihrer Empfehlung 4/99 über die Aufnahme des Grundrechts auf Datenschutz in den Europäischen Grundrechtekatalog vom 7. September 1999 (**Anlage 5** zu Nr. 2.2.1, WP 26) an den Vorsitzenden des Konvents. In einer gemeinsamen Sitzung des Bundestagsausschusses für die Angelegenheiten der EU und des Europa-Ausschusses des Bundesrates am 5. April 2000 in Berlin habe ich für die Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu den Fragen der Aufnahme eines Grundrechts auf Datenschutz in die Charta und seine inhaltliche Ausgestaltung Stellung genommen.

Die in Nizza proklamierte Charta hat die Anliegen des Datenschutzes in erfreulicher Weise aufgegriffen und in Art. 8 mit dem Titel „Schutz personenbezogener Daten" die wesentlichen Grundsätze des Datenschutzes berücksichtigt. Art. 8 lautet:

„(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Personen oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht."

Daneben regelt Art. 42 das Recht auf Zugang zu Dokumenten:

„Die Unionsbürgerinnen und Unionsbürger sowie jede natürliche oder juristische Person mit Wohnsitz oder satzungsmäßigem Sitz in einem Mitgliedstaat haben das Recht auf Zugang zu den Dokumenten des Europäischen Parlaments, des Rates und der Kommission."

Allerdings kommt der Charta eine rechtsverbindliche Wirkung zumindest bis auf weiteres nicht zu, da sie vorerst – entgegen dem von Deutschland unterstützten Vorschlag der französischen Ratspräsidentschaft – nicht in die Verträge über die Europäische Union aufgenommen wurde. Hierfür hätten die in Nizza versammelten Staats- und Regierungschefs einstimmig votieren müssen. Die 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte sich bereits in ihrer Entschließung vom 7./8. Oktober 1999 (s. **Anlage 13**) für eine Verankerung des Grundrechtekatalogs in den Europäischen Verträgen ausgesprochen. Auch das Europäische Parlament plädierte in seiner Entschließung vom 16. März 2000 (BT-Drs. 213/00) für volle Rechtsverbindlichkeit der Grundrechtecharta ebenso wie der Bundesrat in seiner Entschließung vom 14. Juli 2000 (BR-Drs. 378/00) und zuletzt die 26. Europaministerkonferenz der Länder mit ihrem Wismarer Beschluss vom 8./9. November 2000.

Die vorerst wichtigste praktische Bedeutung der Europäischen Grundrechtecharta wird darin liegen, dass der Europäische Gerichtshof sie laut einer entsprechenden Ankündigung in seine ständige Rechtsprechung mit einbeziehen wird.

2.5 Die Konferenz der Datenschutzbeauftragten der Europäischen Union

Die Frühjahrskonferenz der unabhängigen europäischen Datenschutzbehörden vom 14. bis 16. April 1999 in Helsinki behandelte neben allgemeinen Fragen der Daten-

schutzentwicklung in Europa auch die datenschutzrechtlichen Herausforderungen bei Schengen (s. Nr. 11.10), EUROPOL (s. Nr. 11.11) und Interpol. Ein Themenschwerpunkt war dem Phänomen internationaler Datenflüsse und – zugespitzt auf die europäische Rechtslage – dem Drittstaatentransfer nach den Art. 25 und 26 der EG-Datenschutzrichtlinie gewidmet. Daneben standen Fragen der Datenschutzauditierung und die Probleme des Internetzugangs von Arbeitnehmern sowie der Datenschutz im Gesundheitswesen auf der Tagesordnung.

Die Konferenz verabschiedete eine Entschließung zu Aufgaben und Befugnissen der Datenschutzbeauftragten. Vor dem Hintergrund fortlaufender Innovation in der Informationstechnik und den denkbaren Auswirkungen auf die Privatsphäre des Einzelnen sehen es die Datenschutzbeauftragten als besonders wichtig an, eine gute Datenschutzpraxis zu fördern und die Öffentlichkeit hierüber zu unterrichten (s. **Anlage 7**).

Wie auf der Frühjahrskonferenz in Helsinki war auch auf der Stockholmer Tagung dem Schutz von Gesundheitsdaten eine Arbeitssitzung gewidmet. Im Rahmen eines Erfahrungsaustauschs in Form von Länderberichten habe ich dabei über das Thema Gesundheitsreform und Datenschutz in Deutschland referiert. Einen weiteren Themenschwerpunkt bildete eine vergleichende Umschau über die Kontrolltätigkeiten und die Behandlung von Eingaben durch die Datenschutzbehörden in den Mitgliedstaaten der EU. Erörtert wurden in diesem Zusammenhang auch die Ergebnisse des von der Vorjahreskonferenz in Helsinki angeregten Workshops „Complaints Handling“, der am 7./8. Februar 2000 in Manchester die Beschwerdesysteme der einzelnen Mitgliedstaaten in vergleichender Perspektive unter die Lupe nahm. Eine weitere Sitzung des Workshops verfolgte am 26./27. Oktober 2000 in Den Haag u. a. eine Herausarbeitung von Gemeinsamkeiten in den einzelstaatlichen Datenschutzkontrollrechten mit dem Ziel einer Standardisierung bei der Behandlung von Eingaben. Gegenstand weiterer Diskussionen der Konferenz von Stockholm waren das Zusammenspiel von allgemeinem Zugang zu öffentlichen Dokumenten und dem Datenschutz sowie Fragen der internationalen Zuständigkeit und des anwendbaren Rechts nach Art. 4 der EG-Datenschutzrichtlinie. Die Entschließung der Konferenz zur Aufbewahrung von Verkehrsdaten durch Internet Service Provider (s. **Anlage 8**) hat durch den Beschluss der IMK vom 24. November 2000 besondere Bedeutung erlangt. Der Druck seitens der Polizei wird hier sicher weiter zunehmen (s. auch Nrn. 11.8, 14.4).

2.6 Die Umsetzung der Richtlinie 95/46/EG in den Mitgliedstaaten der Europäischen Union

Wie in **Deutschland** (s. o. Nr. 2.1) war in den vergangenen zwei Jahren auch in der Mehrzahl der anderen Mitgliedstaaten der EU das Hauptaugenmerk auf die überfällig gewordene Umsetzung der EG-Datenschutzrichtlinie gerichtet.

Konnten zum Stichtag 24. Oktober 1998 nur die fünf Mitgliedstaaten **Italien, Griechenland, Schweden**, **Portugal** und **Großbritannien** die rechtzeitige Umsetzung nach Brüssel melden und hatte mit geringer Verspätung noch **Belgien** durch das Gesetz vom 11. Dezember 1998 als sechster Mitgliedstaat seine Umsetzungspflichten erfüllt (vgl. 17. TB Nr. 2.1.3), so konnten im Berichtszeitraum vier weitere Länder die Anpassung ihres innerstaatlichen Rechts an die Vorgaben der Richtlinie signalisieren. Auf das Datenschutzgesetz **Finnlands** vom 1. Juni 1999 folgte das Inkrafttreten der Datenschutzgesetze in **Österreich, Spanien** und **Dänemark** im Laufe des Jahres 2000.

Die neugestalteten Datenschutzrechte lassen bereits erkennen, dass die Richtlinie nicht auf einen gleichförmigen europäischen Einheitsdatenschutz zielt, sondern auf harmonisierte nationale Datenschutzsysteme, und dass sie insbesondere von den Mitgliedstaaten zwar ein Tätigwerden fordert, ihnen aber in der konkreten Ausformung die Wahl zwischen mehreren Möglichkeiten lässt. So lassen die bislang in Kraft getretenen reformierten Datenschutzgesetze beispielsweise die in den Mitgliedstaaten vorgefundenen Strukturen der Aufsichtsbehörden unverändert, wonach die bisher schon bestehenden Unterschiede zwischen einer Kommissionsverfassung einerseits (so in Österreich und nach bisherigem und auch künftigem Recht in Frankreich) und einer monokratisch ausgerichteten Stellung der Kontrollstelle andererseits (so in Großbritannien und auch in Zukunft unverändert in Deutschland) aufrecht erhalten bleiben.

Indessen ist der Transformationsprozess in den einzelnen Mitgliedstaaten mit der Notifizierung der die Umsetzung bewirkenden Rechtsakte gegenüber der Europäischen Kommission noch nicht beendet, sondern nur in ein weiteres Stadium getreten. Denn die Kommission unterzieht die innerstaatlichen Umsetzungsmaßnahmen zunächst einer intensiven Prüfung, bevor sie endgültig „grünes Licht“ für eine erfolgreich verlaufene Umsetzung gibt. Hierbei wird sie von der Art. 29-Gruppe (s. o. Nr. 2.2.1) unterstützt, die als Beitrag zur einheitlichen Anwendung der erlassenen einzelstaatlichen Vorschriften diese ebenfalls im Hinblick auf ihre Richtlinienkonformität untersucht.

Bis dahin sind allerdings noch unterschiedlich lange Wege zurückzulegen für die auch jetzt noch säumig gebliebenen Mitgliedstaaten, zu denen – neben **Deutschland** (s. o. Nr. 2.1.1) – die **Niederlande, Luxemburg, Irland** und **Frankreich** zählen. Entsprechend den in Art. 226 des EG-Vertrages vorgesehenen Verfahrensschritten hat die **Europäische Kommission** – nach Versenden eines ersten Mahnschreibens und nach Übermittlung einer sog. begründeten Stellungnahme, die eine formalisierte Zusammenfassung der Tatsachen und Rechtsgründe eines konkreten Vertragsverletzungsverfahrens enthält – nunmehr am 11. Januar 2000 die Einleitung der **dritten Stufe des Vertragsverletzungsverfahrens** gegen die fünf Nachzügler bekannt gegeben. Diese dritte Verfahrensstufe besteht in der Anrufung des Europäischen Gerichtshofs gem. Art. 226 Abs. 2 EG-Vertrag, wenn die in der begründeten Stellungnahme der Kommission gesetzte Frist fruchtlos verstrichen ist. Um einer

Verurteilung zu entgehen, sind die fünf säumigen Mitgliedstaaten nunmehr gehalten, die Verabschiedung der die Umsetzung der Richtlinie bewirkenden Rechtsakte zügig voranzubringen. Am relativ weitesten sind damit die **Niederlande,** in denen beide Kammern des Parlaments den Entwurf eines novellierten Datenschutzgesetzes gebilligt haben, dessen Inkrafttreten aber noch aussteht. In **Luxemburg** wurde der entsprechende Gesetzentwurf im Oktober 2000 dem Parlament unterbreitet, während **Irland** einen noch nicht zwischen allen Ressorts abgestimmten Regierungsentwurf kennt. In **Frankreich** hat die Regierung im Sommer 2000 der Datenschutzkommission (CNIL) ihren Vorentwurf eines novellierten Datenschutzgesetzes zur Prüfung unterbreitet. Mit zahlreichen Änderungen der CNIL wurde der Entwurf dem Conseil d'Etat (Staatsrat) zur weiteren Begutachtung übermittelt. Dessen Votum stand bei Redaktionsschluss noch aus.

Die Art. 29-Gruppe (s. o. Nr. 2.2.1) wies bereits mehrfach auf die zunehmend um sich greifenden Rechtsunsicherheiten mangels Umsetzung der Richtlinie hin und riet zuletzt in ihrer Empfehlung 1/2000 vom 3. Februar 2000 den betroffenen Mitgliedstaaten bzw. ihren Regierungen eindringlich, so schnell wie möglich die erforderlichen Maßnahmen zur Umsetzung der Richtlinie zu ergreifen (s. **Anlage 5**, WP 30).

2.7 Erneuerung der „Zehn Gebote"

Anlässlich der anstehenden Novellierungen der Datenschutzgesetze des Bundes und der Länder wurde im Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Datenschutzbeauftragten von Bund und Ländern eine Empfehlung erarbeitet, die sich mit der Vereinheitlichung der Regelungen zum technischen und organisatorischen Datenschutz befasst. Die Empfehlung soll Hilfen zur Modernisierung der Technikregelungen geben. Die Empfehlung ist über meine Homepage unter „Datenschutz und Technik" abrufbar.

Die Umsetzung der technisch-organisatorischen Verpflichtungen, wie sie im BDSG niedergelegt sind, bereitete in der Praxis immer wieder Schwierigkeiten. Diese wuchsen mit der schnellen Entwicklung der Technik und den dazu nicht mehr passenden oder zeitgemäßen Regelungen im BDSG. Durch diese Entwicklungen, die zunehmende Vernetzung und besonders die Verschmelzung der Informationstechnik mit der Telekommunikation findet ein Paradigmenwechsel im Datenschutz statt.

Die moderne Datenverarbeitung bedarf zur Herstellung einer sicheren Verarbeitung eines methodischen Vorgehens auf der Basis einer Risikoanalyse und eines Sicherheitskonzepts. Um einen sicheren IT-Betrieb zu gewährleisten sollte das IT-Sicherheitshandbuch oder das IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) angewandt werden.

Die Herstellung von Datensicherheit (IT-Sicherheit) bedeutet heute im wesentlichen die Einführung eines Sicherheitsmanagements und ist damit auch eine Managementaufgabe.

Die derzeitigen Technikregelungen in den Datenschutzgesetzen beschreiben konkrete Sicherheitsmaßnahmen und haben dabei im wesentlichen die technischen Komponenten von Datenverarbeitungsanlagen zum Gegenstand. Als Folge hieraus ergibt sich für diese Regelungen eine sehr starke Technologieabhängigkeit. Dies führt zugleich dazu, dass sie in immer kürzer werdenden Abständen der neueren technischen Entwicklung angepasst werden müssen. Besonders die technischen und organisatorischen Maßnahmen

- müssen sich dem Einzelfall anpassen und sind
- vom Schutzbedarf der Daten,
- vom Verarbeitungssystem,
- von der Bedrohungslage und
- vom Stand der Technik abhängig.

Die Anforderungen, die im § 9 BDSG definiert werden, stehen in einem engen sachlichen Zusammenhang mit der Datensicherung (IT-Sicherheit) im Bereich der automatisierten Datenverarbeitung. Man versteht darunter die Summe der Maßnahmen zur Sicherung des ordnungsgemäßen Betriebs einer Datenverarbeitung durch Sicherung der Hardware, Software und Daten vor Verlust, Beschädigung und Missbrauch. Im einzelnen gilt dabei für das Verhältnis von IT-Sicherheit und Datenschutzmaßnahmen folgendes:

- Auf der Ebene des Schutzzweckes: Die IT-Sicherheit dient dem Interesse der datenverarbeitenden Stelle. Die Datenschutzmaßnahmen dienen dem Interesse der Betroffenen.
- Auf der Ebene der Funktion: Die IT-Sicherheit schützt vor Verlust der Vertraulichkeit, Integrität und Verfügbarkeit. Die Datenschutzmaßnahmen schützen vor unzulässiger Verarbeitung und Nutzung personenbezogener Daten.
- Auf der Ebene des Anwendungsbereichs: Die IT-Sicherheit bezieht sich nur auf die automatisierte Datenverarbeitung. Die Datenschutzmaßnahmen beziehen sich auf alle Verarbeitungsarten.
- Auf der Ebene der Maßnahmen: Viele IT-Sicherheitsmaßnahmen dienen der Ausführung des Datenschutzes und viele Datenschutzmaßnahmen erhöhen die IT-Sicherheit.

Aufgrund der aufgezeigten großen Übereinstimmungen hinsichtlich Ziel und Anwendungsbereich der IT-Sicherheit einerseits und den Technikregelungen im BDSG andererseits stellt sich die Frage, warum ähnliche Sachverhalte mit unterschiedlichen Begriffen belegt wurden. Auf der einen Seite die Begriffe der IT-Sicherheit:

- Vertraulichkeit (Schutz vor unbefugter Preisgabe von Informationen)
- Integrität (Schutz vor unbefugter Veränderung von Informationen)
- Verfügbarkeit (Schutz vor unbefugter Vorenthaltung von Informationen oder Betriebsmitteln),

auf der anderen Seite die „Zehn Gebote“ aus der Anlage zu § 9 BDSG:

- Zugangskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Übermittlungskontrolle
- Eingabekontrolle
- Auftragskontrolle
- Transportkontrolle
- Organisationskontrolle

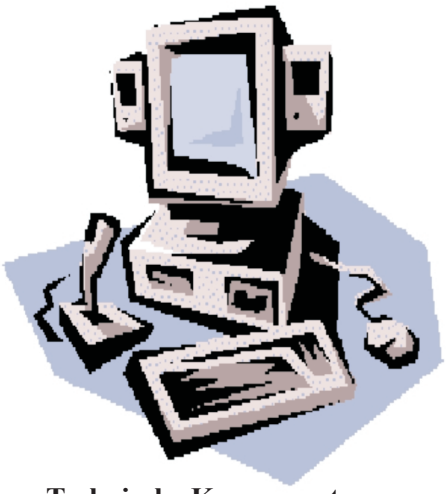
Beide Definitionen weisen sowohl Gemeinsamkeiten als auch Unterschiede auf. Eine Vereinheitlichung würde Klarheit und Sicherheit bringen.

Der technische Datenschutz ist nicht mehr allein an technischen Komponenten festzumachen, sondern auch an den Daten selbst. Den Daten können dabei verschiedene Eigenschaften zugeordnet werden wie **vertraulich, integer und authentisch**. Diese Eigenschaften müssen in jedem Stadium erhalten bleiben unabhängig

- vom Speicherort
- von der Art und Weise der Verarbeitung und
- den technischen Verarbeitungskomponenten (s. Abb. 1).

Abbildung 1 (zu Nr. 2.7)

Technischer Datenschutz



Technische Komponenten

- Vertraulichkeit
- Integrietät
- Verfügbarkeit

Unabhängig vom

– Speicherort

– Art und Weise der Verarbeitung

– den technischen Verarbeitungskomponenten

Technische Komponenten

- vertraulich
- integer
- authentisch

Erkennt man dieses Postulat an, ergibt sich für eine technisch-organisatorische Regelung in Datenschutzrecht ein neuer moderner Ansatz.

Auch die Europäische Datenschutzrichtlinie legt ihr Hauptaugenmerk nicht auf Kontrollen, sondern auf Sicherheitsziele. So werden in den Artikeln 16 und 17 die Sicherheitsziele – Verfügbarkeit, Vertraulichkeit, Integrität – definiert. Ergänzt werden diese Ziele noch durch den Aspekt der Revisionssicherheit (Prüfbarkeit).

Vor diesem Hintergrund wäre es wünschenswert, wenn die Technikregelungen im BDSG in der anstehenden 2. Stufe zur Modernisierung des Datenschutzrechts neu gestaltet und die alten Begrifflichkeiten durch folgende ersetzt würden:

- **Vertraulichkeit**
  Personenbezogene Daten dürfen nur Befugten zur Kenntnis gelangen.
- **Integrität**
  Personenbezogene Daten müssen während der Verarbeitung unverfälscht, vollständig und widerspruchsfrei bleiben.
- **Verfügbarkeit**
  Personenbezogene Daten müssen zeitgerecht für eine ordnungsgemäße Verarbeitung zur Verfügung stehen.

- **Authentizität**
  Personenbezogene Daten müssen jederzeit ihrem Ursprung zugeordnet werden können.
- **Revisionsfähigkeit**
  Es muss festgestellt werden können, wer wann welche personenbezogene Daten in welcher Weise verarbeitet hat.
- **Transparenz**
  Verfahrensweisen bei der Verarbeitung personenbezogener Daten müssen vollständig, aktuell und in einer Weise dokumentiert sein, dass sie in zumutbarer Zeit nachvollzogen werden können.

Durch diese Regelungen kann folgendes erreicht werden:

- Die Begrifflichkeiten des technischen Datenschutzes entsprechen den der IT-Sicherheit.
- Datenschutzkontrollinstanzen und Sicherheitsexperten, Entwicklungsingenieure, Systembetreiber etc. sprechen die gleiche Sprache.
- Technologie-Unabhängigkeit der Sicherheitsziele.
- Sicherheitsziele sind weltweit bekannt und haben sich in Forschung und Praxis als stabil erwiesen.
- Das „Erfüllen“ der Sicherheitsziele erfolgt auf der Basis von anerkannten Methoden und Maßnahmen, da die definierten (Datenschutz-) Sicherheitsziele mit den Zielen der IT-Sicherheit konform sind.
- Es gibt Methoden und Verfahren in der IT-Sicherheit, die als Messlatte für die Sicherheit einer Anwendung herangezogen werden können.
- Die Revisionsfähigkeit eines Verfahrens wird sich an den konkreten Sicherheitsmaßnahmen und an den Sicherheitszielen ausrichten müssen. Auch die Frage der Wirtschaftlichkeit (Ermessensgrundlage) wird dadurch verbessert.
- Mehr Rechtssicherheit, da die Sicherheitsziele nur auf der Basis von methodisch anerkannten Verfahren erreicht werden können.

Besteht ein Bedarf, die Sicherheitsziele noch durch konkrete Maßnahmen zu ergänzen, wäre es ratsam, eine Verordnungsermächtigung im BDSG vorzusehen, mit der das zuständige Ministerium bei besonderen Gefährdungen eingreifen kann.

3 Bundeskanzleramt – LIVE CAM in der Bundeskunsthalle –

Ich bin darauf aufmerksam gemacht worden, dass in der Kunst- und Ausstellungshalle der Bundesrepublik Deutschland in Bonn eine „LIVE CAM“ installiert ist, d. h. eine Kamera, die von dort regelmäßig Bilder in das Internet überträgt. Dabei werden auch Bilder der Ausstellungsbesucher übertragen, die von der LIVE CAM erfasst werden.

Bei einem Besuch der Bundeskunsthalle habe ich mir einen Eindruck über die Arbeitsweise der LIVE CAM verschaffen können. Hierbei habe ich erfreulicherweise feststellen können, dass die Besucher durch verschiedene Hinweisschilder bereits vor Zutritt zur Ausstellung in angemessener Form darüber unterrichtet werden, dass in einem der Ausstellungsräume eine LIVE CAM installiert ist. Diese Hinweise halte ich für unverzichtbar, da die Besucher nur auf diese Weise in die Lage versetzt werden können zu entscheiden, ob sie den von der Kamera erfassten Teil der Ausstellung besuchen und die damit verbundene Möglichkeit akzeptieren wollen, dass ihr Besuch im Internet wahrgenommen wird. Auf ausdrücklichen Wunsch der Besucher wird die Übertragung der Bilder in das Internet aber auch unterbrochen. Insoweit habe ich empfohlen, diejenigen Mitarbeiter, die mit den Besuchern in Kontakt kommen, zu unterrichten, dass sie diese – bei Nachfrage – auf die Möglichkeit der Unterbrechung der Internet-Übertragung hinweisen. Seitens der Bundeskunsthalle wurde mir mitgeteilt, dass dies geschehen sei.

4 Auswärtiges Amt

4.1 Auswärtiges Amt lagert IT-Hilfstätigkeiten aus

Das Auswärtige Amt (AA) hat mich frühzeitig an seinem Vorhaben „partielles Outsourcing im IT-Bereich“ (Gestellung der IT an den Arbeitsplätzen und Aufrechterhaltung der Betriebsbereitschaft) beteiligt. Damit werden IT-Leistungen ausgegliedert und einem privaten Auftragnehmer übertragen. Das AA hat meine Anregungen und Empfehlungen zur Gestaltung des Vertrages mit dem Auftragnehmer übernommen. Der Vertrag enthält Bestimmungen zum Datenschutz und zur Datensicherheit, die den gesetzlichen Vorgaben für die Datenverarbeitung im Auftrag (§ 11 BDSG) Rechnung tragen. Ferner sieht er vor, dass sich der Auftragnehmer verpflichtet, dem behördlichen Datenschutzbeauftragten des AA und unabhängig davon auch mir Kontrollen der Einhaltung datenschutz- und datensicherheitsrechtlicher Vorschriften zu gestatten. Diese Kontrollbefugnisse erstrecken sich auch auf vom Auftragnehmer eventuell beauftragte Dritte (Subunternehmer). Schließlich sind auch Mitteilungs- und Unterrichtungspflichten sowie die Löschungsverpflichtung des Auftragnehmers datenschutzgerecht vertraglich ausgestaltet worden.

4.2 Aufnahme jüdischer Emigranten aus der ehemaligen Sowjetunion

Eingehend habe ich mich mit dem Verfahren zur Aufnahme jüdischer Emigranten aus der ehemaligen Sowjetunion (sog. AjES-Verfahren) auseinandergesetzt. Das Aufnahmeverfahren geht zurück auf eine Vereinbarung, die der Bundeskanzler im Januar 1991 mit dem Zentralrat der Juden in Deutschland getroffen hatte. Danach sollten jüdische Emigranten aus der ehemaligen Sowjetunion ohne zahlenmäßige und zeitliche Begrenzung in der Bun-

desrepublik Deutschland aufgenommen werden. Dieser Vereinbarung haben Bund und Länder unter Berücksichtigung ihrer Aufnahmekapazitäten zugestimmt. Im Gegensatz zu den Spätaussiedlern erhalten die jüdischen Emigranten nicht die deutsche Staatsbürgerschaft, sondern behalten ihre bisherige bei (zum Aussiedleraufnahmeverfahren s. u. Nr. 5.3).

Das AA hat den in Frage kommenden Auslandsvertretungen Anweisungen zur Durchführung des Verfahrens übersandt. Danach wird dieser Personenkreis in analoger Anwendung des Gesetzes über Maßnahmen für im Rahmen humanitärer Hilfsaktionen aufgenommene Flüchtlinge (sog. Kontingentflüchtlingsgesetz) in Deutschland aufgenommen. Die Antragsteller müssen grundsätzlich Staatsangehörige eines Nachfolgestaates der ehemaligen Sowjetunion sein und können ihre Anträge auf Aufnahme nur bei den deutschen Auslandsvertretungen in der ehemaligen Sowjetunion stellen. Sie werden dort über das Verfahren informiert und erhalten die erforderlichen Antragsunterlagen verbunden mit dem Termin für deren Abgabe, der – wegen der Vielzahl der beizubringenden Dokumente, aber auch wegen der erheblichen Zahl der Anträge – regelmäßig auf etwa ein Jahr nach Antragsübergabe anberaumt wird. Die Auslandsvertretung trifft im Regelfall eine abschließende Entscheidung darüber, ob der Antragsteller zum berechtigten Personenkreis gehört. Nach den internen Vorgaben des AA werden alle Anträge der Personen positiv beschieden, die nach den staatlichen Personenstandsurkunden selbst jüdischen Glaubens sind oder von mindestens einem jüdischem Elternteil abstammen. Ohne weitere Prüfung abgelehnt werden Anträge von Personen, deren Mitgliedschaft in einer anderen Religionsgemeinschaft bekannt ist, die bereits in einen anderen Drittstaat übersiedelt oder wegen eines auch nach deutschem Recht strafbaren Vergehens vorbestraft sind.

Ich habe bei der Prüfung der Antragsformulare festgestellt, dass einzelne Datenfelder für die Bearbeitung nicht erforderlich sind und das AA gebeten, die Formulare hinsichtlich der Erforderlichkeit der Angabe personenbezogener Daten eingehend zu überprüfen. Außerdem habe ich einige die Datensicherheit betreffende Mängel festgestellt, deren umgehende Beseitigung mir das AA mündlich zugesagt hat.

Die positiv geprüften Anträge werden an das BVA weitergeleitet, wo nach Eingang der Anträge die Antragsdaten in einer eigens für diesen Personenkreis errichteten Datenbank erfasst werden. Sie bleiben darin bislang ohne spezielle Löschungsregelungen auf Dauer gespeichert.

Die vom AA und BMI erbetenen Stellungnahmen zur Rechtsgrundlage der umfangreichen Datenerhebungen und -speicherungen und zu den Löschungsregelungen lagen bei Redaktionsschluss noch nicht vor.

4.3 Organisation und Einsatz automatisierter Verfahren bei Auslandsvertretungen

Über den Einsatz automatisierter Verfahren bei deutschen Auslandsvertretungen habe ich bereits früher berichtet (vgl. 15. TB Nr. 3.9, 16. TB Nr. 4.1). Nachfolgende Ausführungen gehen auf neue Entwicklungen ein.

4.3.1 Behördlicher Datenschutzbeauftragter für die Auslandsvertretungen

Aus Anlass der Novellierung des BDSG sollte über die Neuorganisation des Datenschutzes bei den Auslandvertretungen nachgedacht werden. Gegenüber dem AA habe ich bereits mehrfach angesprochen, dass der Leiter der Verwaltung in den Auslandsvertretungen, der regelmäßig mit der Funktion des internen Datenschutzbeauftragten betraut wird, in Interessenkonflikte geraten kann, weil er gleichzeitig auch für bestimmte Personalangelegenheiten zuständig ist. Ich habe das AA auf die vorgesehene Möglichkeit der Bestellung eines behördlichen Datenschutzbeauftragten für mehrere Bereiche hingewiesen, wie es der Gesetzentwurf der Bundesregierung zur Novellierung des BDSG in § 4f Abs. 1 Satz 5 vorsieht, und angeregt, die Schaffung von Beauftragten für den Datenschutz bei kleineren Auslandsvertretungen derart zu gestalten, dass ein Datenschutzbeauftragter für einen größeren regionalen Bereich bestellt wird, der nicht zusätzlich Tätigkeiten ausübt, die ihn in Interessenkonflikte bringen können. Bei kleineren Dienststellen könnte ein Ansprechpartner für den Datenschutz bestellt werden, der seine Dienststelle bei einfachen datenschutzrechtlichen Angelegenheiten fachlich beraten kann. Eine vom AA erbetene Stellungnahme zu meinen Vorschlägen steht noch aus.

4.3.2 Mangelhafte Datensicherheit in einer Auslandsvertretung

Den technisch und organisatorisch laxen Umgang mit personenbezogenen Daten in einer Auslandsvertretung habe ich als Verstoß gegen § 9 BDSG beanstandet. Ordner mit besonders schützenswerten Antragsunterlagen für eine Einreise nach Deutschland standen trotz Publikumsverkehrs in offenen Schränken. Aber auch das Verschließen der Schränke hätte angesichts der Qualität der vorgefundenen Schlösser wenig mehr an Sicherheit gebracht. Darüber hinaus waren bei der gleichen Organisationseinheit für mögliche Gerichtsverfahren vorgehaltene Asservate (gefälschte Pässe und sonstige Urkunden) nur in einem einfachen, keiner DIN-Norm entsprechenden Stahlschrank aufbewahrt. Auch war lediglich der Außensicherung auf der Vorderseite des Gebäudes große Aufmerksamkeit geschenkt worden; leider nicht auf der Rückseite. Da das Tor im Zaun ordnungsgemäß verschlossen war, hatten Mitarbeiter den rückwärtigen Zaun etwas heruntergetreten, um bei Bedarf kurzfristig das Botschaftsgelände wieder betreten zu können, ohne lange auf den Kollegen mit dem Schlüssel für das Tor warten zu müssen. Eine schriftliche Stellungnahme zu meiner Beanstandung lag mir bei Redaktionsschluss noch nicht vor. Das AA hat mir aber signalisiert, dass es die festgestellten Mängeln abstellen wird.

4.3.3 Probleme im Zusammenhang mit dem noch verwendeten Betriebssystem

Das AA hat mir mitgeteilt, dass das derzeit in den Auslandsvertretungen noch verwendete Betriebssystem für

die PC und deren Netze durch ein modernes ersetzt werden soll, das bereits in der Zentrale des AA eingesetzt wird. Ich habe das AA aufgefordert, diese Umstellung unverzüglich durchzuführen. Die Nutzung des alten Betriebssystems hat entscheidende Nachteile, da es den Zugriff der Nutzer auf die Betriebssystemebene erlaubt und damit Manipulationsmöglichkeiten eröffnet. Außerdem erschwert es die Aktualisierung der genutzten Viren-Scanner. Die bei Kontrollen vorgefundenen Viren-Scanner mit Viren-Signaturen, die ein bis zwei Jahre alt sind, erfüllen ihren Zweck nicht mehr. Bei Redaktionsschluss lag mir noch keine Zeitplanung zur Umstellung des Betriebssystems vor.

4.3.4 Kontaktpflegeprogramm MAdLAN 2

Das Kontaktpflegeprogramm PERSY, über das ich in meinem 15. TB (Nr. 3.9) berichtet hatte, ist mittlerweile weitgehend durch das Kontaktpflegeprogramm MAdLAN 2 (**M**ultilinguales **Ad**resssystem im **L**ocal **A**rea **N**etwork) ersetzt worden. Es dient im wesentlichen dazu, Adressen von Institutionen und Personen zu speichern, mit denen dienstlicher Kontakt besteht. Neben der Anschrift finden sich in der Regel – insbesondere in den vorhandenen Freitextfeldern – weitergehende Informationen zur Person, etwa zur Stellung in der Behörde des Gastlandes oder in einem Unternehmen sowie zum Zweck der Aufnahme in die Datei (z. B. Einladung zum Empfang anlässlich des 3. Oktober). Aufgrund meiner Kontrollen habe ich das fehlende Anwendungsmanagement gerügt. Dies betrifft z. B. die fehlende Schulung der Mitarbeiter und die mangelnde Absicherung des Systems nach außen. Dem AA habe ich empfohlen, die Anwendung von MAdLAN ausdrücklich zu regeln. Das System muss in jedem Fall so eingerichtet werden, dass der Nutzer nur auf die für seine Aufgabenerfüllung erforderlichen Datensätze zugreifen kann.

4.3.5 Programm VISA

In den Visa-Stellen der deutschen Botschaften und Generalkonsulate wird in der Regel das Programm VISA genutzt, das aus den Dateien Visadatei, Visaversagungsdatei und Konsultationsdatei besteht. In den §§ 7 und 8 der Ausländerdateienverordnung ist im einzelnen geregelt, welche Daten dort wie lange gespeichert werden dürfen. An der erforderlichen Pflege der Dateien mangelt es jedoch häufig. Immer wieder finden sich Eintragungen, deren Grund von den Mitarbeitern vor Ort nicht mehr nachvollzogen werden kann. Gleiches gilt für Mehrfacheintragungen, die nur insoweit gerechtfertigt sind, wie die Transkription von Namen in lateinische Buchstaben zu unterschiedlichen Schreibweisen führen kann. Zwar habe ich für die große Belastung der Mitarbeiter in den Visa-Stellen der Auslandsvertretungen Verständnis, gleichwohl sollte der interne Datenschutzbeauftragte die Datensätze regelmäßig stichprobenhaft auf ihre Erforderlichkeit kontrollieren, damit die mangelhafte Pflege der Dateien abgestellt werden kann.

5 Innere Verwaltung

5.1 Ausländerrecht

5.1.1 Speicherung der Daten von EU-Bürgern im Ausländerzentralregister – Petition an das EU-Parlament –

Im Dezember 1999 wurde mir von der Präsidentin des Europäischen Parlaments eine Petition zur Stellungnahme übersandt, in der es im Kern um die Frage ging, ob die generelle Speicherung von Daten von Staatsangehörigen eines Mitgliedstaates der EU, die ihren Wohnsitz in der Bundesrepublik Deutschland haben, im Ausländerzentralregister (AZR) gegen die europäische Datenschutzrichtlinie 95/46/EG verstößt.

Nach deutschem Recht ist diese Speicherung vorgeschrieben, so dass auch alle in Deutschland lebenden Staatsangehörigen eines Mitgliedstaates der EU als Ausländer im AZR registriert werden. Das BMI, das ich um eine Stellungnahme hierzu gebeten hatte, hält diese Rechtslage für richtlinienkonform, da die Speicherung im AZR für die Aufgabenerfüllung einer Vielzahl von Stellen erforderlich sei. Hieraus ließen sich sowohl das Vorliegen der Freizügigkeitsvoraussetzungen im Sinne des Aufenthaltsgesetzes/EWG entnehmen als auch ausländerrechtliche Entscheidungen wie Ausweisung und Abschiebung, was für die Durchsetzung von Einreise- und Aufenthaltsverboten nach § 8 Abs. 2 AuslG nötig sei. Eine Diskriminierung der EU-Bürger liege nicht vor, da diese hinsichtlich ihres Aufenthaltsrechts nicht vollständig den deutschen Staatsangehörigen gleichgestellt seien.

Bei meiner rechtlichen Prüfung bin ich zu dem Ergebnis gekommen, dass im Einzelfall die Speicherung von Daten eines in der Bundesrepublik Deutschland lebenden Staatsangehörigen eines Mitgliedstaates der EU im AZR erforderlich im Sinne des Art. 7 Buchstabe e) der Richtlinie 95/46/EG sein kann, und zwar dann, wenn es um die Registrierung speziell ausländerrechtlicher Entscheidungen wie Ausweisung oder Abschiebung geht. Dies rechtfertigt aber nicht die systematische Erfassung aller in Deutschland wohnenden Staatsangehörigen eines Mitgliedstaates der EU, deren Daten – wie bei jedem deutschen Staatsangehörigen auch – zusätzlich dezentral in den Melderegistern enthalten sind. Fragen der Verwaltungsvereinfachung, die sich aus einer zentralen Speicherung im AZR ergeben können, begründen keine Erforderlichkeit im Sinne der Richtlinie.

Eine Bewertung der Petition durch das Europäische Parlament selbst ist mir bislang nicht bekannt geworden. Das BMI hat angedeutet, dass es eine Änderung des AZR-Gesetzes in diesem Punkt, die ich aus rechtlichen Gründen für geboten halte, prüfen werde.

5.1.2 Allgemeine Verwaltungsvorschriften zum Ausländergesetz

Wie bereits in meinem 17. TB (Nr. 5.2.1) ausgeführt, war es in der abgelaufenen 13. Legislaturperiode nicht möglich, die Allgemeinen Verwaltungsvorschriften zum Aus-

ländergesetz trotz abschließender Behandlung durch das Bundeskabinett in Kraft zu setzen, da die erforderliche Zustimmung des Bundesrates nicht herbeigeführt werden konnte. Inzwischen hat der Bundesrat den Verwaltungsvorschriften mit der Maßgabe der vollständigen Umsetzung der gleichzeitig beschlossenen Änderungen zugestimmt (BR-Drs. 350/99). Nach erneuter Kabinettsbefassung sind die Allgemeinen Verwaltungsvorschriften zum Ausländergesetz nunmehr am 7. Oktober 2000 in Kraft getreten (Beilage zum Bundesanzeiger Nr. 188a).

Mit dem Inkrafttreten der Verwaltungsvorschriften und dem bereits überarbeiteten Vordruck für die Abgabe einer Verpflichtungserklärung – damit verpflichtet sich eine Person gegenüber der Ausländerbehörde oder einer Auslandsvertretung, für eine bestimmte Zeit die Kosten für den Lebensunterhalt eines von ihr eingeladenen Ausländers zu tragen – gehe ich davon aus, dass eine das Verfahren klarstellende Auslegung der §§ 82 und 84 AuslG für die zuständigen Behörden vorliegt. Erfreulicherweise werden jetzt Angaben zu Einkommens-, Vermögens- und Wohnverhältnissen des Einladenden lediglich für die amtliche Verwendung erhoben. Diese Daten werden dem Eingeladenen oder Dritten nicht mehr bekannt. Dieses Ergebnis entspricht meinen Empfehlungen.

5.1.3 Ausländerrechtliche Vermerke in Pässen

Ein Landesbeauftragter für den Datenschutz hat mich darauf aufmerksam gemacht, dass die Ausländerverwaltung in die Pässe ausländischer Mitbürger nicht nur Einreise- und Aufenthaltsrechte einträgt, sondern auch vermerkt, dass die Verlängerung eines Schengen-Visums abgelehnt worden ist. Darüber hinaus sehen die inzwischen in Kraft getretenen Allgemeinen Verwaltungsvorschriften zum Ausländergesetz (AuslG-VV) anlässlich entsprechender Maßnahmen vor, z. B. den Vermerk „Ausgewiesen“ oder „Abgeschoben“ ebenso anzubringen wie Kontrollvermerke durch Inlandsbehörden, insbesondere zur Überwachung von Visumsfristen. Gegenüber dem BMI habe ich die Auffassung vertreten, dass in den Nationalpässen anderer Staaten allenfalls solche Vermerke vorgenommen werden dürfen, die in einem unmittelbaren Zusammenhang mit der Einreise, dem Aufenthalt und gegebenenfalls der Zulässigkeit einer Erwerbstätigkeit eines Ausländers stehen. Darüber hinausreichende Vermerke sind nach Völkergewohnheitsrecht im internationalen Reiseverkehr und somit von der Zweckbestimmung der Vermerke für die entsprechenden Seiten in den Nationalpässen nicht mehr gedeckt. Bedenken habe ich vor allem zu Vermerken wie „Ausgewiesen“ oder „Abgeschoben“ geäußert. Das BMI stimmt meinen Bedenken zum Umfang der Vermerke zwar grundsätzlich zu, es teilt sie allerdings nicht hinsichtlich der vorgenannten Vermerke und meint, dass ein „numerus clausus“ über erlaubte Passvermerke im Völkerrecht nicht existiere. Die Grenze für die Zulässigkeit von Passvermerken bilde die Maßgabe, dass ein Pass nicht zweckentfremdet werden dürfe. Da aber diese Vermerke das Bestehen einer gesetzlichen Wiedereinreisesperre verdeutlichten, bestehe eine Verbindung zu späteren Einreise- und Aufenthaltskontrollen, denen der Pass diene. Ob die deutsche Vorgehensweise den internationalen Gepflogenheiten entspricht, prüft das BMI derzeit im Zusammenwirken mit dem AA. Darüber hinaus will das BMI meine Anregung prüfen, ob für die Vermerke „Ausgewiesen“ und „Abgeschoben“ nicht nur in den AuslG-VV, sondern im Ausländergesetz selbst eine Rechtsgrundlage geschaffen wird. Ich werde über den Fortgang der Angelegenheit berichten.

5.1.4 Sind Anfragen stellvertretender Behörden an das Ausländerzentralregister zulässig?

Durch Informationen des AZR über die Anfrage einer Polizeidirektion, ob es zulässig sei, im automatisierten Abrufverfahren auch stellvertretend für eine benachbarte Polizeidirektion Informationen aus dem Register abzurufen, wurde ich auf eine ungewöhnliche Praxis in einigen Bundesländern aufmerksam. Diese im AZR-Gesetz nicht vorgesehene Verfahrensweise geht darauf zurück, dass einige Länder aus Rationalisierungsgründen Polizeidirektionen beauftragen, die Aufgaben einer benachbarten Polizeidirektion – besonders für Nachtschichtzeiten – zu übernehmen. Während dieser stellvertretenden Tätigkeit fallen auch Abfragen des AZR an. Diese erfolgen dann aber nur unter der Nutzerkennung der beauftragten und nicht unter der Kennung der vertretenen Dienststelle.

Dadurch lässt sich mit der im AZR erfolgten Protokollierung der Abfragen zwar die abfragende Stelle ermitteln, nicht aber die Dienststelle, für die die Abfrage erfolgt ist. Mein Bestreben war es daher, eine aussagefähige Protokollierung zu finden, die datenschutzrechtlichen Anforderungen genügt. Hierzu hat das BMI nunmehr einen Vorschlag zur künftigen Verfahrensweise unterbreitet. Danach sollen Vertreterabfragen für Behörden, die der gleichen Behördengruppe angehören, künftig ausnahmsweise zulässig sein, wenn in einem sog. Freitextfeld zusätzlich die Angaben der vertretenen Dienststelle und der den Abruf veranlassenden Person eingetragen werden. Diese Angaben würden zwar protokolliert, da es sich dabei aber um Angaben in einem Freitextfeld, also um freiwillige Angaben handelt, werden sie systemseitig nicht zwingend gefordert.

Um den Belangen der Praxis gerecht zu werden, wäre ich bereit, meine Bedenken gegen die vorgeschlagene Verfahrensweise dann zurückzustellen, wenn zwischen Bund und Ländern auf der Basis des vom BMI vorgeschlagenen Verfahrens Vereinbarungen über die Behandlung von Stellvertreteranfragen getroffen würden. Darin sollte unter anderem festgelegt werden, dass es sich bei Vertreterabfragen um Ausnahmefälle handelt und dass in diesen Fällen Angaben im Freitextfeld zwingend erforderlich sind.

5.2 Asylrecht

5.2.1 Bundesamt für die Anerkennung ausländischer Flüchtlinge – BAFl –

5.2.1.1 Sprachspeicherverfahren im BAFl

Um eine gleichmäßigere Auslastung der Kanzleikräfte bei allen Außenstellen zu erreichen, hat das BAFl ein IT-ge-

stütztes Sprachspeicherverfahren eingeführt. Mit diesem Verfahren ist es insbesondere den Einzelentscheidern möglich, ihre Schriftsätze wie bei herkömmlicher Technik in einen digitalen Sprachspeicher zu diktieren. Je nach Auslastung kann der Diktierende sein Diktat auf elektronischem Wege der Kanzlei in der eigenen Außenstelle zuleiten oder es der Koordinierungsstelle der Zentrale des BAFl zur Weiterleitung an eine Außenstelle mit freien Kapazitäten übergeben.

Bei der Sprachspeicherauswertung in einer Außenstelle erkennt die Kanzlei aufgrund von Kennzahlen die Priorität jeden Dokuments. Nach Fertigstellung kopiert die Kanzleikraft das Dokument in einen nur dem jeweiligen Diktierenden zugeordneten elektronischen Ordner und speichert das Dokument ab.

Bei Steuerung des Sprachspeichersystems durch die zentrale Koordinierungsstelle wird der diktierte Text elektronisch an deren Verteilerarbeitsplatz in Nürnberg gesandt. Sie kann aus dem zugeleiteten Diktat u. a. den Absender, die Priorität und den Umfang des Dokuments erkennen. Da sie den Überblick über die Auslastung der Kanzleien aller Außenstellen hat, kann sie die Fertigung der ihr zugeleiteten Schreibaufträge bedarfsgerecht und im Sinne einer gleichmäßigen Auslastung aller Kanzleikräfte steuern. Das gefertigte Dokument wird den Diktierenden unmittelbar elektronisch übermittelt.

Ich konnte mich im BAFl davon überzeugen, dass das Sprachspeichersystem, das auch Bestandteil des neuen Dokumentenmanagement- und Workflowsystems IT-2000 des BAFl werden soll (s. u. Nr. 5.2.2), datenschutzgerecht eingerichtet ist.

5.2.1.2 Sprach- und Textanalyse (S-T-A) im BAFl

Nach den Erfahrungen des BAFl belegt eine größere Zahl von Asylantragstellern die eigene Identität bzw. Herkunft nicht in befriedigender Weise oder versucht, diese bewusst zu verschleiern. Das BAFl setzt daher zur Herkunftsfeststellung dieser Personen das mit Sprachwissenschaftlern entwickelte Sprach- und Textanalysesystem (S-T-A) ein.

Zum Zeitpunkt meiner Kontrolle im Frühjahr 2000 hatte das BAFl etwa 470 S-T-Analysen vorgenommen. Schwerpunkte bildeten dabei der westafrikanische Sprachraum sowie Albanien, Kosovo und Mazedonien und der besonders schwierig zu analysierende kurdisch/armenische Sprachraum. Das Verfahren wurde anfangs in 13 Außenstellen des BAFl eingesetzt, seit Juli 2000 ist es in allen Außenstellen eingeführt.

Asylbewerber, bei denen das „S-T-A-Verfahren“ angewandt werden soll, werden bereits vor der Anhörung darauf aufmerksam gemacht, dass ihre Aussagen zur Überprüfung ihrer Herkunft auch zu Sprachanalysen herangezogen werden können und die auf Tonband aufgenommenen Gespräche an Sprachexperten zur Auswertung übersandt werden. Das Gespräch für eine Sprachanalyse findet nach der Anhörung des Asylbewerbers statt und wird durch den Einzelentscheider unter Hinzuziehung eines Dolmetschers durchgeführt. Das Bundesamt hat zu dem bisher verwendeten Merkblatt „Hinweise für die Aufnahme von Gesprächen mit Asylbewerbern zum Zwecke einer Sprachanalyse“ als verbindliche Regelung zum Ablauf des Verfahrens eine Anweisung „S-T-A-Verfahren“ herausgegeben, die den kompletten Verfahrensablauf regelt. Als positiv habe ich bewertet, dass der Asylbewerber aufgefordert wird, während der Aufnahme weder Aussagen über seine Asylgründe zu machen noch den eigenen Namen oder den dritter Personen zu nennen.

Die Tonbandaufnahme wird nur unter Angabe des Aktenzeichens dem mit der Analyse beauftragten Institut zugeleitet, das sie nach der Auswertung mit dem Gutachten an das BAFl zurücksendet. Eine Löschung der Unterlagen aus dem Sprachanalyseverfahren ist nach der Bestands- oder Rechtskraft des Asylverfahrens in Aussicht genommen. Mit Blick auf diese Zeitvorgabe sind bisher noch keine Löschungen erfolgt.

Insgesamt bewerte ich die im Sprachanalyseverfahren praktizierten Verfahrensschritte aus datenschutzrechtlicher Sicht als sachgerecht. Ob diese ausreichen, werden die praktischen Erfahrungen der nächsten Monate zeigen. Das BAFl habe ich gebeten, mich weiter unterrichtet zu halten.

5.2.1.3 Zugriff des BAFl auf das Schengener Informationssystem

Seit geraumer Zeit versucht das BAFl einen Zugriff auf die Daten des Schengener Informationssystems (SIS) gemäß Art. 96 des Schengener Durchführungsübereinkommens (SDÜ) zu erhalten. Dieser war dem Bundesamt bislang verwehrt, da es in der Liste der zugriffsberechtigten Stellen nach Art. 101 Abs. 2 SDÜ nicht aufgeführt ist. Von einem solchen Zugriff verspricht sich das BAFl größere Chancen, ein erfolgreiches Übernahmeersuchen bei einem anderen Vertragsstaat zu stellen. Nach seiner Ansicht sind SIS-Ausschreibungen zur Einreiseverweigerung als Indiz dafür anzusehen, dass sich ein asylsuchender Ausländer zu einem früheren Zeitpunkt in dem ausschreibenden Staat aufgehalten hat. Das BMI unterstützt diese Bemühungen und hat mich gebeten, dem Zugriff des BAFl auf die beim BVA gemäß Art. 96 SDÜ geführte Kopie des SIS-Datenbestandes zuzustimmen. Als Begründung führt es an, das BAFl sei eine für die Erteilung von Aufenthaltstiteln gemäß § 43 a AsylVfG zuständige Behörde im Sinne von Art. 101 Abs. 2 SDÜ. Der angestrebte Zugriff lediglich auf die beim BVA gespeicherte Kopie des SIS-Datenbestandes, die nicht den Gesamtbestand des SIS enthält, stellt nach Ansicht des BMI sicher, dass das BAFl nur auf die für seine Aufgabenerfüllung erforderlichen Daten zugreifen würde.

Im Dialog mit dem BMI, an dem auch das BMJ beteiligt war, habe ich erreicht, dass dem BAFl der Direktzugriff im Dialogverfahren auf den beim BVA geführten Datenbestand versuchsweise erst dann eingeräumt wird, wenn auf europäischer Ebene keine Bedenken gegen die Aufnahme des Bundesamtes in die Liste der zur unmittelbaren Abfrage der SIS-Daten berechtigten Behörden erhoben werden. Das BMI hat mir inzwischen mitgeteilt, dass

die zuständigen Gremien, nämlich die Ratsarbeitsgruppe Schengener Informationssystem und der Art. 36-Ausschuss, keine Bedenken haben und somit die Zustimmung der anderen EU-Mitgliedstaaten auf fachlicher Ebene erteilt ist. Das BAFl hat daraufhin am 1. Juli 2000 den absprachegemäß bis zum 31. März 2001 befristeten Probebetrieb aufgenommen. Die anschließende Auswertung wird zeigen, ob die vom BAFl prognostizierten Verfahrensvorteile für die Bundesrepublik Deutschland eintreten werden.

5.2.2 Projekt IT-2000 im BAFl

Das BAFl setzt seit 1985 zur Unterstützung der Verfahrensabläufe bei der Entscheidung über die Asylanträge die elektronische Datenverarbeitung ein. Das bislang verwendete Datenbanksystem ASYLON, dessen Kapazität nahezu erschöpft ist, soll künftig durch das System IT-2000 ersetzt werden. Damit soll sowohl ein Dokumentenmanagement- als auch ein sog. Workflowsystem eingerichtet werden, mit dem vor allem das „papierarme Büro“ angestrebt wird. Im Jahr 1999 sind u. a. die Konzepte für die Übernahme der Daten des bisherigen Datenbanksystems in die neue Datenbank (Migration), Datenmodellierung und Gesamtdesign entwickelt worden; derzeit wird ein Prototyp getestet. Es ist vorgesehen, sämtliche Dokumentvorlagen im zentralen Rechenzentrum in Nürnberg vorzuhalten und allen Anwendern bedarfsorientiert zur Verfügung zu stellen (s. Abb. 2). Nach erfolgreichem Wirkbetrieb in der Außenstelle Dortmund soll das Verfahren in allen Außenstellen eingesetzt werden. Dabei wird die Übernahme der gesamten Anwendung des bisherigen Systems ASYLON auch aus datenschutzrechtlicher Sicht von zentraler Bedeutung sein. Ich habe das Projekt IT-2000 schon frühzeitig beratend begleitet und mich mehrfach über die Verfahrensfortschritte vor Ort informiert. Ich gehe davon aus, dass im Jahr 2001 in ausgewählten Bereichen mit dem Echtbetrieb begonnen wird.

5.2.3 Europäisches daktyloskopisches Fingerabdrucksystem zur Identifizierung von Asylbewerbern – EURODAC –

In meinem 17. TB habe ich ausführlich über die Regelungen des geplanten Europäischen daktyloskopischen Fingerabdrucksystems zur Identifizierung von Asylbewerbern berichtet (Nr. 5.7). Das seinerzeit dargestellte Verfahren zur Einführung von EURODAC sah zunächst den Abschluss einer Konvention des Europarats, eines Zusatzprotokolls sowie der erforderlichen Durchführungsbestimmungen vor. Inzwischen sind die ursprünglich getrennt vorgesehenen Regelungen in einer einheitlichen EURODAC-Verordnung zusammengefasst worden. Inhaltlich haben sich aus dieser Entwicklung aus meiner Sicht keine gravierenden Änderungen ergeben.

Die EURODAC-Verordnung ist am 15. Dezember 2000 in Kraft getreten (Verordnung (EG) Nr.2725/2000 des Rates vom 11.12.2000 – Abl. EG L 316 vom 15.12.2000) ; sie gilt unmittelbar in allen Mitgliedstaaten der EU. Die praktische Arbeit kann EURODAC aber erst dann aufnehmen, wenn alle Mitgliedstaaten die technischen Voraussetzungen zur Umsetzung und Anwendung von EURODAC geschaffen haben. Dies wird noch etwa zwei Jahre dauern.

5.3 Datenschutz beim Sprachtest im Aussiedleraufnahmeverfahren

Wer einen Antrag auf Aufnahme als Spätaussiedler stellt, hat auf der Grundlage des § 6 Abs. 2 des Bundesvertriebenengesetzes nachzuweisen, dass er die deutsche Sprache in ausreichendem Maße beherrscht und sie muttersprachlich oder durch den Gebrauch als bevorzugte Umgangssprache in der Familie erlernt hat. Dieser Nachweis erfolgt durch einen Sprachtest, der an ausgewählten deutschen Auslandsvertretungen überwiegend durch Mitarbeiter des BVA durchgeführt wird. Dabei werden in nicht unerheblichem Umfang personenbezogene Daten der Betroffenen erhoben und verarbeitet. Den Umgang mit diesen Daten habe ich an zwei Auslandsvertretungen in Russland geprüft. Dabei habe ich mich im wesentlichen auf den vom BVA entwickelten „Wegweiser für Sprachtester“ gestützt. Der Test soll dem Sprachtester einen Eindruck vermitteln, ob der Betroffene in der Lage ist, eine zwanglose Unterhaltung unter Berücksichtigung der besonderen Bedingungen der Sprachweitergabe in seinem Herkunftsland in deutscher Sprache zu führen. Das Gespräch bewegt sich weitgehend in Themenkreisen aus dem persönlichen Umfeld des Antragstellers oder in seinen Alltagssituationen. Über den Ablauf des Sprachtests fertigt der Tester ein Anhörungsprotokoll. Es enthält alle in den Themenblöcken gestellten Fragen sowie die wortgetreue Wiedergabe der Antworten des Antragstellers. Dieses Protokoll verbleibt nicht in der Auslandsvertretung, sondern wird Bestandteil der beim BVA geführten Akte des Antragstellers.

Die Erhebung und Speicherung personenbezogener Daten der Teilnehmer an Sprachtests im Rahmen des Aussiedleraufnahmeverfahrens bei den von mir geprüften Stellen trägt den datenschutzrechtlichen Anforderungen Rechnung. Dabei bewerte ich insbesondere die Vorgaben des BVA für die Durchführung der Sprachtests als sachgerecht und mit den datenschutzrechtlichen Belangen der Betroffenen vereinbar.

5.4 Kommt ein Suchdienstedatenschutzgesetz?

Seit geraumer Zeit fordere ich gesetzliche Regelungen für die Aufgabenwahrnehmung durch den DRK-Suchdienst und den Kirchlichen Suchdienst (vgl. 13. TB Nr. 5.11). Erfreulicherweise hatte die Bundesregierung im Einklang mit meinen Empfehlungen im Sommer 1998 ihre Bereitschaft erklärt, die Verarbeitung und Nutzung personenbezogener Daten durch die Suchdienste sobald wie möglich gesetzlich zu regeln. In Erwartung dieses Gesetzesentwurfs habe ich mir bei beiden Suchdiensten einen Eindruck über den aktuellen Stand der Datenverarbeitung verschafft. Dabei habe ich mich davon überzeugen können, dass der Einsatz der elektronischen Datenverarbeitung zu

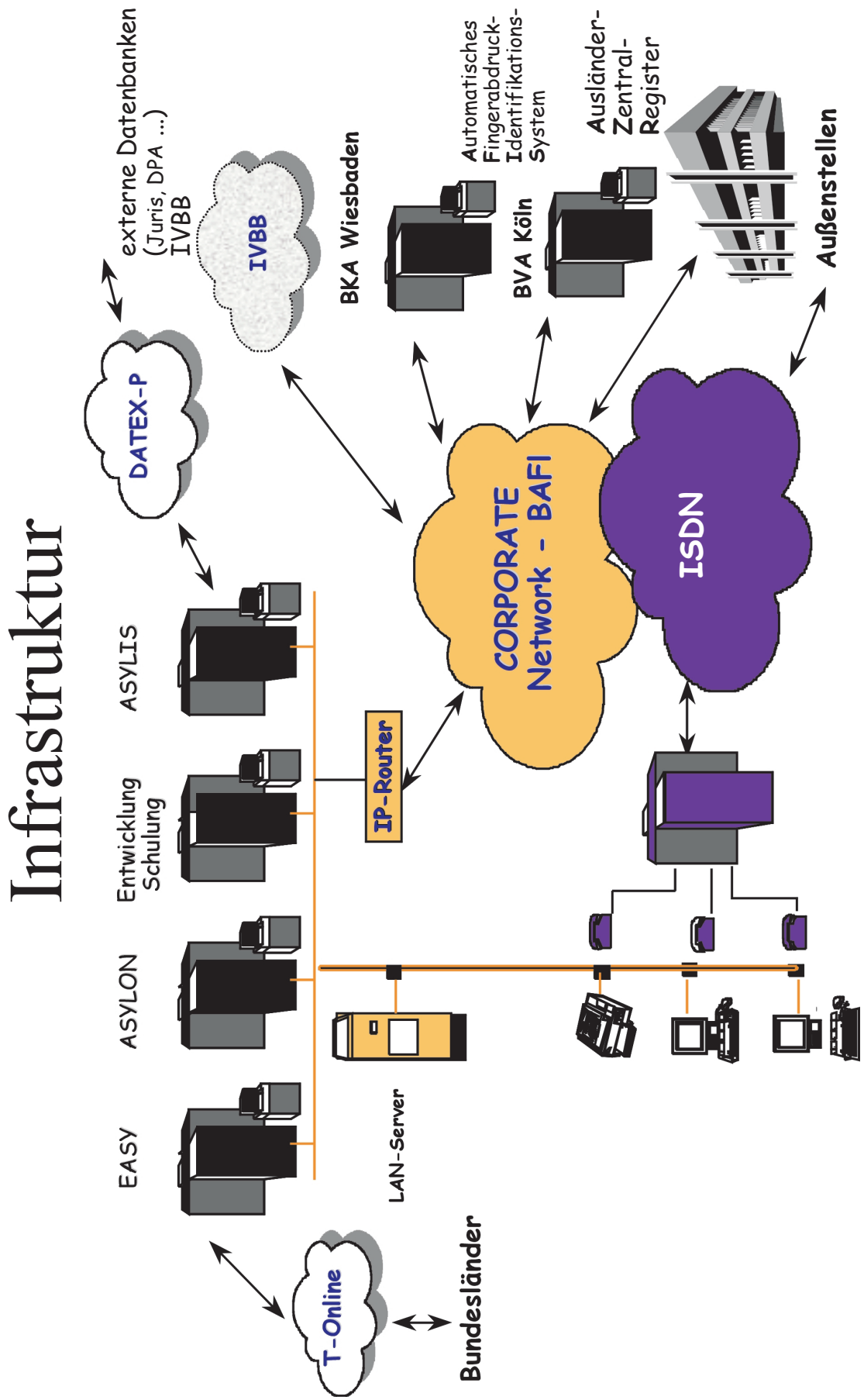


Abbildung 2 (zu Nr. 5.2.2)

datenschutzrechtlichen Verbesserungen, etwa bei der Feststellung der Identität der Gesuchten, geführt hat. Bei Redaktionsschluss lag mir ein erster Entwurf eines Suchdienstedatenschutzgesetzes vor, der aber noch nicht mit den Ressorts und den beteiligten Organisationen erörtert worden ist.

5.5 Bundesanstalt Technisches Hilfswerk

Die Bundesanstalt Technisches Hilfswerk (THW) ist meinen bereits früher erhobenen Forderungen (s. auch 11. TB S. 18 f., 12. TB S. 25), Regelungen für den Einsatz von DV-Systemen zu schaffen und ein IT-Konzept zu erstellen, nachgekommen. Darüber hinaus hat sie inzwischen die Anwendersoftware „THWin" entwickelt, die ein fester Bestandteil der EDV auf allen Arbeitsebenen des THW geworden ist. Im Rahmen eines Beratungs- und Kontrollbesuchs habe ich den Einsatz dieser Software, insbesondere unter dem Aspekt der Verwaltung der personenbezogenen Daten der beim THW tätigen Helfer, sowohl bei der Leitung des THW als auch bei einem Landesverband, einem Geschäftsführer und einem Ortsverband geprüft. Nur bei wenigen Einzelanwendungen musste ich Verbesserungen anregen, für die inzwischen Lösungen gefunden worden sind. Insgesamt sehe ich die Rechte der Helfer in dem vom THW eingesetzten Verfahren „THWin" gewahrt.

5.6 Wer nimmt künftig die datenschutzrechtliche Kontrolle der Bundesdruckerei wahr?

Die Bundesdruckerei GmbH nimmt bei der Herstellung personalisierter Dokumente (z. B. Personalausweise, Reisepässe) eine wichtige Rolle wahr, über die ich wiederholt berichtet habe (zuletzt 17.TB Nr. 5.10). Seit Juli 1994 ist sie eine Gesellschaft mit beschränkter Haftung, deren Anteile zu 100 % der Bundesrepublik Deutschland gehören. Bei derartigen Besitzverhältnissen habe ich stets die Auffassung vertreten, dass ich nach § 2 Abs. 1 und 3 i. V. m. §§ 24 Abs. 1 und 26 Abs. 3 BDSG für die datenschutzrechtliche Kontrolle und Beratung der Bundesdruckerei GmbH weiterhin zuständig bin. Diese Aufgaben habe ich seitdem auch wahrgenommen.

Als sich im Laufe des Jahres 2000 andeutete, dass die Bundesrepublik Deutschland ihre Anteile zu veräußern beabsichtigt, habe ich das BMI auf die Probleme aufmerksam gemacht, die sich aus datenschutzrechtlicher Sicht ergeben können, wenn die Bundesdruckerei GmbH an ein privates Unternehmen verkauft werden sollte. Insbesondere wollte ich mir Klarheit über den künftigen Umfang meiner Kontrollkompetenz verschaffen. Sie wäre weiterhin gegeben, wenn die Bundesdruckerei GmbH, die dann zwar als eine nicht-öffentliche Stelle im Sinne des BDSG, zumindest in den Bereichen, in denen personenbezogene Daten verarbeitet werden (Herstellung der Personalausweise, Pässe und Führerscheine), anzusehen wäre, auch hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen würde.

Auf meine Anfrage hat mir das BMI mitgeteilt, dass die Bundesdruckerei GmbH nach seiner Auffassung in diesen Bereichen keine derartigen Aufgaben wahrnimmt. Diese Rechtsauffassung würde bedeuten, dass die Daten aller Personen, für die die Bundesdruckerei GmbH eines der oben genannten Dokumente herstellt, künftig einem rein privatrechtlich tätigen Unternehmen zugeleitet würden. Eingaben und meine langjährigen Kontakte zur Bundesdruckerei GmbH haben aber gezeigt, dass die Bürger sich in hohem Maße um einen an den gesetzlichen Vorgaben ausgerichteten Umgang mit ihren besonders schützenswerten Daten, die der Bundesdruckerei GmbH anvertraut werden, besorgt sind. Durch meine Beratungen und Kontrollen, aber auch durch frühzeitige Beteiligungen seitens der Bundesdruckerei GmbH, habe ich erreichen können, dass bei der Herstellung der in Rede stehenden Ausweisdokumente ein hoher datenschutzrechtlicher Standard gewahrt ist. Dies muss auch in Zukunft sichergestellt bleiben.

Anfang Dezember 2000 ist die Bundesdruckerei GmbH an ein privates ausländisches Unternehmen verkauft worden. Das BMI geht inzwischen davon aus, dass sich meine Kontrollbefugnis lediglich auf die ordnungsgemäße Speicherung der Seriennummern der hergestellten Dokumente, die aufgrund gesetzlicher Vorgaben zentral bei der Bundesdruckerei GmbH erfasst werden, beschränkt.

Demgegenüber halte ich an meiner umfassenden Kontrollzuständigkeit fest. Zum einem sehe ich die Tätigkeiten der Bundesdruckerei GmbH im Zusammenhang mit der Herstellung von Personaldokumenten als Vorbereitung hoheitlicher Aufgaben. Zum anderen bleibt die Bundesdruckerei GmbH auch nach Änderung der Eigentumsverhältnisse für alle Bundesländer tätig (§ 2 Abs. 3 Nr. 1 BDSG). Zur Wahrung der Rechte der betroffenen Bürger gebietet dies zwingend eine einheitliche Datenverarbeitung, deren Kontrolle wie bislang durch mich wahrzunehmen ist. Das BMI habe ich über meine Auffassung unterrichtet.

5.7 Novellierung des Melderechtsrahmengesetzes – MRRG –

Das BMI bereitet mit dem Entwurf eines 3. Gesetzes zur Änderung des Melderechtsrahmengesetzes eine Novellierung des Melderechts vor.

In diesem Zusammenhang habe ich insbesondere die bisher praktizierte Auskunftserteilung im Rahmen der einfachen Melderegisterauskunft kritisiert. Von wenigen gesetzlichen Ausnahmeregelungen (u. a. Gefahr für Leben, Gesundheit und persönliche Freiheit) abgesehen, kann der Betroffene zur Zeit nicht verhindern, dass seine personenbezogenen Daten bei dieser Auskunftsart an jedermann herausgegeben werden. Ich fordere daher für den Bürger ein Widerspruchsrecht gegen die Weitergabe seiner personenbezogenen Daten im Rahmen der einfachen Melderegisterauskunft. Dabei darf nicht danach unterschieden werden, ob die Melderegisterauskunft in herkömmlicher oder in elektronischer Form an die Meldebehörde gerichtet wird. Nur dann sehe ich den Schutz der

zwangsweise beim Bürger zur Erfüllung hoheitlicher Aufgaben erhobenen Daten gewährleistet.

Weiterhin habe ich gefordert, die technische Ausgestaltung der elektronischen Abrufe von Auskünften aus dem Melderegister in Einzelheiten bereits im Melderechtsrahmengesetz zu regeln. Nur so kann gewährleistet werden, dass die Sicherheitsstandards bundeseinheitlich in gleicher Weise geregelt werden.

Des weiteren ist die Abschaffung der Hotelmeldepflicht für deutsche Staatsangehörige vorgesehen. Dies entspricht einem von mir bereits länger verfolgten Anliegen.

Der Referentenentwurf zum MRRG ging erst nach Redaktionsschluss bei mir ein.

5.8 Die Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR

5.8.1 Verwendung der Stasi-Abhörprotokolle

Im Frühjahr 1999 entwickelte sich anlässlich der Beratungen des parlamentarischen Untersuchungsausschusses zur CDU-Spendenaffäre ein Streit darüber, ob und in welchem Umfang der Untersuchungsausschuss auf Stasi-Abhörprotokolle zurückgreifen darf. Obwohl es sich dabei nicht um eine neue Problematik handelte, führte diese Frage zu einer heftigen politischen Diskussion, in der leider auch behauptet wurde, dass ost- und westdeutsche Personen der Zeitgeschichte unterschiedlich behandelt würden. Dies lag wohl zum einen daran, dass es um die Person des Altbundeskanzlers Helmut Kohl ging, und sich zum anderen die Fragestellung anschloss, ob denn diese und damit auch ähnliche Unterlagen, die andere Personen der Zeitgeschichte betreffen, an Wissenschaftler und Medien herausgegeben werden dürfen.

Ich habe in dieser Diskussion immer den Opferschutzgedanken des Stasi-Unterlagen-Gesetzes (StUG) in den Vordergrund gestellt. Die Stasi-Abhörprotokolle sind illegal entstandene Unterlagen, die nach den Grundsätzen unseres Rechtsstaates nicht hätten entstehen dürfen. Sie dürfen deshalb jetzt nicht zum Nachteil der Opfer der Praktiken des MfS genutzt werden. Eine Unterscheidung der Stasiopfer nach ihrer Herkunft – Ost oder West – habe ich zu jeder Zeit abgelehnt.

In der Zwischenzeit sind verschiedene juristische Gutachten erstellt worden, die wegen ihrer unterschiedlichen Ergebnisse nicht zur endgültigen Klärung der Rechtsfragen beigetragen haben. Bei Redaktionsschluss lag noch keine endgültige Entscheidung vor, wie die BStU die aktuellen und künftigen Anfragen behandeln wird.

5.8.1.1 Herausgabe an parlamentarische Untersuchungsausschüsse

Bereits im Jahre 1995 hatte der sog. Schubladenausschuss des Kieler Landtages ebenfalls Zugriff auf Stasi-Abhörprotokolle der BStU nehmen wollen. Das Landgericht Kiel hatte seinerzeit festgestellt, dass Stasi-Abhörprotokolle nicht an den parlamentarischen Untersuchungsausschuss herausgegeben werden dürfen, weil die Rechte der Betroffenen aus Art. 10 Abs. 1 GG bezüglich der durch das Abhören des Fernmeldeverkehrs gewonnenen Stasi-Unterlagen Vorrang gegenüber dem Aufklärungsinteresse eines parlamentarischen Untersuchungsausschusses hätten. Das Urteil spiegelte somit meine Rechtposition wider (vgl. 16. TB Nr. 5.9.1 und 17. TB Nr. 5.9.1). Aufgrund dieses Urteils und auch im Hinblick auf die Stellungnahme der Bundesregierung zu meinem 16. TB, die sich meiner Auffassung angeschlossen hatte, habe ich eine ursprünglich von mir geforderte eindeutige Regelung im StUG nicht weiterverfolgt.

In Übereinstimmung mit dem Urteil des LG Kiel gehe ich unverändert davon aus, dass parlamentarischen Untersuchungsausschüssen nicht in jedem Fall der Zugang zu Stasi-Abhörprotokollen offen stehen darf. Zwar haben sie nach Art. 44 Abs. 1 GG die „erforderlichen Beweise zu erheben“, aber nach Absatz 2 finden die Vorschriften über den Strafprozess sinngemäß Anwendung, und das Brief-, Post- und Fernmeldegeheimnis bleiben unberührt. Die Frage ist aber zunächst, ob sich das Zugangsrecht parlamentarischer Untersuchungsausschüsse auf alle Stasi-Unterlagen erstreckt oder ob es Grenzen gibt, und wenn ja, wo diese Grenzen liegen. Da es sich um ein verfassungsrechtlich abgesichertes Zugangsrecht parlamentarischer Untersuchungsausschüsse handelt, sind zunächst die Grundsätze zu beachten, die das Bundesverfassungsgericht zur Auslegung von Art. 44 GG bereits entwickelt hat.

Das Beweiserhebungsrecht parlamentarischer Untersuchungsausschüsse und der grundrechtliche Datenschutz stehen sich gleichwertig gegenüber und bedürfen im konkreten Einzelfall einer Abwägung, so dass beide Rechte soweit als möglich zur Geltung kommen können. Demzufolge ist Art. 44 GG so auszulegen, dass einerseits die verfahrensrechtlichen Voraussetzungen für eine wirksame parlamentarische Kontrolle gewährleistet sind und andererseits das Persönlichkeitsrecht sowie auch andere Grundrechte (z. B. Art. 10 GG) gewährleistet bleiben.

Im vorliegenden Fall ist besonders zu beachten, dass es um die Herausgabe von Stasi-Abhörprotokollen geht, also um Informationen, die illegal und auf rechtsstaatswidrige Weise gewonnen wurden. Da gemäß Art. 44 Abs. 2 Satz 2 GG das Brief-, Post- und Fernmeldegeheimnis unberührt bleibt, dürfen parlamentarische Untersuchungsausschüsse nicht in Art. 10 GG eingreifen. Nach der Rechtsprechung des Bundesverfassungsgerichts stellt aber nicht nur die Aufzeichnung der kommunikativen Daten einen Grundrechtseingriff dar, sondern auch deren Kenntnisnahme und Verwertung durch einen Träger der öffentlichen Gewalt (BVerfGE 85, 386, 389). Das bedeutet, dass auch staatliche Maßnahmen, die die Kenntnisnahme ermöglichen (dies wären neben den Protokollen auch Abschriften von Tonträgern) einen Eingriff in Art. 10 GG darstellen. Da parlamentarische Untersuchungsausschüsse öffentliche Gewalt ausüben, sind die Kenntnisnahme und Verwertung der Stasi-Abhörprotokolle durch parlamentarische Untersuchungsausschüsse Eingriffe in den durch Art. 10 GG geschützten Bereich. Auf diesen

Schutz kann der Betroffene allerdings verzichten, beispielsweise wenn er den Kommunikationsvorgang selbst offen legt oder in die Kenntnisnahme durch parlamentarische Untersuchungsausschüsse einwilligt.

Es stellt sich daher die weitere Frage, ob dieser Eingriff in das Brief-, Post- und Fernmeldegeheimnis durch das StUG gerechtfertigt ist, wobei einzig § 22 StUG in Betracht kommt. Dabei ist zu fragen, ob ein parlamentarischer Untersuchungsausschuss unabhängig von seinem Untersuchungsauftrag auf alle Stasi-Unterlagen zugreifen darf oder ob dies nur dann zulässig ist, wenn der Gegenstand der Untersuchung mit den Zielen des StUG in Übereinstimmung steht. Wenngleich der Wortlaut des § 22 StUG für eine unbegrenzte Zugriffsmöglichkeit zu sprechen scheint, ist diese Vorschrift – wie auch die übrigen Regelungen des Gesetzes – vor dem Hintergrund der allgemeinen und grundsätzlichen Bestimmungen des Gesetzes zu betrachten. Damit sind vor allem die besonderen Verwendungsverbote gemäß § 5 StUG angesprochen, vorrangig das sog. Nachteilsverbot gemäß § 5 Abs. 1 Satz 1 StUG. Dieses lautet: „Die Verwendung personenbezogener Informationen über Betroffene oder Dritte, die im Rahmen der zielgerichteten Informationserhebung oder Ausspähung des Betroffenen einschließlich heimlicher Informationserhebung gewonnen worden sind, zum Nachteil dieser Personen ist unzulässig.“ Dieses Verwendungsverbot gilt für alle Vorschriften des StUG, es sei denn, seine Anwendung ist ausdrücklich ausgeschlossen, was in § 22 StUG nicht der Fall ist.

Darüber hinaus ergibt auch eine an Sinn und Zweck des StUG orientierte Auslegung den Vorrang des § 5 StUG. Das StUG regelt die Erfassung, Erschließung, Verwaltung und Verwendung der Unterlagen des MfS. Damit verbunden sind die in § 1 des Gesetzes genannten Zwecke:

- Dem Einzelnen den Zugang zu ermöglichen, um die Einflussnahme der Stasi auf sein persönliches Schicksal aufzuklären;
- den Einzelnen davor zu schützen, durch den Umgang mit den Stasi-Unterlagen in seinem Persönlichkeitsrecht beeinträchtigt zu werden;
- die historische, politische und juristische Aufarbeiung der Tätigkeit der Stasi zu gewährleisten;
- öffentlichen und nicht-öffentlichen Stellen die erforderlichen Informationen für die in diesem Gesetz genannten Zwecke zur Verfügung zu stellen.

Das Gesetz will also vor allem die Persönlichkeitsrechte dieser Personen schützen, ist also ein Gesetz zum Schutz der Opfer. In diesem Lichte ist auch der letztgenannte Zweck zu sehen. In erster Linie sollen die Machenschaften der Stasi aufgeklärt, die Opfer rehabilitiert und die Täter bestraft werden. Somit folgt aus dem Sinn und Zweck des Gesetzes, dass nur solche parlamentarischen Untersuchungsausschüsse Zugang zu den Stasi-Unterlagen erhalten dürfen, deren Gegenstand die Aufarbeitung der Tätigkeit der Stasi oder der Schutz des Persönlichkeitsrechts gegen die von Stasi-Unterlagen ausgehenden Gefahren nach § 1 Abs. 1 Nr. 1 bis 3 StUG ist.

5.8.1.2 Verwendung durch Wissenschaftler und Medien

Bis April 2000 bin ich davon ausgegangen, dass die BStU keine Stasi-Abhörprotokolle von Betroffenen (Opfern) ohne deren Einwilligung an Medien herausgibt. Aufgrund von Presseveröffentlichungen in FOCUS und SPIEGEL vom 3. April 2000 wurde jedoch bekannt, dass Journalisten Anträge auf Akteneinsicht nach dem StUG in Unterlagen über den ehemaligen Schatzmeister der CDU Leisler Kiep gestellt und daraufhin entsprechende Unterlagen erhalten haben. Hierunter befanden sich auch Stasi-Abhörprotokolle, bei denen noch nicht einmal private Details geschwärzt waren. Über die Medien erfuhr ich also erstmals im Fall Leisler Kiep, dass die BStU Stasi-Abhörprotokolle an die Medien herausgegeben hat, in denen der Betroffene nicht Täter oder Begünstigter, sondern Opfer des MfS war, weil er zielgerichtet ausgespäht wurde.

Die Frage, ob und in welchem Umfang Unterlagen der Stasi an Wissenschaftler und Medien herausgegeben und ggf. veröffentlicht werden können, richtet sich nach § 32 Abs. 1 und § 32 Abs. 3 StUG (Forschung) bzw. nach § 34 Abs. 1 i. V. m. § 32 Abs. 1 und § 32 Abs. 3 StUG (Medien).

Nach § 32 Abs. 1 StUG stellt die BStU für die Forschung zum Zwecke der politischen und historischen Aufarbeitung der Tätigkeit der Stasi sowie für Zwecke der politischen Bildung u. a. Unterlagen mit personenbezogenen Informationen über Personen der Zeitgeschichte, Inhaber politischer Funktionen oder Amtsträger in Ausübung ihres Amtes zur Verfügung, soweit sie nicht Betroffene oder Dritte sind und soweit durch die Verwendung keine überwiegend schutzwürdigen Interessen der genannten Personen beeinträchtigt werden. Gemäß § 34 Abs. 1 StUG, der für die Verwendung von Unterlagen durch die Medien die entsprechende Anwendung des § 32 Abs. 1 StUG vorsieht, wird der Zugriff durch die Medien auf die Unterlagen der Stasi unter denselben Voraussetzungen gestattet, unter denen sie für die Forschung und die politische Bildung zur Verfügung stehen. Dabei können nach § 33 Abs. 3 StUG auf Verlangen auch Duplikate der Unterlagen herausgegeben werden, soweit die Einsichtnahme in die Unterlagen gestattet ist.

Wie diese Vorschriften zu verstehen sind, lässt sich nachfolgend am Fall Leisler Kiep gut darlegen:

Aufgrund seiner damaligen Funktion als Schatzmeister der CDU ist Herr Leisler Kiep als Person der Zeitgeschichte bzw. als Inhaber einer politischen Funktion einzustufen. Nach § 32 Abs. 1 Nr. 3 erster Anstrich StUG war demzufolge vor einer Herausgabe von Unterlagen mit personenbezogenen Informationen zu prüfen, ob er Betroffener oder Dritter ist, was eine Herausgabe unzulässig macht.

Nach § 6 Abs. 3 Satz 1 StUG sind Betroffene Personen, zu denen der Staatssicherheitsdienst aufgrund zielgerichteter Informationserhebung oder Ausspähung einschließlich heimlicher Informationserhebung Informationen gesammelt hat. Dies ist bei Opfern illegaler Abhörmaßnahmen

eindeutig der Fall. Dritte sind gemäß § 6 Abs. 7 StUG sonstige Personen, über die der Staatsicherheitsdienst Informationen gesammelt hat. Diese Voraussetzung liegt vor, wenn die Person der Zeitgeschichte inhaltlich Gegenstand der abgehörten Telefongespräche war. Nach § 6 Abs. 8 StUG ist für jede Information gesondert festzustellen, ob Personen Mitarbeiter des Staatssicherheitsdienstes, Begünstigte, Betroffene oder Dritte sind, wobei maßgebend ist, mit welcher Zielrichtung die Informationen in die Unterlagen aufgenommen worden sind. Nach diesen gesetzlichen Definitionen kann es keinen Zweifel geben, dass – für jedes Protokoll nach § 6 Abs. 8 StUG gesondert festgestellt – die Personen, die das Ziel von illegalen Abhörmaßnahmen waren, Betroffene im Sinne des StUG, und die Personen, über die aus abgehörten Telefongesprächen gezielt Informationen gesammelt wurden, Dritte im Sinne des StUG sind, wenn klar ist, dass sie weder Mitarbeiter noch Begünstigte der Stasi waren. Gemäß den Begriffsdefinitionen des StUG ist Herr Leisler Kiep in jedem Fall entweder Betroffener oder Dritter, sodass eine Herausgabe der Protokolle zu Forschungszwecken ohne seine Einwilligung nicht in Betracht kommen darf.

Trotz des insoweit eindeutigen Gesetzestextes vertritt die BStU die Auffassung, bei Personen der Zeitgeschichte und Amtsträgern greife dieser Persönlichkeitsschutz nicht, soweit es um die Ausführung ihrer Ämter und ihre öffentliche Funktion gehe. Lediglich der private Bereich sei geschützt, sie könnten also Betroffene im Sinne des Gesetzes nur als Privatpersonen und nur beschränkt auf den privaten Bereich sein.

Diese Auffassung überzeugt mich nicht, denn auch nach dieser Rechtsmeinung müsste das illegale Abhören des nicht öffentlich gesprochenen Wortes, etwa in einem vertraulichen Telefonat, dem privaten Bereich zugeordnet werden, weil sich der Betroffene nach seinem Selbstverständnis gerade nicht in der Öffentlichkeit bewegt hat. Der BGH hat bereits im Jahr 1978 entschieden, dass grundsätzlich jeder, auch der in der Öffentlichkeit stehende und sie suchende Politiker, Anspruch auf Wahrung seiner Privatsphäre hat, zu der andere nur insoweit Zugang haben, als er ihnen den Zugang gestattet (BGHZ 73, 120 ff). Der BGH hat dies, wenn auch im Zusammenhang mit dem Spannungsverhältnis zwischen Persönlichkeitsrecht und Pressefreiheit, ausdrücklich auch für die Fälle festgestellt, in denen sich die Inhalte der illegal abgehörten Telefongespräche auf gesellschaftliche und politische Fragen beziehen. Andernfalls würde der Persönlichkeitsschutz für Personen der Zeitgeschichte und Amtsträger partiell außer Kraft gesetzt, was mit dem Grundrechtsschutz des Art. 10 GG nicht zu vereinbaren wäre. Selbst wenn unterstellt wird, dass illegal abgehörte Personen der Zeitgeschichte und Amtsträger keine Betroffenen oder Dritte im Sinne des StUG sind, wäre eine Herausgabe der Protokolle nach § 32 Abs. 1 Nr. 3 letzter Halbsatz StUG nur zulässig, soweit durch die Verwendung keine überwiegenden schutzwürdigen Interessen der genannten Personen beeinträchtigt werden. Angesichts des hohen Ranges, der dem verfassungsrechtlich geschützten Fernmeldegeheimnis vom Bundesverfassungsgericht immer wieder eingeräumt worden ist, sehe ich im illegalen Abhören von Telefongesprächen und der Verwendung inhaltlicher Aufzeichnungen davon einen so weitgehenden Eingriff in das Persönlichkeitsrecht, dass die schutzwürdigen Interessen der betroffenen Person überwiegen und eine Herausgabe weder zu Forschungszwecken noch an die Medien möglich ist.

Die Herausgabe der Stasi-Abhörprotokolle im Fall Leisler Kiep war also nach den Vorschriften des StUG nicht zulässig. Aus diesem Grund habe ich dann auch umgehend eine Beanstandung nach § 25 BDSG ausgesprochen.

5.8.2 Rosenholz-Papiere: Verwendung der Agentenkartei der Stasi

Ende 1999 erschienen Pressemeldungen, nach denen die Klarnamenkartei des DDR-Spionageapparates von der Regierung der Vereinigten Staaten an Deutschland zurückgegeben werden sollte. Dabei handelt es sich um die sog. F 16-Kartei, die unter nicht geklärten Umständen durch eine Operation des amerikanischen Geheimdienstes mit dem Decknamen „Rosenholz“ in den Besitz der USA geriet. Diese Kartei enthält u. a. die Namen von Agenten, die in der Bundesrepublik oder in anderen Ländern für die Stasi tätig waren. Es ist jedoch nicht erkennbar, was genau jemand getan hat und ob er Spion oder nur Spionageziel war. Diese Klarheit ergibt sich erst im Zusammenspiel zwischen der F 16-Kartei und der bereits bekannten sog. F 22-Kartei (Vorgangskartei), das erkennbar macht, ob jemand Agent oder Opfer war. Die Pressemeldungen habe ich zum Anlass genommen, beim BMI und bei der BStU nachzufragen, wie diese Unterlagen rechtlich einzustufen sind und wie sie behandelt werden sollen.

Die BStU hat mir mitgeteilt, dass nicht die in den USA vorliegenden Originale, sondern Kopien von Sicherheitsverfilmungen der genannten Karteien sowie von Statistikbögen der für die Auslandsspionage zuständigen Hauptverwaltung Aufklärung (HVA) des Staatssicherheitsdienstes auf CD-ROM übergeben werden. Das BMI hat mitgeteilt, dass es sich bei den Inhalten der Datenträger – bisher wurden drei CD-ROM zur Verfügung gestellt – um „sonstige Duplikate“ im Sinne von § 6 Abs.1 Nr. 1 b) StUG handelt, deren weitere Behandlung sich nach den Vorschriften dieses Gesetzes richtet. Vor diesem Hintergrund gehe ich von einem sorgfältigen Umgang mit diesen sensiblen Daten aus.

Ergänzend hat das BMI darauf hingewiesen, dass die Lieferung der weiteren etwa 1 000 zu erwartenden CD-ROM noch längere Zeit in Anspruch nehmen wird.

5.8.3 Weitere Beratungen und Kontrollen der BStU und ihrer Außenstellen

Im Berichtszeitraum habe ich sowohl die Zentrale in Berlin als auch zwei Außenstellen der BStU beraten und kontrolliert. Dabei habe ich im Großen und Ganzen erneut einen sorgfältigen und gewissenhaften Umgang mit den äußerst sensiblen Unterlagen wahrgenommen. Soweit ich anlässlich der Besuche auf Mängel gestoßen bin, sind diese nach Möglichkeit umgehend behoben worden. Er-

freulicherweise findet auch ein intensiver Dialog zwischen der Zentrale und den Außenstellen statt. So konnte ich vielfach bei der Kontrolle einer Außenstelle feststellen, dass von mir vorher in einer anderen Außenstelle kritisierte Verfahrensweisen bereits entsprechend meiner Empfehlungen geändert worden waren.

Ein Problem in den Außenstellen ist, wie lange Besucherscheine aufzubewahren sind. Besucher einer Außenstelle müssen sich zunächst bei der Wache melden, bei der sie ihren Personalausweis hinterlegen, um einen Besucherschein zu erhalten. Beim Verlassen des Gebäudes geben sie den Besucherschein an der Wache wieder ab und erhalten ihren Ausweis zurück. Die Besucherscheine werden dann in der Regel in einem Stahlschrank für die Dauer von zwei Jahren aufbewahrt, um etwaige Unregelmäßigkeiten aufklären zu können. Ich habe bei meinen Besuchen stets angeregt, die Besucherscheine, sofern sie aufbewahrt werden müssen, höchstens für ein Jahr aufzuheben. Erfreulicherweise ist die BStU jetzt bereit, die Dauer der Aufbewahrung nochmals grundsätzlich zu überprüfen. Ein Ergebnis lag bei Redaktionsschluss aber noch nicht vor.

5.8.4 Stasi-Listen im Internet

Im Januar 2000 wurde ich durch eine Eingabe und Presseanfragen darauf hingewiesen, dass auf der Internetseite der BStU eine Liste aller Stasi-Mitarbeiter veröffentlicht worden war. Bereits in meinem 14. TB (S. 36 ff.) hatte ich mitgeteilt, dass von 1991 bis Anfang 1993 zahlreiche Presseveröffentlichungen mit hochsensiblen, offenkundig aus den Archiven der Stasi stammenden Angaben über mögliche Stasi-Verbindungen von Politikern und Kirchenvertretern erschienen waren, sowie Listen mit Namen und Dienststellen angeblicher hauptamtlicher Mitarbeiter und Offiziere im besonderen Einsatz der Stasi abgedruckt wurden. Ich hatte ferner darauf hingewiesen, dass in der Wendephase in erheblichem Umfang Unterlagen abhanden gekommen sind und nunmehr auf einem grauen Markt feilgeboten wurden.

Die BStU teilte mir zu der erneut veröffentlichten Stasi-Liste mit, dass fremde Nutzer auf ihrer Homepage unter der Rubrik „Schwarzes Brett“ Links zu fremden Websites angebracht hätten, von denen die Liste heruntergeladen werden könnte. Das „Schwarze Brett“ werde von Mitarbeitern der BStU regelmäßig überprüft. Beiträge, die derartige Links oder andere ähnliche personenbezogene Informationen enthalten, würden unverzüglich gelöscht. Ferner hat die BStU an ihrem „Schwarzen Brett“ einen Warnhinweis angebracht, der sowohl auf mögliche Manipulationen bei den Listen selbst, als auch auf den Umstand hinweist, dass nicht alle vom Ministerium für Staatssicherheit besoldeten Personen Mitarbeiter der Stasi waren. Insofern hat die BStU aus meiner Sicht die erforderlichen datenschutzrechtlichen Maßnahmen ergriffen.

Anhand von Pressemitteilungen und aufgrund weiterer Eingaben habe ich festgestellt, dass die Stasi-Liste auch unter anderen Web-Adressen im Internet zu finden war. Der BGH hat in einem Urteil aus dem Jahre 1994 festgestellt, dass die Veröffentlichung des Namens einer Person in einer Liste über „IM-Registrierungen“ eine schwerwiegende Verletzung des Persönlichkeitsrechts des Betroffenen darstellt, die einen Anspruch auf Unterlassung und auf Unkenntlichmachung des Namens in der Liste begründet. Das Bundesverfassungsgericht hat in seinem Beschluss vom 23. Februar 2000 die gegen dieses Urteil eingelegte Verfassungsbeschwerde nicht angenommen. Das Verfassungsgericht hat in seiner Begründung aber darauf hingewiesen, dass es bei der Abwägung zwischen den Grundrechten der Meinungsfreiheit und dem allgemeinen Persönlichkeitsrecht durch den BGH verfassungsrechtliche Defizite sieht. Dabei stellt das Gericht – aus meiner Sicht zurecht – in erster Linie auf das Interesse an der Veröffentlichung der Stasi-Liste und somit auf die Aufarbeitung der Stasi-Vergangenheit ab.

5.9 Staatsangehörigkeitsdatei

Wie bereits früher berichtet (16. TB Nr. 5.7 und 17. TB Nr. 5.14), wird seit 1982 beim BVA die Staatsangehörigkeitsdatei – STADA – ohne die hierfür erforderliche Rechtsgrundlage automatisiert geführt. Die Schaffung einer solchen Regelung im Gesetz zur Reform des Staatsangehörigkeitsrechts vom 15. Juli 1999 (BGBl. I S. 1618) war nach Mitteilung des BMI aufgrund politischer Vorgaben nicht möglich, denn zunächst sollten vor allem die Koalitionsvereinbarungen für den staatsangehörigkeitsrechtlichen Bereich umgesetzt werden. Nunmehr soll allerdings eine besondere Rechtsgrundlage für die STADA bei der anstehenden Neuregelung (Gesamtreform) des Staatsangehörigkeitsrechts geschaffen werden. Dabei wird insbesondere zu prüfen sein, ob und inwieweit der Datenbestand der STADA im Rahmen einer etwaigen Neustrukturierung reduziert werden kann. In diese Prüfung sind auch aufwachsende Datenbestände einzubeziehen, wie beispielsweise die Übernahme von Daten aus dem Datenbestand des AZR in die STADA (im Fall der Einbürgerung).

Des weiteren werden die Auswirkungen der mit dem Gesetz zur Reform des Staatsangehörigkeitsrechts erfolgten Erweiterungen der Aufgaben des BVA zu prüfen sein. Nach § 17 des Gesetzes zur Regelung von Fragen der Staatsangehörigkeit in der ab dem 1. Januar 2000 geltenden Fassung ist das BVA zuständig, wenn der Erklärende oder der Antragsteller seinen dauernden Aufenthalt im Ausland hat. Dies betrifft neben der Zuständigkeit für die Feststellung der deutschen Staatsangehörigkeit beispielsweise die Entgegennahme von Geburtsanzeigen sowie die Erteilung von Beibehaltungsgenehmigungen und die Durchführung der Optionsverfahren bei Erklärungspflichtigen, soweit nicht eine Zuständigkeit der Länder gegeben ist. In diesen Fällen sowie bei Einbürgerungen von im Ausland lebenden Personen verarbeitet das BVA personenbezogene Daten im Rahmen eigener Aufgabenerfüllung.

Auch in Bezug auf die bei den Behörden der Länder angefallenen bzw. anfallenden Daten sind Fragen zu klären, wobei u. a. zu beachten ist, dass das Gesetz zur Reform

des Staatsangehörigkeitsrechts keine Regelungen für den Nachweis der deutschen Staatsangehörigkeit enthält. Obwohl durch die Einbeziehung der Länder bei den schwierigen Fragen einer etwaigen Neustrukturierung der STADA der Abstimmungsprozess noch schwieriger wird, werde ich mich dafür einsetzen, dass die angemahnte besondere Rechtsgrundlage für die STADA möglichst kurzfristig geschaffen wird.

5.10 Wahlen

5.10.1 Veröffentlichung der Anschrift der Wahlbewerber

Ein Mitglied des Deutschen Bundestages wandte sich mit der Bitte an mich, für eine datenschutzgerechtere Regelung der §§ 38, 43 Abs. 1 und 45 Abs. 1 Satz 2 Nr. 1 Bundeswahlordnung einzutreten, damit die Anschrift des einzelnen Bewerbers um ein Mandat im Deutschen Bundestag nicht mehr öffentlich bekannt gemacht werden muss.

Meiner Anregung, die Rechtslage zu ändern und die Privatanschrift künftig nicht mehr zu veröffentlichen, ist die Bundesregierung nicht gefolgt. Den Kern ihrer Argumente bildete das überwiegende Allgemeininteresse an der Öffentlichkeit des Wahlgeschäfts, das dem Interesse des Wahlbewerbers an der Geheimhaltung seiner personenbezogenen Daten vorgehe. Die öffentliche Bekanntmachung personenbezogener Daten von Bewerbern um ein Mandat im Deutschen Bundestag ermögliche es dem Wähler, sich rechtzeitig verlässlich mit den Wahlvorschlägen vertraut zu machen. Diesem Anspruch werde aber nur eine öffentliche Bekanntmachung mit Angaben zur vollen Anschrift gerecht, da sich der Wähler nur so noch vor der Wahl postalisch an den Bewerber wenden könne, um ihn zu seiner Bewerbung zu befragen. Ein Weglassen der Anschrift komme im Einzelfall dann in Betracht, wenn der Bewerber glaubhaft machen kann, dass ihm bei der Veröffentlichung seiner Anschrift konkrete Gefahren für Leben, Gesundheit oder ähnliche schutzwürdige Belange erwachsen können. Der Bundesregierung sei ein solcher Fall bisher noch nicht bekannt geworden.

Obwohl ich diese Verfahrensweise und die ihr zugrundeliegende Rechtslage nach wie vor für problematisch halte, sehe ich aufgrund der Haltung der Bundesregierung gegenwärtig keine Möglichkeit, eine Änderung zu erreichen, zumal diese nur in Abstimmung mit den Ländern möglich wäre.

5.10.2 Änderung des Bundeswahlgesetzes – Was lange währt ... –

Bereits in meinem 2. TB für das Jahr 1979 forderte ich die Abschaffung der öffentlichen Auslegung des Wählerverzeichnisses und habe dies in den folgenden Jahren, zuletzt in meinem 17. TB (Nr. 34.4), wiederholt. Dieser Forderung wurde jedoch stets entgegengehalten, die Öffentlichkeit der Wahlhandlung gebiete eine Einsichtnahme in das Wählerverzeichnis. Dieses wird bisher vom 20. bis zum 16. Tag vor der Wahl zur allgemeinen Einsicht öffentlich ausgelegt. Die darin enthaltenen, aus dem Melderegister stammenden Angaben über die Wahlberechtigten (Vor- und Familiennamen, Anschriften sowie Geburtsdaten) sind also während dieses Zeitraumes jedermann zugänglich.

Durch das vom Deutschen Bundestag am 13. Oktober 2000 verabschiedete 15. Gesetz zur Änderung des Bundeswahlgesetzes (BT-Drs. 14/3764) sollte die öffentliche Auslegung des Wählerverzeichnisses abgeschafft werden. Das Gesetz ist jedoch bis Redaktionsschluss noch nicht in Kraft getreten, weil der Bundesrat den Vermittlungsausschuss angerufen hat.

In dem Gesetzentwurf ist vorgesehen, die öffentliche Auslegung des Wählerverzeichnisses durch ein Recht auf Einsichtnahme in das Wählerverzeichnis unter bestimmten Voraussetzungen zu ersetzen. Es müssen Tatsachen glaubhaft gemacht werden, aus denen sich z. B. eine Unrichtigkeit des Wählerverzeichnisses ergibt. Das Recht auf Einsichtnahme erstreckt sich dabei aber nicht auf die Daten, für die im Melderegister ein Sperrvermerk eingetragen ist. Durch diese Regelung würden endlich Wahl- und Melderecht harmonisiert, denn bislang kann die melderechtliche Auskunftssperre durch Einsichtnahme in das Wählerverzeichnis umgangen werden.

Eine weitere vorgesehene Änderung des Bundeswahlgesetzes soll die Gewinnung von Wahlhelfern erleichtern. Die Gemeindebehörden wären dann befugt, personenbezogene Daten von Wahlberechtigten zum Zweck ihrer Berufung zu Mitgliedern von Wahlvorständen zu erheben und zu verarbeiten. Dies wäre auch für künftige Wahlen zulässig, d. h., die Daten würden auf Dauer in einer Wahlhelferdatei gespeichert. Der Betroffene könnte dieser Verarbeitung aber widersprechen, und wäre deshalb über sein Widerspruchsrecht zu unterrichten. Ferner sieht das Gesetz vor, dass sich die Gemeindebehörden zur Gewinnung von Wahlhelfern insbesondere an die Behörden des Bundes und der Länder wenden können, die auf ein entsprechendes Ersuchen verpflichtet wären, aus dem Kreis ihrer Bediensteten Personen zu benennen, die im Gebiet der ersuchenden Gemeinden wohnen.

6 Rechtswesen

6.1 Berichtspflicht der Bundesregierung über die akustische Wohnraumüberwachung

Die Einführung der akustischen Wohnraumüberwachung für Strafverfolgungszwecke im Jahre 1998 hatte eine starke innenpolitische Debatte ausgelöst, bei der sich Befürworter und Gegner einen heftigen Schlagabtausch lieferten, ehe letztlich der „Große Lauschangriff“ durch eine Änderung des Grundrechts auf Unverletzlichkeit der Wohnung in Art. 13 GG Gesetzeskraft erlangte.

Gemäß Art. 13 Abs. 6 GG wurde die Bundesregierung verpflichtet, den Deutschen Bundestag jährlich über die akustischen Wohnraumüberwachungen zu unterrichten, die für Zwecke der Strafverfolgung durchgeführt wurden. § 100e StPO konkretisiert diese Berichtspflicht dahingehend, dass die Unterrichtung aufgrund von Mitteilungen der Staatsanwaltschaften der Länder über Anlass, Umfang, Dauer, Ergebnis und Kosten der Maßnahmen zu erfolgen hat. Der Deutsche Bundestag, der zu diesem Zweck ein Gremium nach Art. 13 Abs. 6 GG gewählt hat, soll aufgrund der Berichte in die Lage versetzt werden, die Angemessenheit und Eignung der Maßnahme zu überprüfen und somit eine laufende parlamentarische Kontrolle dieser mit intensiven Grundrechtseingriffen verbundenen Maßnahmen gewährleisten. Diese Berichtspflicht habe ich seinerzeit als wirksames Instrument zur Gewährleistung der parlamentarischen Kontrolle begrüßt (vgl. 17. TB Nr. 6.1).

Der Bericht für das Jahr 1998 (BT-Drs. 14/2452) wird nicht den Anforderungen gerecht. So wird nur die Gesamtzahl der von einer Anordnung auf Wohnraumüberwachung Betroffenen erfasst, wobei zwischen beschuldigten und nicht beschuldigten Wohnungsinhabern unterschieden wird. Wesentliche Informationen, die schlüssige Aussagen zur Effizienz der Maßnahmen und zur Intensität der damit verbundenen Grundrechtseingriffe ermöglicht hätten, enthält der Bericht jedoch nicht. Insbesondere fehlen Angaben über die Anzahl aller von der Maßnahme betroffenen Personen, also auch z. B. von unverdächtigen Familienangehörigen, Bekannten oder sonstigen zufälligen Besuchern. Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb im Juni 2000 die Entschließung „Effektive parlamentarische Kontrolle von Lauschangriffen durch aussagekräftige jährliche Berichte der Bundesregierung“ verabschiedet (s. **Anlage 22**).

Inzwischen liegt auch der Bericht der Bundesregierung für das Jahr 1999 vor (BT-Drs. 14/3998). Dieser unterscheidet sich hinsichtlich der Angaben nicht vom ersten Bericht. Da er dem Deutschen Bundestag jedoch bereits mit Schreiben vom 27. Juli 2000 zugeleitet wurde, bestand wohl aufgrund des Zeitablaufs keine Möglichkeit, die Empfehlungen der Entschließung zu berücksichtigen.

Bei einem Vergleich der beiden vorliegenden Berichte fallen keine signifikanten Unterschiede auf. Bezüglich der Anzahl der Verfahren (1998: 11, 1999: 26) ist zu berücksichtigen, dass das Gesetz zur Verbesserung der Bekämpfung der Organisierten Kriminalität erst am 9. Mai 1998 in Kraft getreten ist. Die Anlasstaten verteilen sich unverändert nahezu gleichwertig auf Mord bzw. Totschlag und Betäubungsmitteldelikte. Die Anzahl der Betroffenen hat zwar überproportional zugenommen (1998: 26, 1999: 142), doch ist dies überwiegend auf drei größere Verfahren zurückzuführen. Eine Benachrichtigung der Betroffenen ist im Jahr 1998 in fast allen Fällen erfolgt (9 von 11), im Jahr 1999 wegen noch laufender Verfahren in weniger Fällen (12 von 26). Positiv entwickelt hat sich die Statistik der Relevanz der Maßnahmen für das Verfahren. Während die Relevanz im Jahr 1998 nur in 3 von 11 Verfahren vorlag, war sie im Jahr 1999 in 13 von 26 Verfahren gegeben.

Ungeachtet dieser ersten Auswertungen werde ich mich auch künftig dafür einsetzen, dass die Berichte der Bundesregierung noch geeignetere Angaben für eine parlamentarische Kontrolle enthalten.

6.2 Strafverfahrensänderungsgesetz 1999 endlich in Kraft getreten

Nahezu 17 Jahre hat es seit dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 gedauert, bis am 1. November 2000 das Strafverfahrensänderungsgesetz 1999 (StVÄG 1999) in Kraft getreten ist (BGBl. I S. 1253ff). Damit wurden endlich bereichsspezifische gesetzliche Grundlagen für die Erhebung und Verarbeitung besonders schützenswerter personenbezogener Daten im Bereich der Justiz geschaffen. Zugleich wurde ein Zustand beendet, der in den letzten Jahren allenfalls noch mit dem sog. Übergangsbonus des Bundesverfassungsgerichts gerechtfertigt werden konnte.

Das Gesetz basiert auf den Beratungen des Entwurfs eines StVÄG 1996, der in mühseligen Verhandlungen zwischen Bund und Ländern im Sommer 1998 fast konsensreif war, ehe er in letzter Minute doch noch scheiterte (s. 17. TB Nr. 6.2). In der jetzigen, der 14. Legislaturperiode, war dieser Entwurf mit kleinen Änderungen als StVÄG 1999 erneut ins parlamentarische Verfahren eingebracht worden, in dessen Beratungen die Ausschüsse des Deutschen Bundestages zahlreiche datenschutzrechtliche Verbesserungen beschlossen. Diese fanden aber leider nicht die Zustimmung des Bundesrates, der im Gegenteil die Interessen der Strafverfolgungsbehörden einseitig in den Vordergrund stellte und den Vermittlungsausschuss anrief. Die Datenschutzbeauftragten des Bundes und der Länder haben daraufhin auf ihrer 59. Konferenz eine Entschließung verabschiedet, um eine Absenkung des Datenschutzniveaus zu verhindern (s. Entschließung vom 14./15. März 2000, **Anlage 21**). Der Vermittlungsausschuss hat einen Kompromiss erarbeitet, der nun Gesetz geworden ist.

Zu den wesentlichsten Neuerungen des Gesetzes zählen detaillierte Regelungen für strafprozessuale Ermittlungsmethoden, die, wie z. B. die Öffentlichkeitsfahndung und die längerfristige Observation, einen tiefen Eingriff in das Persönlichkeitsrecht des Betroffenen darstellen. Künftig können bei Straftaten von erheblicher Bedeutung, beispielsweise bei Totschlag, sowohl der Richter als auch die Staatsanwaltschaft aufgrund eines Haftbefehls auch Öffentlichkeitsfahndungen veranlassen, wenn andere Formen der Aufenthaltsermittlung erheblich weniger Erfolg versprechend oder wesentlich erschwert wären. Unter den gleichen Voraussetzungen darf auch eine Öffentlichkeitsfahndung zur Aufenthaltsermittlung eines Beschuldigten oder eines Zeugen angeordnet werden. Damit liegt nun auch eine Regelung für eine Fahndung im Internet vor, deren sich die Strafverfolgungsbehörden in letzter Zeit zunehmend bedienen. Diese Vorschriften zur Öffentlichkeitsfahndung bergen naturgemäß das Risiko, dass

öffentlich nach einer Person als – möglichem – Straftäter gesucht wird, die sich später als unschuldig erweist. Die Verletzung des Persönlichkeitsrechts eines so Gesuchten ist nicht wieder rückgängig zu machen. Die Ausstrahlung eines Fahndungsaufrufes u. a. im Fernsehen nach einem potentiellen Straftäter erzeugt eine dauerhafte Öffentlichkeitswirkung. Insofern sind die Strafverfolgungsbehörden aufgefordert, gerade von der Öffentlichkeitsfahndung nur restriktiven Gebrauch zu machen.

Kritisch sehe ich auch die Vorschriften, die sich mit der Zulässigkeit der Verwendung von präventiv-polizeilich erhobenen Daten für den Strafprozess befassen. Der Grundgedanke, die Verwendung von solchen Daten grundsätzlich auch für die Zwecke der Strafprozessordnung zu erlauben, wird von mir im Interesse einer funktionierenden Strafverfolgung selbstverständlich akzeptiert. Jedoch wird durch die vom Vermittlungsausschuss vorgenommene Streichung eines Absatzes auch die Zweckbindung von präventiv-polizeilichen Daten aufgehoben, die durch besonders eingriffsintensive Maßnahmen gewonnen wurden. Dies bedeutet, dass z. B. Daten, die in einem Verfahren zurecht durch einen Großen Lauschangriff oder den Einsatz verdeckter Ermittler gewonnen wurden, nun auch in einem Verfahren benutzt werden können, in dem die Voraussetzungen für einen solchen Eingriff nicht vorliegen. Oder anhand eines Beispieles ausgedrückt: Daten, die bei einer akustischen Wohnraumüberwachung gewonnen wurden, dürfen jetzt auch für die Aufklärung eines Fahrraddiebstahls verwendet werden, obwohl für die Aufklärung eines Fahrraddiebstahls eine akustische Wohnraumüberwachung nicht hätte angeordnet werden dürfen. Verwendungsbeschränkungen für derart gewonnene Daten bestehen im Wesentlichen nur noch hinsichtlich solcher Informationen, die bei dem Einsatz von technischen Mitteln in Wohnungen anfallen, wenn dieser im Rahmen der Eigensicherung der handelnden Polizeibeamten erforderlich war.

Auch der umgekehrte Fall, d. h. die Verwendung von strafprozessual erhobenen Daten für präventiv-polizeiliche Zwecke, wird gesetzlich geregelt. Danach dürfen den Polizeibehörden nach Maßgabe der Polizeigesetze personenbezogene Informationen aus Strafverfahren zu den dort genannten Zwecken übermittelt werden. Eine Einschränkung ist nur dann vorgesehen, wenn die Polizei ausschließlich zum Schutz privater Rechte tätig wird. Damit hat der Vermittlungsausschuss die Befugnisse der Polizei erweitert. Der Gesetzentwurf des Deutschen Bundestages hatte eine Datenübermittlung nur zur Gefahrenabwehr zugelassen. Die von mir stets geforderte Zweckbindung der strafprozessual erhobenen Daten ist somit ausgehöhlt worden.

Das StVÄG 1999 enthält umfassende Regelungen über die Erteilung von Auskünften und Akteneinsicht aus Strafverfahren, die bislang nur in Bezug auf Verfahrensbeteiligte vorhanden waren. In einem umfangreichen Katalog ist die Zulässigkeit der Übermittlung personenbezogener Daten an öffentliche Stellen festgelegt, wohingegen das Auskunftsrecht für Privatpersonen lediglich an das Vorliegen eines berechtigten Interesses geknüpft ist. Bedauerlicherweise hat der Vermittlungsausschuss nicht die ursprünglich engere Formulierung übernommen, wonach ein rechtliches Interesse erforderlich gewesen wäre. Abschließend regelt das Gesetz auch die Akteneinsicht und die Erteilung von Auskünften an Forschungseinrichtungen.

Schließlich finden sich noch umfangreiche Vorschriften für die Verarbeitung von personenbezogenen Daten in Dateien und deren Nutzung. Diese Regelungen über Inhalt, Ausmaß und Umfang von Dateien und Informationssystemen mit personenbezogenen Daten erlauben die Einrichtung von Datensammlungen mit weitgehenden Zugriffsmöglichkeiten der Strafverfolgungsbehörden. So können Dateien für Zwecke des laufenden Strafverfahrens, künftiger Strafverfahren sowie der Vorgangsverwaltung angelegt werden; Daten können auch in gemeinsamen Dateien der entsprechenden Stellen gespeichert werden.

Zusammenfassend möchte ich jedoch festhalten, dass die Genugtuung über die Schaffung von Vorschriften zur Wahrung des Persönlichkeitsrechts im Bereich der Justiz überwiegt. Jetzt gilt es zu beobachten, wie sie sich in der Praxis bewähren.

6.3 Weitere Entwicklung der Genomanalyse im Strafverfahren – Kann die Einwilligung der Betroffenen die Prognose des Richters ersetzen? –

In meinem letzten Tätigkeitsbericht habe ich ausführlich über die neuen gesetzlichen Vorschriften für den Einsatz gentechnischer Methoden im Strafverfahren berichtet (17. TB Nr. 6.3). In § 2 DNA-Identitätsfeststellungsgesetz war u. a. geregelt worden, dass molekulargenetische Untersuchungen zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren auch bei bereits rechtskräftig Verurteilten durchgeführt werden dürfen, wenn die entsprechende Eintragung im Bundeszentralregister noch nicht getilgt ist. Es traten aber alsbald Unsicherheiten darüber auf, ob nach dieser Rechtsgrundlage Auskünfte aus dem Bundeszentralregister auch dann zulässig sind, wenn die entsprechenden Anfragen nicht auf der Angabe von konkreten Personendaten der Betroffenen beruhen, sondern eine Auswertung des Datenbestandes im Bundeszentralregister erfordern.

Den im Rahmen der parlamentarischen Beratungen daraufhin vorgelegten Gesetzentwurf der Koalitionsfraktionen habe ich nachdrücklich unterstützt, weil ich eine eindeutige Rechtsgrundlage für die Verpflichtung des Bundeszentralregisters zur Mitwirkung bei der Übermittlung der Eintragung einschlägiger Personen zu schaffen, für erforderlich gehalten habe. Das Bundeszentralregistergesetz geht von der Rechtsfigur der Individualauskunft aus und enthält keine Rechtsgrundlage für eine Auskunft über Personen, die durch die Anfrage erst ermittelt werden sollen.

Das inzwischen in Kraft getretene Gesetz zur Änderung des DNA-Identitätsfeststellungsgesetzes vom 2. Juni 1999 (BGBl. I S. 1242) ist diesem Petitum gerecht geworden. Es enthält daneben erfreulicherweise eine Vorschrift hinsichtlich der präventiven Speicherung von verfahrensbezogenen DNA-Identifizierungsmustern.

Dadurch wurde im wesentlichen meiner ursprünglichen Forderung nach Schaffung einer gesetzlichen Grundlage für die Speicherung der Daten, die gemäß § 81e StPO erhoben und bislang auf der unzureichenden Grundlage des § 8 Abs. 6 BKAG in der DNA-Analsye-Datei des Bundeskriminalamtes gespeichert wurden, entsprochen (vgl. 17. TB Nr. 6.3). Leider enthält diese Regelung aber keine ausdrückliche Verweisung auf den Richtervorbehalt in § 81g Abs. 3 StPO. Dies erfolgte laut Gesetzesbegründung bewusst, da der Richtervorbehalt für Anordnungen nach § 81e StPO gemäß § 81f StPO bereits ohnehin gelte. Diese Argumentation halte ich jedoch nur zum Teil für zutreffend. Denn der Richter entscheidet im Rahmen seiner Anordnung nach §§ 81e, f StPO nur über die rein verfahrensbezogene Erforderlichkeit einer DNA-Analyse zum Zwecke der Zuordnung des Spurenmaterials (bzw. der Feststellung der Abstammung). Er entscheidet jedoch nicht über die DNA-Identitätsfeststellung i. S. des § 81g StPO. Damit entscheidet er auch nicht über das Vorliegen einer Straftat von erheblicher Bedeutung und einer besonderen Wiederholungsgefahr. Somit liegt ein Wertungswiderspruch zu der Intention des DNA-Identitätsfeststellungsgesetzes vor, da der Richtervorbehalt in § 81g Abs. 3 StPO auch gewährleisten soll, dass die Gefahrenprognose durch den Richter getroffen wird. Der Verzicht auf die durch einen Richter zu treffende Gefahrenprognose führt leider dazu, dass die Anordnung einer DNA-Analyse im laufenden Verfahren automatisch die Speicherung dieser Daten in der DNA-Analyse-Datei nach sich zieht.

Im Rahmen des Einsatzes der DNA-Analyse für Fälle künftiger Strafverfolgung sind Strafverfolgungsbehörden in einigen Bundesländern dazu übergegangen, bei Strafgefangenen eine DNA-Analyse allein auf die Einwilligung der Betroffenen zu stützen, anstatt eine richterliche Anordnung einzuholen. Diese Praxis verstößt nach meiner Auffassung gegen geltendes Recht. Denn gem. § 81g i. V. m. § 81f StPO erfolgt eine Untersuchung zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren auf Anordnung des Richters. Dieser entscheidet auf der Grundlage der von ihm zu treffenden Prognose. § 81g Abs. 1 StPO setzt dabei die Erwartung voraus, dass wegen Art oder Ausführung der Tat, der Persönlichkeit des Beschuldigten oder sonstigen Erkenntnissen Grund zu der Annahme besteht, dass gegen ihn künftig erneut Strafverfahren wegen bestimmter Straftaten zu führen sind. An dieser Prognoseentscheidung würde es aber fehlen, wenn die molekulargenetische Untersuchung aufgrund einer Einwilligung eines Betroffenen zulässig wäre. Eine solche Praxis würde die gesetzlich vorgesehenen Schutzmechanismen beseitigen und damit zu einer erheblichen Schlechterstellung derjenigen Personen führen, die „freiwillig“ eine Speichelprobe abgeben. Hinzu kommt, dass von einer echten Freiwilligkeit kaum die Rede sein kann, da Strafgefangene annehmen können, dass die Verweigerung der Einwilligung Auswirkungen etwa auf die Gewährung von Vollzugslockerungen hat; maßgebend ist hier die subjektive Einschätzung des Betroffenen.

Die Datenschutzbeauftragten des Bundes und der Länder haben diese Thematik in ihrer 58. Konferenz aufgegriffen und gefordert, DNA-Analysen zum Zwecke der Identitätsfeststellung für künftige Strafverfahren nur noch auf der Grundlage richterlicher Anordnungen durchzuführen (s. Entschließung vom 7./8. Oktober 1999, **Anlage 25**).

6.4 Zugriff der Strafverfolgungsbehörden auf Telekommunikationsdaten

6.4.1 Erneute Verlängerung der Geltungsdauer des § 12 FAG

In meinem letzten Tätigkeitsbericht habe ich über die Bemühungen des Gesetzgebers berichtet, eine Nachfolgeregelung für § 12 Fernmeldeanlagengesetz (FAG) zu verabschieden (s. 17. TB Nr. 6.4). Nach dieser Vorschrift können Richter und bei Gefahr im Verzuge auch die Staatsanwaltschaft in strafgerichtlichen Verfahren von Telekommunikationsunternehmen Auskunft darüber verlangen, wer wann mit wem wie lange kommuniziert hat. Es handelt sich dabei um die sog. Verbindungsdaten, also nicht um die Überwachung der Gesprächsinhalte. Die parlamentarischen Beratungen hierzu führten jedoch nur zu dem Ergebnis, die Geltungsdauer der bisherigen Norm bis zum 31. Dezember 1999 zu verlängern.

Nachdem in dieser Legislaturperiode der Bundesrat die zeitliche Befristung aufheben wollte, womit es bei dem verfassungsrechtlich bedenklichen Rechtszustand geblieben wäre, haben sich die Datenschutzbeauftragten des Bundes und der Länder im Rahmen ihrer 58. Konferenz mit dieser Thematik befasst. In einer Entschließung fordern sie eine Neufassung der Vorschrift unter Beachtung der Anforderungen, die sich aus dem von Art. 10 GG geschützten Telekommunikationsgeheimnis ergeben (s. Entschließung vom 7./8. Oktober 1999, **Anlage 14**).

Der Gesetzgeber hat jedoch die Geltungsdauer des § 12 FAG erneut um zwei weitere Jahre verlängert, also bis zum 31. Dezember 2001 (BGBl. I S. 2492). Erfreulicherweise wurden aber durch eine Verweisung auf die Vorschriften der §§ 100b Abs. 6 und 101 Abs. 1 Satz 1 StPO zwei datenschutzrechtliche Verbesserungen eingefügt, die meinen langjährigen Forderungen entsprechen. Aufgrund dieser Verweisungen müssen nämlich zum einen künftig Unterlagen, die zur Strafverfolgung nicht mehr erforderlich sind, unverzüglich vernichtet werden. Zum anderen müssen Beteiligte der Maßnahmen nach § 12 FAG benachrichtigt werden, sofern nicht bestimmte Ausnahmetatbestände, z. B. Störung des Ermittlungsverfahrens, vorliegen.

Diese Ergänzungen des § 12 FAG begrüße ich nachdrücklich. Sie stellen einen wichtigen Schritt in die richtige Richtung dar. Damit entspricht diese Vorschrift

deutlich mehr dem heutigen verfassungsgerichtlichen Verständnis von Wert und Bedeutung des Fernmeldegeheimnisses.

Ich appelliere allerdings weiter an den Gesetzgeber, möglichst rasch § 12 FAG neu zu gestalten und in die Strafprozessordnung einzugliedern. Dabei sollte ein Katalog der Straftaten entwickelt werden, bei denen die Verbindungsdaten für die Verfolgung von Straftaten mitgeteilt werden dürfen. Wichtig ist auch, eine Schutzklausel für Telefonate von Personen zu schaffen, die zur Wahrung von Berufsgeheimnissen verpflichtet sind, wie z. B. Priester, Ärzte, Rechtsanwälte oder Journalisten. Der vom Gesetzgeber durch die bestehenden Zeugnisverweigerungsrechte anerkannte Schutz des Vertrauensverhältnisses zwischen bestimmten Berufsangehörigen und Dritten, die deren Hilfe und Sachkunde in Anspruch nehmen, muss auch im Zeitalter moderner Telekommunikation gewahrt bleiben.

6.4.2 Erneut alarmierender Anstieg der Telefonüberwachung!

In den letzten Jahren ist die Zahl der nach der Strafprozessordnung angeordneten Telefonüberwachungen ständig angestiegen. Mit Zahlen lässt sich dies wie folgt belegen: In 1995 wurden 4 674, in 1996 bereits 6 428, in 1997 dann 7 776 und in 1998 insgesamt 9 802 Anordnungen erlassen. Im Jahr 1999 schließlich wurden 12 651 Anordnungen vorgelegt. Das bedeutet auf das Jahr 1995 bezogen eine Steigerung um fast 175 %, allein für das Jahr 1999 immerhin eine Steigerung um fast 30 %. Angesichts dieser sehr hohen Zahl von Eingriffen in einen besonders sensiblen Bereich, nämlich den der Vertraulichkeit des gesprochenen Wortes, muss Klarheit über die Gründe für diesen großen Anstieg geschaffen werden.

Diesen Anstieg von Eingriffen in das Fernmeldegeheimnis beobachte ich mit großer Sorge. Seit Jahren appelliere ich an die Strafverfolgungsbehörden, dieses Mittel sparsam einzusetzen; zugleich fordere ich vertrauensbildende Maßnahmen.

Der Katalog der Straftaten, die eine Telefonüberwachung nach der Strafprozessordnung erlauben, ist in der Vergangenheit mehrfach erweitert worden. Wenn dies auch für eine wirksame Verbrechensbekämpfung notwendig sein mag, so ist es aber erforderlich, den tatsächlichen Erfolg zu prüfen und das Persönlichkeitsrecht im Ausgleich hierfür zu stärken. Nach der Rechtsprechung des Bundesverfassungsgerichts bedarf es einer gründlichen Bestandsaufnahme und Evaluierung des strafprozessualen und polizeirechtlichen Instrumentariums, um einerseits wegen der gebotenen Effizienz und andererseits wegen der Einschränkung von Grundrechten Verdächtiger und erst recht Unbeteiligter das richtige Maß zu finden. Eingriffsbefugnisse müssen deshalb nach ihrer Einführung und Anwendung hinsichtlich ihrer Wirkungen bewertet werden können, um sowohl ein Unter- als auch ein Übermaß zu vermeiden. Der Bürger muss nachvollziehen können, weshalb solche Eingriffe in seine Freiheit auch in einem Rechtsstaat gerechtfertigt sind.

Ich habe in der Diskussion um derartige besonders einschneidenden strafprozessualen Ermittlungsbefugnisse mehrfach neue, vertrauensbildende Maßnahmen für eine Stärkung des Persönlichkeitsrechts gefordert (s. 17. TB Nr. 1.5). Solche vertrauensbildenden Maßnahmen könnten sein:

- Jährliche Berichterstattung an den Deutschen Bundestag über Anlass, Verlauf, Ergebnis, Anzahl der Betroffenen und Kosten der Telefonüberwachung.
- Verbesserung des Verfahrens der richterlichen Anordnung, z. B. indem die Zustimmung zur Überwachungsmaßnahme umfassend zu begründen ist, und bestimmte Richter über den Überwachungsantrag entscheiden, um die Verantwortung bis zur Beendigung der Maßnahme an diese Richter zu binden.
- Einführung interner Erfolgskontrollen um festzustellen, ob die Telefonüberwachung wirklich nur als „ultima ratio“, also als letztes mögliches Mittel, eingesetzt und nicht bereits als eine bequeme Standardmaßnahme in etwas komplexeren Ermittlungsverfahren angesehen wird.
- Berücksichtigung von Zeugnisverweigerungsrechten, d. h., es sollten abgestufte Erhebungs- und Verwertungsverbote von Gesprächsinhalten geschaffen werden, wenn durch Überwachungsmaßnahmen Gespräche von nicht tatverdächtigen Personen, denen ein Zeugnisverweigerungsrecht zusteht (wie z. B. Ärzten oder Geistlichen) aufgenommen wurden.

Für die Fälle der akustischen Wohnraumüberwachung hat der Gesetzgeber erfreulicherweise Berichtspflichten der Staatsanwaltschaft gegenüber der obersten Justizbehörde und der Bundesregierung gegenüber dem Deutschen Bundestag auferlegt, die sogar im Grundgesetz verankert worden sind (s. o. Nr. 6.1). Entsprechende Berichtspflichten halte ich auch für den Bereich der Telefonüberwachung für unabdingbar. Es reicht einfach nicht aus, immer nur auf die wachsende Bedrohung durch die Kriminalität hinzuweisen und die Telefonüberwachung als besonders wichtiges Hilfsmittel im Kampf gegen Kriminalität darzustellen. Ich zweifle deren Notwendigkeit nicht an, der Gesetzgeber sollte aber darüber informiert sein, wie sie in der Praxis wirkt, welche Erfolge sie gebracht hat und was mit den nicht mehr für das laufende Ermittlungsverfahren benötigten Daten passiert. Bei einer umfassenden und fairen Erfolgskontrolle kann es letztlich nur Gewinner geben, da sie auf das von allen Beteiligten gleichermaßen akzeptierte Ziel eines Freiheit und Sicherheit garantierenden Rechtsstaates gerichtet ist (vgl. u. Nr. 16.1.2 zu G10-Maßnahmen).

Auch die Bundesregierung sieht ein Hauptaugenmerk in der Frage, inwieweit Telefonüberwachungsmaßnahmen wirklich zum Erfolg der staatlichen Strafverfolgung geführt haben. Hierzu wird auch das Ergebnis der vom BMJ in Auftrag gegebenen Studie zur Frage der Rechtswirklichkeit und Effizienz von Telefonüberwachungen beitragen (s. u. Nr. 11.8). Ohne diesem Ergebnis vorgreifen zu wollen, sollte ein sich gegebenenfalls zeigender Hand-

lungsbedarf zügig umgesetzt werden. Ich hoffe gerade in diesem empfindlichen Bereich auf Unterstützung meiner Vorschläge durch den Deutschen Bundestag.

6.5 Gesetz zum Täter-Opfer-Ausgleich verabschiedet

Am 28. Dezember 1999 ist das Gesetz zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs in Kraft getreten (BGBl. I S. 2491 f). Damit gibt es erstmals eine gesetzliche Grundlage für die Übermittlung der notwendigen Daten der Betroffenen durch die Justizbehörden an die staatlichen und privaten Stellen, denen die schwierige Aufgabe des Täter-Opfer-Ausgleichs übertragen bzw. denen die Wahrnehmung dieser Aufgaben ermöglicht werden soll. Bereits im Jahre 1994 wurde mit § 46a StGB die materiell-rechtliche Grundlage dafür geschaffen, das Instrument des Täter-Opfer-Ausgleichs bei der Strafzumessung zu berücksichtigen, was zu einer Strafmilderung oder zum Absehen von Strafe führen kann. Allerdings haben die letzten Jahre gezeigt, dass nur in einem kleinen Teil aller Strafverfahren dieser Ausgleich mit dem Verletzten praktiziert wurde, weil die Durchführung des Verfahrens in der Praxis zu erheblichen Schwierigkeiten führte.

Das neue Gesetz bildet das strafverfahrensrechtliche Äquivalent zur Regelung im Strafgesetzbuch. Zentraler datenschutzrechtlicher Punkt im Gesetzgebungsverfahren war die Frage, inwieweit die Weitergabe von personenbezogenen Daten des Opfers zwischen den beteiligten Stellen von seiner Einwilligung abhängen muss. Denn die Achtung und wirksame Unterstützung des Opfers müssen ein wesentliches Anliegen eines jeden Strafverfahrens sein. Dem wird in den Fällen des Täter-Opfer-Ausgleichs aber nur dann ausreichend Rechnung getragen, wenn der Wille des Opfers respektiert wird. Nachdem der Bundesrat in seiner Stellungnahme die Auffassung vertreten hatte, dass es für solche Datenübermittlungen auf den Willen des Opfers überhaupt nicht ankommen soll, haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer 58. Konferenz gefordert, dass eine Einwilligung des Opfers Voraussetzung einer Datenübermittlung sein muss (s. Entschließung vom 7./8. Oktober 1999, **Anlage 15**). Der Gesetzgeber ist dieser Empfehlung leider insoweit nicht gefolgt, als das Gesetz eine Einwilligung des Opfers nicht ausdrücklich vorschreibt. Statt dessen heißt es: „...Gegen den ausdrücklichen Willen des Verletzten darf die Eignung (gemeint ist der Ausgleich zwischen Beschuldigtem und Verletztem) nicht angenommen werden." Es wird also lediglich der „ausdrückliche Wille" des Opfers angesprochen. Aus meiner Sicht besagt die Formulierung aber dennoch unmissverständlich, dass gegen den ausdrücklichen Willen des Opfers der Ausgleich nicht durchgeführt werden darf und deshalb davon auszugehen ist, dass in der Praxis die zuständigen Behörden zunächst einmal den Willen des Opfers in Erfahrung bringen werden. Eine andere Vorgehensweise würde das Ziel des Gesetzgebers unterlaufen. Das Opfer kann sich also frei entscheiden, ob es einer Datenübermittlung zustimmt oder nicht. Im Ergebnis begrüße ich somit das Gesetz und gehe davon aus, dass der Täter-Opfer-Ausgleich im Rahmen der Strafverfolgung zukünftig eine gewichtigere Rolle einnimmt.

6.6 Gesetzentwurf über den Vollzug der Untersuchungshaft

In meinem letzten Tätigkeitsbericht (17. TB Nr. 6.6.2) habe ich über die Bemühungen des BMJ berichtet, eine gesetzliche Regelung für den Vollzug der Untersuchungshaft zu erarbeiten. Inzwischen liegt ein Gesetzentwurf der Bundesregierung vor, der meiner seit langem erhobenen Forderung nach einer bereichsspezifischen Regelung Rechnung trägt. Dieser Gesetzentwurf enthält eine weitgehend angemessene Abwägung zwischen dem Strafverfolgungs- und dem Sicherheitsinteresse des Staates im Rahmen des gesetzlichen Zwecks der Untersuchungshaft einerseits und dem Persönlichkeitsrecht der Untersuchungsgefangenen andererseits. Nachdem der Bundesrat im Laufe des parlamentarischen Verfahrens einseitig das staatliche Vollzugsinteresse in den Vordergrund gestellt hat, haben die Datenschutzbeauftragten des Bundes und der Länder im Rahmen einer Entschließung ihre Empfehlungen formuliert, um datenschutzrechtliche Verschlechterungen zu vermeiden (s. Entschließung vom 16. August 1999, **Anlage 12).**

Hervorzuheben sind insbesondere die Überwachung der Außenkontakte von Untersuchungsgefangenen, wo beim Gesetzentwurf hinsichtlich der Überwachung der Unterhaltung mit Besuchern und der Kontrolle von Schriftstücken sachgerecht nach Haftgründen differenziert wird, während der Bundesrat von einer solchen Überwachung nur ausnahmsweise nach dem Ermessen des Gerichts absehen will. Weiterhin gewährleistet der Gesetzentwurf ein Recht auf ungehinderten und unüberwachten telefonischen Kontakt zwischen Verteidiger und Untersuchungsgefangenem, während der Bundesrat diesen Kontakt von der Erlaubnis des Gerichts abhängig machen will. Bei den künftigen parlamentarischen Beratungen werde ich mich dafür einsetzen, dass die Vorschriften des Gesetzentwurfs der Bundesregierung weiterhin den datenschutzrechtlichen Standard bilden.

6.7 Ausdehnung des Zeugnisverweigerungsrechts von Medienmitarbeitern

Die Bundesregierung hat einen Gesetzentwurf vorgelegt, der eine Erweiterung des strafprozessualen Zeugnisverweigerungsrechts für Presse- und Rundfunkangehörige beabsichtigt (BR-Drs. 441/00). Zweck der bestehenden Zeugnisverweigerungsrechte nach § 53 StPO ist der Schutz des Vertrauensverhältnisses zwischen bestimmten Berufsangehörigen und den Personen, die deren Hilfe und Sachkunde in Anspruch nehmen. In engem, untrennbarem Zusammenhang hierzu stehen die Regelungen über das Beschlagnahmeverbot in § 97 StPO, das an das Zeugnisverweigerungsrecht anknüpft und seine Umgehung verhindern soll. Der Schutz dieses Vertrauensverhältnisses dient der im öffentlichen Interesse liegenden Tätigkeit von Presse und Rundfunk, die jedoch ihrerseits in

Einklang mit einer effektiven Strafverfolgung zu bringen ist.

Die Aufklärung schwerer Straftaten ist nach der Rechtsprechung des Bundesverfassungsgerichtes ein wesentlicher Auftrag des rechtsstaatlichen Gemeinwesens. Zeugnisverweigerungsrechte und Beschlagnahmeverbote sind dabei Ausnahmen von der Pflicht zur umfassenden Aufklärung der materiellen Wahrheit und bergen demzufolge das Risiko in sich, dass die Gerichte ihre Entscheidungen auf nicht vollständiger Tatsachengrundlage treffen.

Darüber hinaus geht es um die Freiheit des Betroffenen, ein Vertrauensverhältnis unter Offenbarung seiner personenbezogenen Daten in Anspruch nehmen zu können, ohne befürchten zu müssen, dass die Person, der er sich anvertraut, einem prozessualen Zwang zur Preisgabe seiner personenbezogenen Daten unterliegt. Mit Blick auf das Persönlichkeitsrecht des betroffenen Medienmitarbeiters geht es um dessen Dispositionsrecht zur Bewältigung einer Konfliktsituation, nämlich um die Gewährleistung der individuellen Entscheidungsfreiheit im Einzelfall zwischen Preisgabe und Zurückhaltung der Information anstelle der Durchsetzung des staatlichen Anspruches.

In diesem Spannungsverhältnis hat der Gesetzgeber mit der bisherigen Regelung über das Zeugnisverweigerungsrecht in § 53 Abs. 1 Nr. 5 StPO die aus der Sicht des Datenschutzes für den notwendigen Interessenausgleich grundlegende Entscheidung getroffen. Journalistisches Wissen speichert sich aber nicht nur als Gedächtnisleistung in den Köpfen von Journalisten, sondern auch ganz herkömmlich in Schränken und Redaktionsarchiven. Eine zentrale datenschutzrechtliche Frage ist deshalb, ob die Regelungen über Zeugnisverweigerungsrechte einerseits und Beschlagnahmeverbote und Zugriffsrechte andererseits in ihrem Verhältnis zueinander stimmig sind, mit anderen Worten, ob diese Eingriffsrechte der grundlegenden Wertentscheidung des Zeugnisverweigerungsrechtes folgen.

Vor diesem Hintergrund ist zunächst die im Gesetzentwurf vorgesehene Ausdehnung des Zeugnisverweigerungsrechts auf selbsterarbeitete Materialien sowie über berufsbezogene Wahrnehmungen zu bewerten. Dadurch wird der eigentliche Schutzzweck der Zeugnisverweigerungsrechte, also der Schutz des Vertrauensverhältnisses, zwar nicht unmittelbar tangiert, weil es keinen zu schützenden Informanten gibt, aber es wird erstmals ein Sonderrecht für einen Berufsstand geschaffen, dessen ungehinderte Betätigung für die freie politische Willensbildung und damit für einen demokratischen Staat insgesamt herausragende Bedeutung hat. In der Praxis der Medienarbeit ist es aber nicht möglich, immer eine deutliche Trennung vorzunehmen zwischen solchen Informationen, die von Informanten stammen, und solchen, die aufgrund eigener Recherche ermittelt worden sind. Diese Gemengelage kann dazu führen, dass durch eine Zeugenaussage bzw. eine Beschlagnahme von selbsterarbeitetem Material auch Informationen über den Informanten und dessen Angaben preisgegeben werden und damit doch der Schutzzweck der Vorschriften verletzt wird. Insofern begrüße ich die vorgesehene Erweiterung, auch wenn sie einen gewissen Bruch im bisherigen System der Zeugnisverweigerungsrechte darstellt.

Dieses Recht zur Zeugnisverweigerung entfällt dem Entwurf zufolge jedoch dann, wenn die Aussage zur Aufklärung eines Verbrechens beitragen soll, und zwar unabhängig davon, ob gegen eine bestimmte Person ein dringender Tatverdacht besteht. Diese Abwägung halte ich unter datenschutzrechtlichen Gesichtspunkten für unbedenklich. Ob sie rechtspolitisch sinnvoll ist, weil dadurch der Aushebelung des Zeugnisverweigerungsrechts Tür und Tor geöffnet wird, ist aber eine andere Frage. Ich verweise in diesem Zusammenhang darauf, dass in Ermittlungsverfahren oft am Anfang schwerwiegende Vorwürfe erhoben werden, die sich erst im Zuge der weiteren Untersuchungen als deutlich geringfügiger erweisen (z. B. Anfangsverdacht ist Mordversuch, Anklage wird wegen Widerstandes gegen die Staatsgewalt erhoben).

Bedenken habe ich aber gegen die vorgesehene Übertragung dieser Regelungen auf das Beschlagnahmeverbot. Gemäß § 97 Abs. 2 Satz 3 StPO führen nämlich der Teilnahmeverdacht und der Verdacht der Begünstigung, Strafvereitelung und Hehlerei zur Aufhebung des Beschlagnahmeverbotes. Dabei wird in der Praxis nicht vorausgesetzt, dass gegen den Zeugnisverweigerungsberechtigten schon ein Ermittlungsverfahren eingeleitet worden ist oder dass seiner Einleitung keine rechtlichen Hindernisse entgegenstehen. Auch ist nicht erforderlich, dass es sich um einen dringenden (wie z. B. beim Erlass eines Haftbefehls) oder um einen hinreichenden Tatverdacht (wie z. B. bei der Eröffnung des Hauptverfahrens) handelt. Ich werde deshalb darauf hinwirken, die Schwelle des Teilnahmeverdachtes auf „dringenden Tatverdacht“ heraufzusetzen, da es hier – anders als in den Fällen des Zeugnisverweigerungsrechts – um konkrete Verfahren geht, in denen der Journalist selbst einer Straftat verdächtig ist. Nur damit lässt sich eine Umgehung des Beschlagnahmeverbotes verhindern.

6.8 Elektronische Fußfessel – Fluch oder Segen für Gefangene?

Im Berichtszeitraum wurde in der Öffentlichkeit oft über die Einführung der „Elektronischen Fußfessel“, genau genommen des sog. elektronisch überwachten Hausarrestes berichtet. Dabei wurden unterschiedliche Modelle und Varianten dargestellt sowie verschiedene Positionen vertreten. Die Gegner kritisierten insbesondere, dass der elektronisch überwachte Hausarrest den Menschen zum Objekt des technischen Überwachungsapparates degradiere.

Im parlamentarischen Gesetzgebungsverfahren befindet sich bislang nur ein Entwurf des Bundesrates (BT-Drs. 14/1519), der durch eine Änderung des Strafvollzugsgesetzes den Ländern befristet die Möglichkeit einräumt, Regelungen für die Einführung und Ausgestaltung eines elektronisch überwachten Hausarrestes zu schaffen. Damit soll erprobt werden, ob der elektronisch überwachte

Hausarrest ein brauchbares Instrument ist, das in geeigneten Fällen und Fallgruppen an die Stelle der stationären Unterbringung in einer Justizvollzugsanstalt treten kann.

Voraussetzung für eine solche Unterbringung ist, dass

- der Gefangene nicht mehr als voraussichtlich sechs Monate einer Freiheitsstrafe oder Restfreiheitsstrafe zu verbüßen hat,
- der Gefangene den besonderen Anforderungen des elektronisch überwachten Hausarrestes genügt und
- nicht zu befürchten ist, dass der Gefangene sich dem Vollzug des Hausarrestes entziehen oder den Hausarrest zu Straftaten missbrauchen wird.

Die Unterbringung im elektronisch überwachten Hausarrest erfordert ferner die schriftliche Einwilligung des Gefangenen sowie sämtlicher im Haushalt lebenden erwachsenen Personen.

Die Überwachung selbst setzt als unabdingbare Voraussetzung einen funktionierenden Telefonanschluß des Gefangenen voraus. Es stehen zwei verschiedene technische Systeme zur Verfügung, das sog. Aktivsystem und das sog. Passivsystem, wobei der Gesetzentwurf nicht vorschreibt, welches System eingesetzt werden soll. Das Aktivsystem besteht aus einem Sender, der am Körper des Gefangenen (z. B. Fußgelenk) getragen wird, einem am Telefon installierten Empfänger und einem hiermit verbundenen Computer in einer Überwachungszentrale. Der Sender übermittelt chiffrierte Signale an den Empfänger, die über den Telefonanschluss an den Computer weitergeleitet werden. Entfernt sich der Gefangene aus dem Umfeld des Empfängers (der Bewegungsradius beträgt ca. 50 m) oder entfernt er den Sender, so wird das Übertragungssignal unterbrochen und ein Alarm ausgelöst. Der Computer lässt sich so programmieren, dass nur bestimmte Zeiten kontrolliert werden. Das Passivsystem besteht aus einem Codeleser, der fest mit dem Gefangenen verbunden ist, einem an das Telefon angeschlossenen Bestätiger und einem hiermit verbundenen Computer. Der Computer wählt nach einem bestimmten Programm den Telefonanschluss an und der Gefangene bestätigt seine Anwesenheit, in dem er den Codeleser in die Bestätigungsbox einführt. Das Passivsystem ist im Vergleich zum Aktivsystem unkomplizierter, zuverlässiger und kostengünstiger, lässt aber keine permanente Kontrolle zu.

Der elektronisch überwachte Hausarrest stellt einen tiefgreifenden Eingriff in das Recht des Betroffenen auf informationelle Selbstbestimmung dar. Eine solche Maßnahme fordert eine bereichsspezifische und normenklare Regelung, insbesondere wenn die Maßnahme über den zeitlich befristeten Modellversuch hinausgehen soll. Es sprechen jedoch aus datenschutzrechtlicher Sicht keine grundsätzlichen Bedenken gegen die probeweise Einführung des elektronisch überwachten Hausarrestes, vielmehr ist die konkrete Ausgestaltung des Verfahrens entscheidend. Ich teile auch nicht die Auffassung, der elektronisch überwachte Hausarrest widerspreche dem Menschenbild des Art. 1 GG, weil der Mensch zum Objekt des technischen Überwachungsapparates degradiert werde. Zwar ist sicherlich zutreffend, dass bei den Gefangenen eine durchgehende Überwachung gewährleistet werden muss, schon allein um eine Akzeptanz dieser Maßnahme in der Öffentlichkeit zu erreichen; der Gefangene muss wissen, dass er permanent kontrolliert und dass bei Verstößen eine sofortige Reaktion erfolgen wird. Der elektronisch überwachte Hausarrest soll aber eine gesonderte Unterbringungsform neben dem geschlossenen und dem offenen Vollzug sein. Aus diesem Grund ist die Situation des Gefangenen, der sich im elektronisch überwachten Hausarrest befindet, mit der Situation des Gefangenen in einer Justizvollzugsanstalt zu vergleichen, der ebenfalls permanent überwacht wird. Auch dieser hat keine Freiräume, in denen er sich der Kontrolle der Anstalt entziehen kann. Auch er muss jederzeit damit rechnen, dass seine momentane Beschäftigung kontrolliert wird. Es ist deshalb hervorzuheben, dass der elektronisch überwachte Hausarrest keine Alternative zur Freiheit, sondern zum Vollzug der Freiheitsstrafe in einer Haftanstalt darstellt.

Problematischer erscheint die Frage der Datenerhebung: Durch den elektronisch überwachten Hausarrest werden Daten über den Gefangenen aus dessen Wohnung und aus seinem sonstigen Umfeld erhoben. Hier dürfen nicht mehr Daten erhoben und verarbeitet werden als unbedingt erforderlich. Eine gesetzliche Grundlage für die Erhebung oder gar Speicherung dieser Daten ist ebenso notwendig wie Regelungen für die Löschung der Daten nach Ablauf einer bestimmten Frist.

Eine entscheidende Frage ist ferner, von welchen Personen eine Einwilligung einzuholen ist. Der Gesetzentwurf schreibt die Einwilligung *„sämtlicher im Haushalt lebenden erwachsenen Personen“* vor. Dies erscheint ebenso wie die Altersgrenze sachgerecht, da durch die Kontrollmaßnahmen auch die Rechtspositionen dieses Personenkreises beeinträchtigt werden können. Allerdings sollte vor dem Hintergrund, dass durch den elektronisch überwachten Hausarrest das Beschäftigungsverhältnis des Gefangenen bewahrt bleiben soll, auch überlegt werden, die Einwilligung des Arbeitgebers einzuholen. Dies gilt um so mehr, als auch Kontrollmaßnahmen am Arbeitsplatz durchzuführen sind. Jedoch sollte die Zustimmung des Arbeitgebers nur mit Einwilligung des Gefangenen eingeholt werden.

Aus datenschutzrechtlicher Sicht bestehen also keine durchgreifenden Bedenken gegen den Gesetzentwurf des Bundesrates. In den parlamentarischen Beratungen des Deutschen Bundestages werde ich mich dafür einsetzen, eine die Persönlichkeitsrechte aller Betroffenen wahrende Regelung zu erreichen.

6.9 Internationale Rechtshilfe in Strafsachen

In meinem 17. TB (Nr. 6.10) habe ich ausführlich über den „Entwurf eines Übereinkommens über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union“ berichtet, der dem Ziel der Verbesserung der justitiellen Zusammenarbeit in Strafsachen dient. Das

Übereinkommen wurde am 29. Mai 2000 von den Vertretern der Regierungen der EU-Mitgliedstaaten gezeichnet; vor einer Umsetzung ist noch der erläuternde Bericht zu dem Übereinkommen anzunehmen, der zur Zeit auf Fachebene beraten wird.

Anlässlich der Beratungen des Übereinkommensentwurfs habe ich Wert darauf gelegt, dass Gewährleistungen des Persönlichkeitsrechts im deutschen Strafverfahrensrecht nicht aufgegeben werden. Dies gilt insbesondere für den sensiblen Bereich der Überwachung von Telekommunikation. Das Übereinkommen sieht vor, dass zum Zwecke einer strafrechtlichen Ermittlung eine zuständige Behörde in einem Mitgliedstaat ein Ersuchen an die zuständige Behörde eines anderen Mitgliedstaats um Überwachung des Telekommunikationsverkehrs richten kann. Dabei kann es sich um die Bitte nach technischer Hilfe handeln, es kann jedoch auch, wenn sich die Zielperson im ersuchten Mitgliedstaat aufhält, um die eigenständige Überwachung der Telekommunikation und die Weiterleitung der Aufnahmen ersucht werden. In solchen Fällen ist der ersuchte Staat verpflichtet, dem Ersuchen nachzukommen, wenn er bestimmte Informationen erhalten hat und dem Ersuchen dann stattgeben würde, wenn es von einer seiner nationalen Behörden gestellt worden wäre. Die zuständige Behörde, die diese Prüfung vorzunehmen hat, ist in Deutschland in der Regel die Staatsanwaltschaft, in deren Bezirk die Überwachungsmaßnahme stattfinden soll. Die Prüfung bemisst sich nach nationalem Recht und somit insbesondere nach §§ 100a f. StPO. Liegen die dort geregelten Voraussetzungen nicht vor, kann dem Ersuchen nicht stattgegeben werden.

Hinsichtlich der Verwendung der Ergebnisse von Überwachungsmaßnahmen, insbesondere bezüglich Zweckänderung, Vernichtung und Benachrichtigungspflichten, enthält das Übereinkommen zwar keine explizite Regelung. Es besteht aber die Möglichkeit, dass der ersuchte Mitgliedstaat seine Zustimmung von der Erfüllung von Bedingungen abhängig machen kann, die in einem vergleichbaren Fall aufgrund des jeweiligen nationalen Rechts zu erfüllen wären. Insoweit kann im Rahmen der Bewilligung des Ersuchens durch die Auferlegung entsprechender Bedingungen die Verwendung und Vernichtung des erlangten Materials geregelt werden.

Die nach deutschem Recht geltenden Schutzvorkehrungen im Zusammenhang mit der Überwachung der Telekommunikation konnten folglich weitgehend in das Übereinkommen übernommen werden. Dies bewerte ich positiv, insbesondere mit Blick darauf, dass bei europäischen Übereinkommen jeder Mitgliedstaat mit Kompromissen leben muss.

Ferner wurde erfreulicherweise eine Datenschutzklausel im Übereinkommen selbst aufgenommen und nicht nur, wie ursprünglich vorgesehen, im Rahmen eines Zusatzprotokolls. Diese Regelung enthält eine Zweckbindung zum Schutz personenbezogener Daten, von der entweder nur mit Zustimmung des übermittelnden Mitgliedstaats oder beispielsweise zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit abgewichen werden darf.

6.10 Cyber Crime – Übereinkommen des Europarates über Datennetzkriminalität

Im Frühjahr 1999 wurde ich vom BMJ erstmals im Rahmen der Ressortabstimmung an dem Entwurf eines Übereinkommens des Europarates über Datennetzkriminalität beteiligt, allgemein auch als „Cyber-Crime Convention“ bekannt. Der Übereinkommensentwurf geht von der Überzeugung aus, dass eine wirksame Bekämpfung der Datennetzkriminalität eine verstärkte und rasche internationale Zusammenarbeit in Strafsachen verlangt. Der Schutz der Gesellschaft vor der Gefahr, dass Rechnernetze und elektronische Daten auch zur Begehung von Straftaten genutzt werden können, soll unter anderem durch die Schaffung angemessener Rechtsvorschriften erreicht werden. Im Übereinkommen befinden sich daher sowohl Regelungen zum materiellen Strafrecht, also konkrete Straftatbestände, als auch zum Verfahrensrecht, d. h. wie diese Straftaten verfolgt werden sollen; ein weiterer Komplex befasst sich mit Fragen der internationalen Zusammenarbeit.

Im Laufe der Beratungen auf nationaler und auf internationaler Ebene hat der Entwurf zahlreiche inhaltliche Änderungen erfahren. Besonderes Augenmerk habe ich auf die Bestimmungen zu den Überwachungsmaßnahmen im Bereich der elektronischen Kommunikation gelegt. Hier geht es um die Überwachung der sog. Verbindungsdaten, d. h. der Daten, die bei der Inanspruchnahme der elektronischen Kommunikationswege anfallen, und um die sog. Inhaltsdaten, also um die Gespräche selbst. Dabei konnte ich erreichen, dass – zumindest in der aktuellen Entwurfsfassung – eine Überwachung der Telekommunikation auf schwerwiegende Delikte beschränkt ist und unter dem Vorbehalt nationalen Rechts steht. Hinsichtlich der Verbindungsdaten ist eine Sammlung oder Aufzeichnung nur zu Zwecken strafrechtlicher Ermittlungen und Verfahren möglich, wenn nationale Bestimmungen nicht entgegenstehen. Einer in früheren Entwürfen vorgesehenen Verpflichtung der Diensteanbieter, Verbindungsdaten, die sich auf die über ihre Computersysteme ablaufenden Datenübertragungen beziehen, quasi auf Vorrat für einen längeren Zeitraum zu speichern, bin ich erfolgreich entgegengetreten.

6.11 Bundeszentralregistergesetz

6.11.1 Novellierung des Bundeszentralregistergesetzes

Unter Nr. 6.9 meines 17. TB habe ich über die Arbeiten zur Novellierung des Bundeszentralregistergesetzes (BZRG) berichtet, die allerdings in der abgelaufenen Legislaturperiode nicht mehr abgeschlossen werden konnten. Seit dem Frühjahr 2000 befindet sich nunmehr der neue Referentenentwurf eines Vierten Gesetzes zur Änderung des BZRG in der Ressortabstimmung. Dieser orientiert sich im Wesentlichen an dem Inhalt des Vorentwurfs und berücksichtigt zahlreiche meiner Empfehlungen.

Zum jüngsten Entwurf habe ich gegenüber dem BMJ angeregt, in § 41 Abs. 1 Nr. 2 BZRG die im Vorentwurf enthaltene Einschränkung, wonach Auskunftsersuchen der obersten Bundes- und Landesbehörden *„für eigene Zwecke“* begrenzt werden, wieder aufzunehmen. Die Einschränkung hätte lediglich eine Klarstellung zur Folge, denn in den vergangenen Jahren führte die geltende Regelung zu erheblichen praktischen Problemen, insbesondere im Hinblick auf die Ausnahmeregelung des § 43 BZRG. Danach dürfen oberste Bundes- oder Landesbehörden Eintragungen, die in ein Führungszeugnis nicht aufgenommen werden, an eine nachgeordnete oder ihrer Aufsicht unterstehende Behörde im überwiegenden Allgemeininteresse weiterleiten. Eine solche Datenübermittlung halte ich aber dann nicht für zulässig, wenn ihr nur der Umstand zugrunde liegt, dass das Gesetz einer nachgeordneten oder ihrer Aufsicht unterstehenden Behörde nicht die Möglichkeit gibt, selbst eine unbeschränkte Auskunft einzuholen. Deshalb sollte das Recht oberster Bundes- und Landesbehörden auf unbeschränkte Auskunft ausdrücklich dahingehend eingegrenzt werden, dass ein Auskunftsersuchen nur zur Erfüllung eigener Aufgaben zulässig ist, nicht aber zur Erfüllung von Aufgaben einer nachgeordneten oder ihrer Aufsicht unterstehenden Behörde. Davon unberührt bleibt die Frage, inwieweit die oberste Bundes- oder Landesbehörde eine einzelne Angelegenheit einer nachgeordneten Behörde im Rahmen der Rechts- oder Fachaufsicht zu einer eigenen Aufgabe machen kann. Das BMJ ist meiner Empfehlung nicht gefolgt. Bei Beharren auf dieser Klarstellung wäre allerdings nicht auszuschließen, dass der Kreis der berechtigten Behörden erheblich anwachsen würde. Angesichts derartiger datenschutzrechtlich nicht zu begrüßenden Folgen habe ich in Abwägung dieser widerstreitenden Interessen von einer Weiterverfolgung meiner Forderung Abstand genommen.

Im Hinblick auf die vom BMJ zügig vorangeführten Arbeiten halte ich das Ziel, den Gesetzentwurf noch in dieser Legislaturperiode abschließend in den parlamentarischen Gremien zu beraten, für realistisch.

6.11.2 Fehler des BZR beim Versand von Führungszeugnissen und unbeschränkten Auskünften

Durch verschiedene Eingaben bin ich darauf aufmerksam gemacht worden, dass beim Versand von Führungszeugnissen und unbeschränkten Auskünften durch die Absendestelle des BZR Fehler oder Nachlässigkeiten aufgetreten sind. So wurde moniert, dass in Sammelpostsendungen an Behörden keine Einzelcouvertierung für die unterschiedlichen Ämter erfolgt sei oder dass Führungszeugnisse verschiedener Personen in einem Umschlag an eine Person versandt worden seien. In allen Fällen habe ich mich mit dem BZR in Verbindung gesetzt, um die Sachverhalte zu klären und den Ursachen nachzugehen.

Nach den Stellungnahmen des BZR ist der Hauptgrund darin zu sehen, dass – durch die Behördenverlagerung von Berlin nach Bonn bedingt – das bisherige Personal nahezu vollständig ersetzt wurde und dass trotz intensiver Schulungsmaßnahmen die notwendige Sensibilität bei dem neuen Personal noch nicht erzielt ist. Hinzu kommt aus Sicht des BZR, dass bei einem Postversandaufkommen von ca. 30 000 bis 40 000 Poststücken täglich Bearbeitungsfehler nie ganz auszuschließen sind. Die Mitarbeiter der Versandstelle seien aufgrund der vorliegenden Eingaben zusätzlich zu den Regelungen der Dienstanweisung unterwiesen worden. Da die Eingaben sich allerdings über einen längeren Zeitraum erstreckten und zum Teil auch die gleichen Verfahrensfehler betreffen, habe ich Zweifel, ob diese vom BZR getroffenen Maßnahmen – trotz allen Bemühens – ausreichend geeignet sind, die Fehler abzustellen. Ich werde mir in Kürze daher deren Wirkung in der Praxis ansehen und mit dem BZR gegebenenfalls weitere erforderliche Verfahrensverbesserungen beraten.

6.11.3 Zentrales Staatsanwaltschaftliches Verfahrensregister

In meinem 17. TB (Nr. 6.8) habe ich ausführlich über die organisatorische und technische Umsetzung des Vorhabens zur Einrichtung eines zentralen staatsanwaltschaftlichen Verfahrensregisters (ZStV) berichtet. Im Frühjahr 1999 wurde der Echtbetrieb aufgenommen. Bei einem Informations- und Kontrollbesuch konnte ich mich von der sachgerechten Durchführung überzeugen.

Gegenwärtig sind erst einige Bundesländer und Behörden aus dem berechtigten Nutzerkreis angeschlossen, da vielfach noch die technischen Voraussetzungen geschaffen werden müssen. Die Datenübermittlung von und zum ZStV erfolgt in einer geschlossenen Benutzergruppe im ISDN-Netz. Auch in dem ebenfalls benutzten TESTA-Overlaynetz der Deutschen Telekom AG sollten Bedingungen geschaffen werden, die denen des ISDN-Netzes vergleichbar sind. Ich habe daher auf der kurzfristigen Einrichtung einer zusätzlichen Leitungsverschlüsselung in diesem Netz bestanden. Da diese jedoch nur als Übergangslösung dienen soll, habe ich gegenüber dem BMJ und dem BZR wiederholt auf die Einrichtung der im Sicherheitskonzept des BSI festgelegten „Ende-zu-Ende-Verschlüsselung“ hingewiesen und daran erinnert, die Entwicklung und Installation eines dem MailTrusT-Standard entsprechenden Verschlüsselungssystems mit Nachdruck zu betreiben.

Die technische Betreuung des ZStV erfolgt durch eine Fremdfirma, deren Pflichten vertraglich festgelegt sind. Die Beschäftigten des Dienstleistungsunternehmens verfügen für die Erledigung der vertraglichen Pflichten über alle Administratorenrechte, so dass zwar theoretisch die Möglichkeit des Zugangs zu Registereinträgen gegeben ist, wegen der Komplexität des Registers dies jedoch nur mit sehr hohem Programmieraufwand zu erreichen wäre. Damit ist bereits ein gewisser faktischer Schutz gegen missbräuchliche Nutzung gegeben. Zusätzlich werden allerdings noch stichprobenartige Kontrollen durchgeführt, durch die missbräuchliche Zugriffe aufgedeckt und ermittelt werden können. Darüber hinaus sind sämtliche Mitarbeiter des Dienstleisters besonders verpflichtet und über die strafrechtlichen Folgen missbräuchlichen Handelns aufgeklärt worden. Da nach Abschluss des Umzuges des BZR von Berlin nach Bonn die technische Betreuung

sukzessive von der Fremdfirma auf hauseigenes Personal übergehen soll, gehe ich von einer weiteren Minimierung der Missbrauchsrisiken aus.

Zur Zeit befinde ich mich in einem kontrovers geführten Dialog mit dem BMJ zu Art und Inhalt der nach § 495 StPO (§ 477 StPO a. F.) auf Antrag aus dem ZStV zu erteilenden Auskünfte. Hierbei geht es darum, dass die Registerbehörde im Einvernehmen mit der Staatsanwaltschaft, die die personenbezogenen Daten zur Eintragung in das Verfahrensregister mitgeteilt hat, über den Umfang der Auskunft zu entscheiden und dabei auch zu berücksichtigen hat, welche sonstigen Rückschlüsse aus der Art der jeweiligen Auskunft geschlossen werden können. Ich hoffe, dass dieses Problem in nächster Zeit gelöst werden kann.

6.12 Generalbundesanwalt beim Bundesgerichtshof

Beim Generalbundesanwalt (GBA) beim Bundesgerichtshof habe ich mir ein Bild über den dortigen Umgang mit besonders schutzwürdigen personenbezogenen Daten verschafft. Thematische Schwerpunkte meines Besuches waren die Anordnung und Durchführung von Telefonüberwachungsmaßnahmen nach § 100 a StPO, insbesondere die Benachrichtigung der Beteiligten nach § 101 Abs. 1 StPO und die Vernichtung der Unterlagen nach § 100b Abs. 6 StPO.

Nach § 101 Abs. 1 StPO sind bei einer Überwachung der Telekommunikation die Beteiligten zu benachrichtigen, sobald dies ohne Gefährdung des Untersuchungszwecks, der öffentlichen Sicherheit, von Leib oder Leben einer Person sowie der Möglichkeit der weiteren Verwendung eines eingesetzten nicht offen ermittelnden Beamten geschehen kann.

Sowohl die Prüfung von Akten als auch die Diskussion mit dem GBA hat ergeben, dass die Problematik hauptsächlich im Begriff des „Beteiligten“ liegt. Der Gesetzeswortlaut lässt sich an dieser Stelle sehr weit auslegen und kann dazu führen, dass neben dem Beschuldigten jede Person, mit der dieser den überwachten Fernmeldeverkehr geführt hat, sowie jede Person, die den überwachten Telefonanschluß benutzt hat – sei es als Anrufer oder als Angerufener – zu benachrichtigen ist. In der Praxis ergeben sich hier bereits erhebliche Schwierigkeiten bei der Ermittlung bzw. Identifizierung dieses Personenkreises. Ein Teil der Gesprächsteilnehmer oder Anschlussbenutzer wird zwar zunächst namentlich bekannt, falls aber das entsprechende Gespräch nicht zur weiteren Strafverfolgung gegen den Beschuldigten erforderlich ist, nehmen die Ermittlungsbehörden keine genaue Personenidentifizierung vor mit der Folge, dass sich aus den Akten nicht entnehmen lässt, welche Person genau zu benachrichtigen ist. Darüber hinaus gibt es in der Regel auch Gesprächsteilnehmer, die zwar zu Beginn des Ermittlungsverfahrens aufgrund bestimmter Anhaltspunkte für die Strafverfolgung relevant sind, bei denen sich aber später herausstellt, dass keine Verbindung zum Strafverfahren besteht. Bei diesem Personenkreis wurde zwar zunächst eine Personenidentifizierung vorgenommen, im Laufe des Ermittlungsverfahrens werden aber keine Änderungen, wie z. B. ein Wohnungswechsel, festgehalten. So ist in einem der geprüften Verfahren fast die Hälfte der Benachrichtigungsschreiben als unzustellbar zurückgekommen, weil die Adressaten unter der aus den Akten entnommenen Anschrift nicht mehr erreichbar waren. An diesen Beispielen wird deutlich, dass eine weite Auslegung des Begriffes des Beteiligten die Praxis der Strafverfolgungsbehörden vor große Probleme stellt.

Neben diesen eher praktischen Problemen stellt sich bei der Benachrichtigung eines großen Personenkreises die Frage, inwieweit durch die Benachrichtigung selbst unverhältnismäßig in die schutzwürdigen Belange Dritter oder auch des ursprünglich Beschuldigten selbst eingegriffen wird. Hinsichtlich verfahrensunbeteiligter Dritter kann das insbesondere dann der Fall sein, wenn ihre Identität und Anschrift erst zum Zwecke der Benachrichtigung mit eventuell großem Aufwand ermittelt wird, weil dadurch ein erneuter Eingriff in ihre Persönlichkeitsrechte erfolgt. Im Hinblick auf den ursprünglich Beschuldigten ist zu bedenken, dass durch die Benachrichtigung seiner Gesprächspartner und anderer Anschlussbenutzer notwendigerweise offenbart wird, dass gegen ihn ein Ermittlungsverfahren wegen des Verdachts eines Delikts, das eine Telefonüberwachungsmaßnahme rechtfertigt, stattgefunden hat, und dies, obwohl möglicherweise Jahre vergangen sind. Eine derartige Benachrichtigung könnte insbesondere dann unverhältnismäßig sein, wenn sich der Verdacht nicht erhärtet hat und das Verfahren eingestellt worden ist oder wenn ein geschäftlich genutzter Anschluss (z. B. Unternehmen, Rechtsanwaltskanzlei) überwacht wurde und auf diese Weise Kunden und Geschäftspartner über das Ermittlungsverfahren informiert werden. Eine Abwägung zwischen den möglicherweise entgegenstehenden schutzwürdigen Belangen aller betroffenen Personen sieht das Gesetz aber nicht vor.

Die Diskussion, aber auch die Kontrolle der vorgelegten Akten ergab, dass die Frage, wer wann zu benachrichtigen ist, einheitlich für die gesamte Behörde zu regeln ist. Im Nachgang zu meinem Besuch hat der GBA erfreulicherweise Richtlinien erlassen, die sowohl dem gesetzlichen Gebot der Benachrichtigung als auch den schutzwürdigen Belangen des Beschuldigten Genüge tun.

Von den Maßnahmen der Telefonüberwachung sind demnach in jedem Fall der Beschuldigte und, falls keine Identität besteht, der Anschlussinhaber zu benachrichtigen. Ferner werden die bekannten Nutzer eines privaten Telefonanschlusses benachrichtigt. Dabei kann es sich z. B. um im Haushalt des Anschlussinhabers lebende Familienangehörige oder um Mitbewohner einer Wohngemeinschaft handeln. Die Benachrichtigungen sind an die Adresse der Wohnanschrift zu senden. Falls diese Person dort nicht mehr wohnt und die neue Adresse nicht bekannt ist, werden in der Regel keine Ermittlungen zur Feststellung des Aufenthaltsortes eingeleitet.

Nach § 100b Abs. 6 StPO sind die durch die Telefonüberwachung erlangten Unterlagen unverzüglich zu vernichten, wenn sie zur Strafverfolgung nicht mehr erforderlich

sind. Zum Zeitpunkt meines Besuches hatte der GBA keine für alle Mitarbeiter verbindlichen Richtlinien erlassen, wie die Unterlagen zu vernichten sind. Vielmehr entschied jeder Bearbeiter im Rahmen der gesetzlichen Vorschriften nach eigenem Ermessen. Auch gab es keine festen Fristen, innerhalb derer die Frage, ob Unterlagen vernichtet werden sollen, zu prüfen war. Die Löschung der Unterlagen aus der Telefonüberwachung erfolgte in den Fällen, in denen es nicht zu einem gerichtlichen Verfahren kam, ca. sechs Monate nach Einstellung des Verfahrens. Ansonsten wurden die Unterlagen in der Regel etwa sechs Monate nach Bestandskraft des Urteils gelöscht, wobei allein die Möglichkeit einer Wiederaufnahme des Verfahrens – also ohne erkennbare Anzeichen – nicht zum Anlass genommen wurde, die Löschung aufzuschieben.

Inzwischen hat der GBA – ebenfalls in Form einer Richtlinie – eine einheitliche Regelung für seinen Dienstbetrieb entwickelt. Demnach ist nach Beendigung einer Maßnahme zu prüfen, ob die Unterlagen für das weitere Ermittlungsverfahren benötigt oder umgehend vernichtet werden können. Sofern eine Löschung noch nicht in Betracht kommt, ist die Prüfung im Abstand von drei Monaten erneut vorzunehmen. Darüber hinaus soll die Vernichtung sechs Monate nach Abschluss des Ermittlungsverfahrens bzw. nach rechtskräftiger Entscheidung erfolgen, sofern nicht ausnahmsweise eine weitere Aufbewahrung erforderlich ist.

Die Reglungen in den Richtlinien des GBA bewerte ich positiv. Sie werden sowohl den strafprozessualen als auch den datenschutzrechtlichen Anforderungen gerecht und bieten gleichzeitig praktikable Lösungen. Die aufgezeigten Probleme verdeutlichen aber auch, dass eine Klarstellung des Begriffs „Beteiligter“ in § 101 Abs. 1 StPO durch den Gesetzgeber wünschenswert ist, um zu einer angemessenen Interessenabwägung bei der Frage der Benachrichtigung zu gelangen und eine einheitliche Praxis der Strafverfolgungsbehörden zu gewährleisten.

6.13 Veröffentlichung heimlicher Bildaufnahmen – Gesetzeslücke im Strafgesetzbuch –

Im Strafgesetzbuch finden sich zahlreiche Straftatbestände, die die Verletzung des persönlichen Lebens- und Geheimbereichs sanktionieren. So wird in § 201 StGB die heimliche Aufnahme des nichtöffentlich gesprochenen Wortes und dessen Veröffentlichung unter Strafe gestellt. Vorschriften gegen das unbefugte Aufnehmen des Bildes von Menschen und die Veröffentlichung solcher Aufnahmen existieren jedoch nicht. Dabei ermöglichen es vor allem die technischen Entwicklungen in der Videotechnik und im Internet, Bilder von Menschen unbemerkt aufzunehmen und auch weltweit zu verbreiten, ohne dass der Einzelne dies je wahrnimmt, geschweige denn seine Zustimmung geben könnte.

Vor diesem Hintergrund habe ich in letzter Zeit mit großer Besorgnis immer öfter Eingriffe in die Persönlichkeitsrechte von Bürgern festgestellt. So werden im Internet Fotos von Personen veröffentlicht, die weder von der Aufnahme noch von deren Veröffentlichung Kenntnis haben. Dabei bewegen sich diese Personen nur zum Teil in der Öffentlichkeit, zum Teil aber in Bereichen, wo sie sich bewusst der Öffentlichkeit entziehen wollen und deshalb auch gar nicht mit der Aufnahme von Bildern rechnen können bzw. müssen. Dazu zählen z. B. eine Privatwohnung, Umkleidekabinen in Schwimmbädern oder Geschäften. Es kann nicht angehen, dass so etwas weiterhin straffrei ist. Dies bedarf aus meiner Sicht dringend einer gesetzlichen Regelung. Es ist äußerst unbefriedigend, wenn die Veröffentlichung von heimlichen Tonaufnahmen unter Strafe gestellt ist, während die mindestens einen ebenso tiefen Eingriff in die Persönlichkeitsrechte darstellende Nutzung oder Veröffentlichung von heimlichen Bildaufnahmen nur dann strafbar ist, wenn sie in Verbindung mit anderen Delikten steht. Für diese unterschiedliche Behandlung sehe ich gerade mit Blick auf die technischen Möglichkeiten keinen sachlichen Grund, so dass es nur folgerichtig ist, im Strafgesetzbuch eine Regelung zumindest für die Fälle zu schaffen, in denen mittels Bildaufnahme bzw. -veröffentlichung unbefugt in den Kernbereich der Privatsphäre und in die Intimsphäre eingegriffen wird.

Das BMJ hat mir auf Nachfrage mitgeteilt, dass es diese Problematik seit längerem aufmerksam beobachtet, über das weitere Vorgehen jedoch noch nicht abschließend entschieden habe. Ich halte eine gesetzliche Regelung für unabweisbar und werde weiterhin darauf hinwirken.

6.14 Einsatz der Videotechnik im finanzgerichtlichen Verfahren

In meinem 17. TB (Nr. 6.5) hatte ich über die Einführung der Videotechnik bei Zeugenvernehmungen im Strafverfahren berichtet. Inzwischen darf die Videotechnik auch in der mündlichen Verhandlung des finanzgerichtlichen Verfahrens eingesetzt werden. Mit dem Zweiten Gesetz zur Änderung der Finanzgerichtsordnung und anderer Gesetze (2. FGOÄndG, BGBl. 2000 I S. 1757, 1758) sind in den neuen §§ 91a und 93a Regelungen in die Finanzgerichtsordnung (FGO) aufgenommen worden, die es den Finanzgerichten gestatten, Verfahrensbeteiligte nach § 57 FGO im Wege der Videokonferenz an der mündlichen Verhandlung teilnehmen zu lassen, auf diese Weise Zeugen und Sachverständige zu vernehmen und darüber hinaus deren Aussagen auch aufzuzeichnen.

Im Regierungsentwurf des 2. FGOÄndG (BT-Drs. 14/4061) war zur Videoaufzeichnung der Aussagen von Zeugen und Sachverständigen lediglich vorgesehen gewesen, dass das Gericht sie nach Ermessen anordnen kann. Wenn ein am Verfahren Beteiligter dies wünscht, sollte die Aussage im Regelfall aufgezeichnet werden.

Die Aufzeichnung von Zeugen- und Sachverständigenaussagen *„in Bild und Ton“* (vgl. § 93a Sätze 2 und 3 FGO) ist ein Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen, für den es einer ausreichenden gesetzlichen Grundlage bedurfte, die im Interesse des Betroffenen die Voraussetzungen dafür festlegt und die

Grenzen der Verwendungsmöglichkeiten der Aufzeichnung bestimmt. Die knappen Regelungen des Regierungsentwurfs reichten hierfür nicht aus. Ich begrüße es daher, dass meine Vorschläge zur Änderung und Ergänzung der §§ 91a und 93a FGO im Rahmen der parlamentarischen Beratungen übernommen worden sind.

Hiernach wird zunächst in § 91a FGO ausdrücklich klargestellt, dass die Äußerungen der selbst am Verfahren Beteiligten nicht aufgezeichnet werden dürfen. Als Voraussetzung für die Aufzeichnung der Aussagen von Zeugen und Sachverständigen wurde in Anlehnung an § 247a StPO festgelegt, dass diese nur erfolgen soll, *„wenn zu besorgen ist, dass der Zeuge oder Sachverständige in einer weiteren mündlichen Verhandlung nicht vernommen werden kann und die Aufzeichnung zur Erforschung des Sachverhalts erforderlich ist“*. Damit wird vom Gesetzgeber festgelegt, dass das informationelle Selbstbestimmungsrecht des Zeugen oder Sachverständigen hinter dem überwiegenden öffentlichen Interesse an der Erforschung des Sachverhalts durch das Gericht zurücktritt.

Außerdem bestimmt nunmehr über den ursprünglichen Entwurf hinaus ein neuer Abs. 2 des § 93a FGO, dass die Aufzeichnung nur innerhalb des Verfahrens verwendet werden darf, für das sie gefertigt worden ist. Eine Verwendung in einem anderen Verfahren oder für sonstige Zwecke, wie z. B. die Weitergabe an Dritte außerhalb des Verfahrens, wäre eine Zweckänderung, die einer eigenen gesetzlichen Grundlage bedürfte. Auch ist hier festgelegt, dass das Recht zur Zeugnisverweigerung nach § 84 FGO zu wahren ist. Dies bedeutet etwa, dass eine Nutzung der Aufnahme zum Zwecke des Vorhalts ausgeschlossen ist, wenn sich ein Zeuge auf sein Zeugnisverweigerungsrecht beruft. Im Hinblick auf den persönlichen Charakter der Aufzeichnung und die Notwendigkeit, achtlosen Umgang oder Missbrauch mit möglichen Kopien auszuschließen, ist dort weiterhin geregelt, dass die Einsicht in Aufzeichnungen nach § 78 Abs. 1 FGO nur auf der Geschäftsstelle erfolgen darf und Kopien nicht erteilt werden. Schließlich bestimmt § 93a FGO, dass die Aufzeichnung zu löschen ist, sobald sie nicht mehr benötigt wird. Dies hat spätestens nach rechtskräftigem Abschluss des Verfahrens zu geschehen.

Mit diesen Ergänzungen dürften wesentliche Voraussetzungen für die Videoaufzeichnung der Aussagen von Zeugen und Sachverständigen gesetzlich festgelegt sein. Ich schließe jedoch nicht aus, dass vor allem aufgrund von Erfahrungen in der Praxis weitere Regelungen zum Schutz des Persönlichkeitsrechts der Zeugen und Sachverständigen hinzutreten können.

6.15 Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich

Auf die Notwendigkeit einer gesetzlichen Grundlage für die Aufbewahrung von Akten und die Speicherung personenbezogener Daten in Dateien der Justiz habe ich bereits in meinem 16. TB (Nr. 6.14, vgl. auch 17. TB Nr. 34, dort Nr. 7) hingewiesen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte hierzu auf ihrer 49. Sitzung im Frühjahr 1995 eine Entschließung verabschiedet (vgl. 16. TB Anlage 6), um die Bedeutung der Angelegenheit zu unterstreichen.

Auch die Oberlandesgerichte Frankfurt a. M. und Hamm haben in Beschlüssen aus dem Jahre 1998 hierzu eine gesetzliche Grundlage gefordert. Insbesondere das OLG Frankfurt a. M. hat in seinem Beschluss festgestellt, dass der derzeitige Zustand nur noch für eine Übergangszeit hinzunehmen sei und der Gesetzgeber die Schaffung einer gesetzlichen Grundlage für die Aufbewahrung von Akten im Justizbereich alsbald in Angriff nehmen solle. Daraufhin hat sich die Konferenz der Datenschutzbeauftragten auf ihrer 58. Sitzung im Herbst 1999 erneut mit dem Thema befasst und mit einer weiteren Entschließung (s. **Anlage 16**) auf die Dringlichkeit der Schaffung gesetzlicher Grundlagen sowohl für die Aufbewahrung von Strafakten als auch von Zivilprozessakten und Akten im Bereich der freiwilligen Gerichtsbarkeit hingewiesen.

Das BMJ hat mir hierzu mitgeteilt, es sei nach wie vor mit der Prüfung befasst, welche Maßnahmen im einzelnen erforderlich seien. Derzeit prüfe es intensiv Fragen der Gesetzgebungskompetenz. Im Hinblick auf den bestehenden Diskussionsbedarf sehe es jedoch kaum Chancen für eine kurzfristige Erarbeitung einer auf den notwendigen Regelungsumfang beschränkten, rechtspolitisch von allen Betroffenen akzeptierbaren gesetzliche Regelung. Immerhin hat sich die Konferenz der Justizministerinnen und -minister am 24./25. Mai 2000 mit der Thematik befasst und eine länderoffene Arbeitsgruppe mit der Beantwortung der Frage beauftragt, ob und ggf. welche gesetzlichen Regelungen für die Aktenaufbewahrung bei Gerichten und Staatsanwaltschaften zu schaffen sind. Die Arbeitsgruppe hat im September 2000 konstituierend und ohne abschließende Ergebnisse getagt. Die Zeit drängt. Derzeit bleibt abzuwarten, welche Ergebnisse die Arbeitsgruppe der Justizministerkonferenz vorlegen wird.

7 Finanzwesen

7.1 Außenprüfer am PC des Steuerpflichtigen

§ 147 AO ist um einen neuen Abs. 6 erweitert worden, wonach die Finanzbehörde im Rahmen einer Außenprüfung das Recht hat, im Datenverarbeitungssystem des Steuerpflichtigen gespeicherte Buchhaltungsunterlagen einzusehen und das Datenverarbeitungssystem zur Prüfung dieser Unterlagen zu nutzen. Auch kann die Finanzbehörde danach u. a. verlangen, dass die gespeicherten Unterlagen und Aufzeichnungen auf einem maschinell verwertbaren Datenträger zur Verfügung gestellt werden (BGBl. 2000 I S. 1433, 1460). Da auf diesem Wege wie bisher nur die nach § 147 Abs. 1 AO aufbewahrungspflichtigen Unterlagen geprüft werden dürfen, bestehen hiergegen grundsätzlich keine Bedenken. Die Vorschrift

bedurfte allerdings ergänzender datenschutzrechtlicher Regelungen:

Im Datenverarbeitungssystem der jeweiligen Betriebe befinden sich neben den von der Finanzbehörde im Einzelfall zu prüfenden steuerlich relevanten Daten weitere, vor allem auch personenbezogene Daten der Mitarbeiter, von Kunden und von Geschäftspartnern. Soweit der Betrieb keine Zugriffsregelungen für sein System programmiert hat, kann die Finanzbehörde bei ihrer Prüfung auch auf diese Daten zugreifen. Die für die Finanzbehörden nach § 147 Abs. 6 AO zugelassenen Möglichkeiten, das Datenverarbeitungssystem des Steuerpflichtigen zu nutzen, sind relativ weit. Insofern wird es den Betrieben – je nach Art der eingesetzten Datenverarbeitungs-Verfahren – nicht immer möglich sein, die Zugriffe der Finanzbehörden tatsächlich auf die Unterlagen zu begrenzen, die für die Prüfung relevant sind.

Aus Gesprächen mit Verbandsvertretern ist mir bekannt, dass viele Betriebe nicht über Personaldatenverarbeitungssysteme verfügen, die eine Abschottung zwischen dem Lohnkonto und gegebenenfalls anderen steuerlich relevanten Daten eines Mitarbeiters und seinen übrigen Personaldaten (z. B. Daten über den beruflichen Werdegang oder auch über Abwesenheiten, Pfändungen usw.) ermöglichen. Da dies im Hinblick auf Nr. 5 der Anlage zu § 9 Satz 1 BDSG gegen das Gebot der Zugriffskontrolle verstößt, habe ich zunächst dem BMF und ebenso dem Finanzausschuss des Deutschen Bundestages vorgeschlagen, das Inkrafttreten des § 147 Abs. 6 AO bis zum 31. Dezember 2002 hinauszuschieben. Dem wurde zum Teil gefolgt. § 147 Abs. 6 AO ist zwar – wie ursprünglich vorgesehen – bereits am Tag der Verkündung, d. h. am 26. Oktober 2000, in Kraft getreten. Im Einführungsgesetz zur Abgabenordnung wurde jedoch u. a. geregelt, dass diese Vorschrift erst ab dem 1. Januar 2002 anzuwenden ist. Ob dieser Zeitraum für die Umstellung ausreicht, wird die Praxis zeigen. Es bleibt jedoch anzumerken, dass die Rechtsverpflichtung, Maßnahmen zur Zugriffskontrolle vorzusehen, wenn in einem Datenverarbeitungssystem Daten verarbeitet werden, die zu unterschiedlichen Bereichen eines Betriebes gehören, schon im ersten BDSG von 1977 festgelegt worden war. Insofern scheinen hier einige Betriebe ihre rechtlichen Verpflichtungen schon über längere Zeit etwas locker gesehen zu haben.

Ähnlich wie in den Fällen des automatisierten Datenabrufs ist der „vor Ort“ im Datenverarbeitungssystem des Steuerpflichtigen prüfenden Finanzbehörde das Recht eingeräumt, auf bestimmte gespeicherte Daten zuzugreifen. Die Finanzbehörde darf nach § 147 Abs. 6 AO allerdings nur Daten einsehen, soweit dies sich im Rahmen der Prüfungsanordnung (§ 196 AO) hält. Daher hatte ich auch empfohlen, in der Abgabenordnung entsprechend den Regelungen über den automatisierten Datenabruf eine Protokollierung der Zugriffe der Finanzbehörde auf die Daten des Steuerpflichtigen in dessen Datenverarbeitungssystem und auf bereitgestellten maschinell verwertbaren Datenträgern sowie der Nutzungen des Datenverarbeitungssystems festzulegen. Damit sollte ein Schutz gegen unbefugte Einsichtnahme in Daten des Steuerpflichtigen und gegen unbefugte Nutzung des Datenverarbeitungssystems erreicht werden.

Der Finanzausschuss des Deutschen Bundestages ist meinem Vorschlag für eine entsprechende Regelung in der Abgabenordnung nicht gefolgt. In der von ihm dazu gegebenen Begründung führt er jedoch aus, die Ausschussmehrheit halte eine Regelung, *„die die Finanzverwaltung zur Protokollierung der Einsichtnahme in gespeicherte Daten und der Nutzung des DV-Systems des Steuerpflichtigen sowie der Prüfung der auf Datenträgern zur Verfügung gestellten Buchführungsdaten verpflichtet...“*, *„für nicht erforderlich, weil eine Pflicht zur Protokollierung der Zugriffe auf DV-Systeme bereits sowohl im BDSG (§ 9 BDSG i.V. mit der Anlage dazu) als auch im BMF-Schreiben vom 7. November 1995 (BStBl I 1995 S. 738) zur Auslegung des unbestimmten Rechtsbegriffs „Ordnungsmäßigkeit der Buchführung“ der §§ 238, 239, 257 und 261 HGB sowie §§ 145 bis 147 AO enthalten sei“* (BT-Drs. 14/3366 S. 115). Wenn ich auch nach wie vor eine eindeutige Regelung in der Abgabenordnung vorziehe, ist mir doch wichtig, dass der Finanzausschuss die Pflicht zur Protokollierung und damit mein datenschutzrechtliches Anliegen der Sache nach bestätigt hat.

7.2 Datenschutzrechtliche Überarbeitung der Abgabenordnung in Sicht

In meinem 17. TB (Nr. 7.3) habe ich von der damals ablehnenden Haltung des BMF gegenüber meinen Vorschlägen zur datenschutzrechtlichen Verbesserung der Abgabenordnung und davon berichtet, dass der Deutsche Bundestag bereits bei der Behandlung meines 16. TB die Erwartung ausgesprochen hatte, die Bundesregierung werde im Einzelfall datenschutzrechtliche Empfehlungen zur Abgabenordnung auch künftig sorgfältig prüfen und erforderliche Änderungen aufgreifen.

Inzwischen hat mich das BMF – insbesondere vor dem Hintergrund neuerer Entwicklungen im Bereich der Informations- und Kommunikationstechniken – zu bilateralen Gesprächen über die Berücksichtigung datenschutzrechtlicher Belange in der Abgabenordnung eingeladen. Neben Fragen der Abgrenzung zwischen den Regelungsbereichen der Abgabenordnung und der Datenschutzgesetze des Bundes und der Länder wurden hierbei zunächst thematische Schwerpunkte wie

- die automatisierte Datenverarbeitung,
- der Anspruch des Steuerpflichtigen auf Auskunft und Akteneinsicht,
- Outsourcing/Datenverarbeitung im Auftrag und
- die Dauer der Aufbewahrung von Steuerdaten/Löschungsfristen,

diskutiert, um so gemeinsam den Regelungsbedarf im Einzelnen zu ermitteln. In einem nächsten Schritt sollen anhand erster Formulierungen konkrete Lösungsvorschläge erarbeitet werden.

Ich begrüße es, dass das BMF sich nunmehr für eine umfassende Diskussion über die Berücksichtigung meiner

Empfehlungen zur Verbesserung der Abgabenordnung aufgeschlossen zeigt. Ich verbinde dies mit der Hoffnung, dass als Ergebnis dieser Gespräche auch die dann als notwendig erkannten datenschutzrechtlichen Regelungen für den Bereich der Abgabenordnung getroffen werden.

7.3 Besteuerung der Internetnutzung und von Telefonaten am Arbeitsplatz

Eine überaus heftige Diskussion löste im Sommer 2000 die Überlegung des BMF aus, das private Surfen am Arbeitsplatz zu besteuern. Schnell gab es eine feste Allianz aus Wirtschaft, Politik und Medien, dass es keinen gläsernen Arbeitnehmer geben darf und dass diese Überlegung dem politischen Ziel der Bundesregierung zuwiderliefe, Internet und E-Mail zum von jedermann beherrschten normalen alltäglichen Hilfsmittel werden zu lassen.

Das BMF veröffentlichte im Bundessteuerblatt sein Schreiben an die obersten Finanzbehörden der Länder vom 24. Mai 2000 zum Thema „Auslagenersatz, Werbungskosten und geldwerter Vorteil im Zusammenhang mit Telekommunikation des Arbeitnehmers“ (BStBl 2000 I S. 613 f.). Die darin behandelte und vor allem in den Medien herausgestellte Frage, ob das private Surfen des Arbeitnehmers am PC seines Arbeitgebers als geldwerter Vorteil nach § 8 EStG zu versteuern ist, war keine datenschutzrechtliche Frage. Gegenüber dem BMF habe ich jedoch problematisiert, dass die zu erbringenden Nachweise zu einer umfassenden Kontrolle des Informations- und Kommunikationsverhaltens des Arbeitnehmers führen könnten. Nach dem BMF-Schreiben sollten gegenüber dem Finanzamt folgende Nachweise erbracht werden:

- für vom Arbeitnehmer gegenüber dem Finanzamt geltend gemachte *Werbungskosten* wegen beruflich veranlasster Telefonate mit seinem privaten Telefon und
- für unentgeltliche oder verbilligte Mitbenutzung des Telefonanschlusses oder des Internet-Zugangs des Arbeitgebers zu privaten Zwecken des Arbeitnehmers bei der *Besteuerung* als geldwerter Vorteil.

Hinsichtlich der Nachweise für Telefonate durch den mit dem BMF-Schreiben geforderten Einzelverbindungsnachweis über beruflich veranlasste Telefonate habe ich dem BMF in Anlehnung an § 6 Abs. 3 Satz 2 Telekommunikationsdienstunternehmen-Datenschutzverordnung (vgl. jetzt § 7 Abs. 3 Satz 3 Telekommunikations-Datenschutzverordnung, BGBl. 2000 I S. 1742) empfohlen, dass die darin enthaltenen Zielrufnummern bei einer Vorlage beim Finanzamt zumindest zunächst um die letzten drei Ziffern gekürzt werden. Unter Hinweis auf in der Kommentarliteratur erhobene Kritik habe ich außerdem Bedenken erhoben, ob § 413 AO eine ausreichende Regelung dafür enthält, dass das Finanzamt unter Durchbrechung des Fernmeldegeheimnisses überhaupt Kenntnis von den vollständigen Zielrufnummern erhält, auch wenn es diese überprüfen will. Das ebenfalls beteiligte BMJ vertrat hierzu zwar die Ansicht, § 413 AO *„würde allerdings dem Zitiergebot des Artikels 19 Abs. 1 Satz 2 GG noch genügen“*. Dennoch werde ich diese Frage gegenüber dem BMF nochmals ansprechen.

Hinsichtlich des erst spät und nur mit einer kurzen Frist zur Stellungnahme nachgeschobenen Teils des Entwurfs für das BMF-Schreiben über die Besteuerung der privaten Nutzung des Internets durch den Arbeitnehmer habe ich u. a. darauf hingewiesen, dass die dort geforderte Internet-Adresse nach § 6 Abs. 2 Nr. 1 Teledienstedatenschutzgesetz spätestens unmittelbar nach Ende der jeweiligen Nutzung zu löschen ist. In der weiteren Diskussion nach Veröffentlichung des BMF-Schreibens habe ich mich nochmals ausdrücklich gegen die nach dessen Wortlaut geforderte vollständige Protokollierung sämtlicher Online-Zugriffe gewandt, da sie das Persönlichkeitsrecht des Arbeitnehmers unverhältnismäßig beschneidet.

Das BMF war meinen Einwänden und Bedenken zunächst nicht gefolgt. Inzwischen wurde sein Schreiben vom 24. Mai 2000 mit einem weiteren Schreiben des BMF vom 16. Oktober 2000 aufgehoben (BStBl 2000 I S. 1421), da es der von der Bundesregierung angestrebten Entwicklung einer breiten Nutzung des Internet entgegenstand. Darüber hinaus sind *„die Vorteile des Arbeitnehmers aus der privaten Nutzung von betrieblichen Personalcomputern und Telekommunikationsgeräten“* ab 1. Januar 2001 durch eine entsprechende Ergänzung des § 3 EStG um eine neue Nr. 45 steuerfrei gestellt worden (BGBl. 2000 I S. 1850, 1853). Damit haben sich meine Bedenken gegen das Schreiben vom 24. Mai 2000 endgültig erledigt.

7.4 Auskunftsersuchen von Finanzämtern an Telekommunikationsdiensteanbieter

Durch eine Eingabe wurde ich darauf aufmerksam gemacht, dass Finanzämter bei Telekommunikationsdiensteanbietern die Namen und Bankverbindungen der Inhaber von Fernsprechanschlüssen mittels Anschriften erfragen. Dies geschieht beispielsweise durch Steuerfahndungs- oder Vollstreckungsstellen, wenn sie einen Hinweis darauf haben, dass sich eine von ihnen gesuchte Person, etwa ein Vollstreckungsschuldner, unter einer bestimmten Anschrift aufhält und sie sich hierüber die nötige Gewissheit verschaffen möchten.

Ob die Telekommunikationsdiensteanbieter die Fragen der Finanzämter beantworten müssen, konnte ich bisher mit dem BMF nicht klären. Das BMF ist der Auffassung, die Telekommunikationsdiensteanbieter seien hierzu sowohl nach § 93 AO als auch nach § 93 i.V. mit 208 Abs. 1 Satz 1 Nr. 3 und Satz 3 AO verpflichtet. Dem stimme ich nur für den Fall zu, dass Auskunftsersuchen nicht allein auf § 93 AO, sondern auf § 93 i.V. mit § 208 Abs. 1 Satz 1 Nr. 3 und Satz 3 AO gestützt werden und zumindest die Möglichkeit einer strafbaren oder bußgeldbewehrten Handlung besteht. Dies entspricht den Voraussetzungen des § 89 Abs. 6 TKG, wonach Telekommunikationsdiensteanbieter Daten, die *sie „für die Begründung in-*

haltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erhoben haben", u. a. an die *„zuständigen Stellen"* zu übermitteln haben, *„soweit dies für die Verfolgung von Straftaten und Ordnungswidrigkeiten...erforderlich ist"*. Allerdings dürfen nach meiner Auffassung nur Daten abgefragt werden, die einen speziellen Telekommunikationsbezug aufweisen. Hierzu zählen beispielsweise die Namen der Telekommunikationskunden, nicht aber deren Bankverbindungen.

Auskunftsersuchen allein aufgrund § 93 AO steht nach meiner Auffassung § 89 Abs. 6 TKG entgegen. Diese Vorschrift regelt nach ihrem Wortlaut eindeutig, unter welchen Voraussetzungen die Telekommunikationsdiensteanbieter an welche Stellen Vertragsdaten (Bestandsdaten) ihrer Kunden übermitteln dürfen. Die Einholung von Auskünften *„zur Feststellung eines für die Besteuerung erheblichen Sachverhaltes"* nach § 93 AO ist dort nicht als zulässiger Grund für Datenübermittlungen genannt. Die Bestandsdaten der Telekommunikationsdiensteanbieter sind für vertragliche Zwecke der Unternehmen gegenüber ihren Kunden gespeichert. Sinn des § 89 Abs. 6 TKG ist es, Durchbrechungen dieser Zweckbestimmung angemessen zuzulassen und entsprechende Verpflichtungen der Telekommunikationsdiensteanbieter zu begründen. Die Vorschrift ist dementsprechend eng auszulegen. Das BMJ unterstützt meine Auffassung, dass § 89 Abs. 6 TKG die speziellere Vorschrift ist, die der allgemeinen Verpflichtung des § 93 AO zur Auskunft gegenüber den Finanzbehörden vorgeht.

Das BMF macht demgegenüber geltend, die Befugnisse der Finanzbehörden richteten sich nach der Abgabenordnung. Dort sei in den maßgeblichen §§ 101 ff. kein Auskunftsverweigerungsrecht für die Telekommunikationsdiensteanbieter eingeräumt.

Das für das Telekommunikationsgesetz federführende BMWi hat nach erneuter Abstimmung mit dem BMJ und der Regulierungsbehörde für Telekommunikation und Post meine Auslegung bestätigt, soweit es um das Auskunftsrecht der Finanzbehörden nach § 93 AO im Verhältnis zu § 89 Abs. 6 TKG geht. Es ist der Auffassung, dass § 89 Abs. 6 TKG nur in den dort geregelten Fällen diejenigen, die Telekommunikationsdienste geschäftsmäßig erbringen, zur Herausgabe von Bestandsdaten verpflichtet, da § 89 TKG eine sektorspezifische Datenschutzregelung bezüglich der bei der Telekommunikation anfallenden Daten darstellt. Die Regelung ist von einer engen Zweckbindung getragen, die nur im Rahmen der vom Gesetz ausdrücklich gestatteten Art und Weise durchbrochen werden darf. Für die Frage der Übermittlung von Bestandsdaten an Behörden enthält § 89 Abs. 6 TKG eine abschließende Regelung. Bestandsdaten dürfen daher von denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen, nur im Rahmen des § 89 Abs. 6 TKG an den dort erwähnten Kreis befugter Behörden übermittelt werden. Hierzu zählen die Finanzbehörden dann nicht, wenn sie ausschließlich auf der Grundlage des § 93 AO tätig werden und ein Bezug zu einer (Steuerstraftat oder Ordnungswidrigkeit nicht erkennbar ist.

Angesichts der klaren Bestätigung meiner Auffassung nunmehr auch durch das BMWi werde ich an das BMF herantreten, damit es seine Meinung nochmals überprüft und die obersten Finanzbehörden der Länder auffordert, dieser Interpretation des § 89 Abs. 6 TKG zu folgen.

7.5 Auskunft an Familienkasse durch das über 18 Jahre alte Kind

In dem Kindergeld-Antragsformular für über 18 Jahre alte Kinder ist vorgesehen, dass der Kindergeldberechtigte, in der Regel also Vater oder Mutter, darin Angaben zu den Einkünften und Bezügen des Kindes zu machen hat. Dessen Kindergeldanspruch setzt u. a. voraus, dass Einkünfte und Bezüge des erwachsenen Kindes, bei denen auch das Nettoeinkommen des Ehepartners zu berücksichtigen ist, im Kalenderjahr einen bestimmten Betrag nicht überschreiten (im Jahr 2000: 13 500,– DM). Das Formular ist vom Kindergeldberechtigten **und** von dem Kind zu unterschreiben.

In Eingaben von über 18 Jahre alten Kindern, deren Ehepartnern und von Kindergeldberechtigten selbst wurden Bedenken dagegen geltend gemacht, dass das erwachsene Kind oder sogar dessen Ehepartner dem Kindergeldberechtigten gegenüber seine Einkommensverhältnisse offen legen soll, damit dieser das Antragsformular ausfüllen kann.

Die Gewährung von Kindergeld ist regelmäßig ein steuerliches Verfahren (vgl. 17. TB Nr. 7.7). Daher ist es vom Ansatz her zutreffend, wenn die Familienkasse nach § 93 AO mit dem Formular zunächst von dem Antragsteller selbst die Angaben erfragt, mit denen dieser seinen Kindergeldanspruch begründet. Ich habe das BMF jedoch darauf hingewiesen, dass die Erteilung der Auskünfte an die Familienkasse nicht in jedem Fall durch den Kindergeldberechtigten erfolgen muss. Entscheidend ist nur, dass die von Amts wegen ermittelnde Familienkasse letztlich über den steuerlich maßgeblichen Sachverhalt unterrichtet wird. Wenn das erwachsene Kind oder dessen Ehepartner nicht damit einverstanden sind, dass der Kindergeldberechtigte durch die Eintragung in das Antragsformular Kenntnis über deren Einkommensverhältnisse erhält, reicht es aus, wenn das im übrigen nach § 68 Abs. 1 Satz 2 EStG ebenfalls zur Aufklärung des Sachverhalts verpflichtete Kind oder sein Ehepartner die Familienkasse entsprechend unterrichtet.

Das BMF hatte mir daraufhin zunächst mitgeteilt, dass keine Bedenken bestehen, wenn der Kindergeldberechtigte und sein Kind oder dessen Ehepartner die notwendigen Angaben gegenüber der Familienkasse getrennt machen. Dies bedeutet, dass das Kind oder dessen Ehepartner die Angaben entweder dem Kindergeldberechtigten in einem verschlossenen Umschlag zur Weiterleitung an die Familienkasse übergeben können oder dass sie ihre Angaben der Familienkasse unmittelbar zuleiten. Auf mein weiteres Drängen hin, dass die Kindergeldberechtigten über diese Möglichkeit aber auch unterrichtet werden müssten, hat mir das BfF schließlich mitgeteilt, es sei geplant, bei der für das Jahr 2001 vorgesehenen nächsten Überarbeitung des Kindergeld-Merkblattes einen entsprechenden Hinweis aufzunehmen, womit eine gute Lösung gefunden ist.

7.6 Auskunft durch das Bundesamt für Finanzen über Freistellungsaufträge

7.6.1 Gilt § 19 BDSG? – Das ist hier die ungelöste Frage

In meinem 17. TB (Nr. 7.1) konnte ich berichten, dass das BfF nach meinen eingehenden Bemühungen aufgrund eines entsprechenden Erlasses des BMF den Auftraggebern von Freistellungsaufträgen Auskunft über ihre dort gespeicherten Daten erteilt, wenn ein berechtigtes Interesse an der Auskunft gegeben ist und kein Versagungsgrund vorliegt. Diese Regelung hatte dazu geführt, dass das BfF nahezu ausnahmslos Auskunft erteilte.

Diese Situation hat sich jedoch geändert, seit die zur Mitteilung der Daten über den Freistellungsauftrag verpflichteten Kreditinstitute und sonstigen Stellen nach einer Änderung des § 45d EStG – erstmals für 1998 – nicht mehr die Rahmen der erteilten Freistellungsaufträge, sondern die tatsächlich aufgrund eines Freistellungsauftrags freigestellten Zinsen an das BfF melden müssen. Auf diese Weise kann das BfF bereits selbst feststellen, ob sich diese Beträge innerhalb der Grenzen der steuerlichen Freibeträge halten oder diese überschreiten. Im Gegensatz zu dem bisherigen Verfahren wird hierdurch vermieden, dass das BfF unnötigerweise Finanzämter wegen Überschreitens des erlaubten Rahmens für Freistellungsaufträge unterrichtet und Steuerpflichtige zu Unrecht in den Verdacht geraten, die zulässigen Freigrenzen überschritten zu haben, obwohl überhaupt keine Zinsen über die erlaubte Höhe hinaus angefallen waren.

So sinnvoll die Änderung über die zu meldenden Daten aus den Freistellungsaufträgen für die Ausgestaltung des Kontrollverfahrens ist, so bedauerlich ist die gewandelte Auffassung des BfF, wonach ein *berechtigtes Interesse* an einer Auskunft jetzt grundsätzlich nicht mehr vorliegt. Da man in der Regel wisse, wo man ein Guthabenkonto habe und da die Höhe der Zinsen dem Kontoauszug zu entnehmen sei, könne ein berechtigtes Interesse nur in Ausnahmefällen anerkannt werden, z. B. wenn ein Erbe durch eine Anfrage erfahren will, ob und gegebenenfalls wo ein Erblasser Konten unterhalten hat.

Bisher habe ich vergeblich versucht, das BMF und das BfF davon zu überzeugen, dass ein berechtigtes Interesse an der Auskunft überhaupt nicht gefordert werden darf, da § 19 BDSG diese Voraussetzung nicht kennt. Das BMF geht allerdings davon aus, dass § 19 BDSG vom BfF nicht angewandt zu werden braucht.

Außerdem macht das BfF jetzt geltend, würde eine Auskunft erteilt, würde der mit dem Verfahren nach § 45d EStG beabsichtigte *Kontrollzweck* gefährdet. Angesichts der großen Menge gemeldeter Daten sei es im Hinblick auf mögliche Übertragungsfehler der meldenden Stellen aus den schriftlich erteilten Freistellungsaufträgen und auch weil programmtechnische Gründe es im Einzelfall erschweren könnten, alle Daten einer Person zusammenzuführen, nicht möglich zu garantieren, dass die Kontrollmitteilungen an die Finanzämter oder die Auskünfte an den Betroffenen oder an andere Behörden stets vollständig sind. Der einzig erkennbare Grund, die beim BfF gespeicherten Daten über Freistellungsaufträge zu erfragen, sei daher zu erfahren, ob es notwendig ist, insoweit gegenüber einer Behörde wahrheitsgemäße Angaben zu machen, weil Falschangaben gegebenenfalls durch Mitteilungen des BfF aufgedeckt werden könnten. Das BfF befürchtet, mit einer Auskunft unter Umständen sogar Beihilfe zur Steuerhinterziehung oder zum Sozialbetrug zu leisten. Der Kontrollzweck könne nur dann erreicht werden, wenn für den Betroffenen unklar bleibe, ob dem BfF tatsächlich alle freigestellten Beträge bekannt sind.

Ich schließe zwar nicht aus, dass es Bürger gibt, die beim BfF wegen ihrer Freistellungsaufträge nachfragen, um abzuschätzen, ob es notwendig ist, gegenüber einer bestimmten Behörde hierzu wahrheitsgemäße Angaben zu machen. Insoweit habe ich durchaus Verständnis für die Position des BfF. Dennoch kann man nicht davon ausgehen, dass jeder, der wegen seiner Freistellungsaufträge beim BfF nachfragt, unredliche Absichten verfolgt.

Das Problem der Auskunftserteilung durch das BfF wird einen Schwerpunkt der mit dem BMF aufgenommenen Gespräche über die Berücksichtigung datenschutzrechtlicher Belange in der Abgabenordnung bilden und dort noch eingehend zu erörtern sein (s.o. Nr. 7.2).

7.6.2 Eine falsche Verdächtigung und ihre Folgen

Wegen unzutreffender Mitteilung eines Freistellungsauftrags an das BfF hatte sich ein Petent an mich gewandt. Meine Nachforschungen ergaben, dass die Bundesschuldenverwaltung aufgrund eines Programmfehlers für das Jahr 1996 einen Freistellungsauftrag des Petenten über 6 100 DM an das BfF gemeldet hatte, obwohl dieser für Vorjahre erteilte Auftrag nicht mehr bestand. Zusammen mit einer weiteren – korrekten – Meldung einer Bank über einen Freistellungsauftrag des Petenten ebenfalls über 6 100 DM führte dies dazu, dass das BfF das für den Petenten zuständige Finanzamt benachrichtigte, damit es klärt, ob der Petent die für ihn geltende Höchstgrenze für Freistellungen von 6 100 DM überschritten hatte.

Das Finanzamt wählte in dem an den Petenten gerichteten Schreiben die wenig glückliche Formulierung, vom BfF sei *„festgestellt“* worden, dass *„für 1996 höhere Freistellungsaufträge als gesetzlich zulässig erteilt wurden“*. Damit wurde der Petent von seinem Finanzamt zu Unrecht verdächtigt, seine Freistellungsaufträge nicht im Rahmen der gesetzlichen Freistellungsgrenzen erteilt zu haben. Über die in der Formulierung des Finanzamts liegende – vom BfF nicht zu vertretende – Verdächtigung hinaus war der Petent durch die mangelhafte Datenverarbeitung bei der Bundesschuldenverwaltung weitergehend in eine missliche Lage geraten, da das BfF sich damals (November 1998; s. 17. TB Nr. 7.1) zunächst noch geweigert hatte, Anfragen von Freistellungsauftraggebern zu beantworten. Der Petent hätte hiernach nicht die Möglichkeit gehabt, durch eine Anfrage beim BfF Kenntnis über die dortigen, ihn betreffenden unrichtigen Daten zu erhalten. Ebenso wenig hätte er gegenüber dem BfF eine Berichtigung dieser Daten erreichen können. Auf entsprechende Anfragen in anderen Fällen hatte das BfF stets mitgeteilt,

eine Berichtigung müsse von der meldenden Stelle veranlasst werden. Die Bundesschuldenverwaltung selbst hatte es jedoch als meldende Stelle nicht für nötig gehalten, von sich aus für eine Korrektur der von ihr unzutreffend übermittelten und infolgedessen vom BfF falsch gespeicherten Daten zu sorgen.

Nachdem es außerdem bereits einige Jahre zuvor bei der Bundesschuldenverwaltung infolge fehlerhafter Datenverarbeitung zu nicht unerheblichen Datenschutzverstößen gekommen war, habe ich diese erneute schwerwiegende Persönlichkeitsverletzung beanstandet. Das BMF hat mir hierzu geantwortet, der Programmfehler sei inzwischen behoben.

7.7 Steuerliche Fahrtenbücher – praktikabler Kompromiss

In meinem 17. TB (Nr. 7.2) hatte ich über die damalige Forderung des BMF berichtet, dass Ärzte bei der Führung eines steuerlichen Fahrtenbuchs nach § 6 Abs. 1 Nr. 4 Satz 3 EStG darin die Namen und Anschriften der von ihnen aufgesuchten Patienten eintragen sollen. Ich hatte diese Forderung beanstandet, da sie nach meiner Auffassung nicht mit dem im Hinblick auf die ärztliche Schweigepflicht in § 102 Abs. 1 Nr. 3 Buchstabe c AO festgelegten Auskunftsverweigerungsrecht vereinbar ist. Die Gespräche mit dem BMF hatten allerdings schon seinerzeit eine pragmatische Lösung erwarten lassen.

Das BMF vertritt zwar nach wie vor die Auffassung, § 102 Abs. 1 Nr. 3 Buchstabe c AO gebe Ärzten, die ein Fahrtenbuch führen, um steuerliche Nachteile zu vermeiden, kein Recht, die Angabe der Namen und Anschriften der mit dem Kraftfahrzeug aufgesuchten Patienten gegenüber dem Finanzamt zu verweigern, wenn es diese verlangt. Dennoch gestattet das BMF nunmehr, dass in dem Fahrtenbuch selbst – wie bereits früher – nur *„Patientenbesuch“* vermerkt wird (vgl. 16. TB Nr. 7.3). Dies gilt allerdings nur, wenn die Namen und Anschriften dieser Patienten in einem hiervon getrennt zu führenden Verzeichnis festgehalten werden. Dessen Vorlage soll nur verlangt werden, wenn tatsächliche Anhaltspunkte für Zweifel an der Richtigkeit und Vollständigkeit der Eintragungen im Fahrtenbuch vorliegen und diese sich nicht anders ausräumen lassen. Wenn ein Arzt sich weigert, das von ihm angeforderte Verzeichnis vorzulegen, wird das Finanzamt dessen Herausgabe – wie das BMF insoweit erklärt hat – erfahrungsgemäß nicht mit Zwangsmitteln zu erreichen versuchen. Es wird vielmehr den privaten Nutzungswert des Kraftfahrzeugs pauschal ansetzen. Bei dieser Lösung hat letztlich das Finanzgericht im Rahmen einer möglichen gerichtlichen Überprüfung des Steuerbescheides über die Reichweite des Auskunftsverweigerungsrechts des Arztes nach § 102 Abs. 1 Nr. 3 Buchstabe c AO zu entscheiden.

Die Rechtsfrage, welche Befugnisse das in der Abgabenordnung festgelegte Auskunftsverweigerungsrecht dem Arzt gegenüber dem Finanzamt einräumt, konnte damit zwar nicht einvernehmlich gelöst werden. Dadurch, dass sie im Verfahrensablauf weiter „nach hinten“ verlegt wurde, dürfte sie aber weitaus seltener praktisch werden. Insgesamt sehe ich in dem jetzigen Verfahren einen brauchbaren Kompromiss, der es trotz weiterhin unterschiedlicher Rechtsauffassungen jedenfalls in der Praxis ermöglicht, die Belange des Datenschutzes angemessen zu berücksichtigen.

7.8 Hauptzollamt ermittelt jenseits seiner Zuständigkeiten

Eine Petentin hat mich auf folgenden Sachverhalt aufmerksam gemacht: Eine Handwerkskammer wandte sich in Form eines Amtshilfeersuchens an ein Hauptzollamt wegen des Verdachts der unzulässigen Handwerksausübung eines Unternehmens. Daraufhin wurde das Hauptzollamt in der Form tätig, dass es seine weitreichenden Prüfungsbefugnisse nach den §§ 304 SGB III, 107 SGB IV, wie Zugangsrechte zu Geschäftsräumen zu prüfender Unternehmen und Einsichtsrechte in deren Geschäftsräume, dazu benutzte, die Baustelle dieses Unternehmens zu überprüfen (zur Außenprüfung der Hauptzoll- und Arbeitsämter nach den §§ 304 SGB III, 107 SGB IV, s. u. Nr. 20.1). Die Voraussetzungen der §§ 304 SGB III, 107 SGB IV waren jedoch nicht gegeben, da weder der Verdacht eines Leistungsmissbrauchs noch der einer unzulässigen Beschäftigung ausländischer Arbeitnehmer vorlag. Weiterhin bestand auch kein Anhaltspunkt für eine Verletzung von Meldepflichten nach dem SGB IV oder für einen Verstoß nach dem Arbeitnehmer-Entsendegesetz.

Der Gesetzgeber hat durch die vorgenannten Regelungen des Sozialgesetzbuches aufgrund wichtiger Interessen der Allgemeinheit tief in das Recht auf informationelle Selbstbestimmung und weitere Grundrechte, wie z. B. in das auf Unverletzlichkeit der Wohnung nach Art. 13 GG, eingegriffen. Diese Einschränkungen sind für den Bürger jedoch nur bei Vorliegen der entsprechenden gesetzlichen Voraussetzungen hinzunehmen. Im vorliegenden Fall war die Datenerhebung und damit der Eingriff in die Grundrechte der Betroffenen unzulässig, da die Prüfung einem anderen als dem gesetzlich vorgesehenen Zweck diente. Diesen Verstoß gegen das Datenschutzrecht habe ich gegenüber dem BMF beanstandet. Auch dessen nachgeschobene Begründung eines präventiven Tätigwerdens im originären Prüfbereich des Hauptzollamtes konnte in Anbetracht des vorliegenden Amtshilfeersuchens der Handwerkskammer nicht überzeugen.

Das sieht mittlerweile auch das BMF so. Es hat den Vorfall zum Anlass genommen, die entsprechenden Arbeitsbereiche der Hauptzollämter durch einen Erlass auf die besondere datenschutzrechtliche Relevanz gleich oder ähnlich gelagerter Geschäftsvorfälle hinzuweisen.

7.9 Software für das künftige EG-Zollinformationssystem – EG-ZIS – korrekturbedürftig

Auf der Grundlage der Verordnung (EG) Nr. 515/97 des Rates vom 13. März 1997 über die gegenseitige Amtshilfe

zwischen den Verwaltungsbehörden der Mitgliedstaaten und die Zusammenarbeit dieser Behörden mit der Kommission im Hinblick auf die ordnungsgemäße Anwendung der Zoll- und Agrarregelung, der sog. EG-Amtshilfeverordnung (14. TB S. 57; 15. TB Nr. 5.6; 16. TB Nr. 35, dort Nr. 4) soll das EG-Zollinformationssystem – EG-ZIS – eingerichtet werden. Zweck dieser den Mitgliedstaaten und der Kommission zugänglichen Datenbank soll nach Art. 23 Abs. 2 EG-Amtshilfeverordnung sein, *„die Verhinderung, Ermittlung und Bekämpfung von Handlungen, die der Zoll- oder der Agrarregelung zuwiderlaufen, zu unterstützen und hierfür durch eine raschere Verbreitung von Informationen die Effizienz von Kooperations- und Kontrollmaßnahmen der zuständigen Behörden im Sinne dieser Verordnung zu steigern“*.

Die EG-Amtshilfeverordnung legt im Einzelnen fest, dass personenbezogene Daten nur für die Kategorien *„Waren“, „Transportmittel“, „Unternehmen“* und *„Personen“* gespeichert werden dürfen. Auch bestimmt sie die Art der personenbezogenen Daten, die aufgenommen werden dürfen, so vor allem Name, Geburtsname, Vorname und angenommene Namen, Geburtsdatum und Geburtsort, Staatsangehörigkeit, amtliches Kennzeichen des Transportmittels sowie vorgeschlagene Maßnahmen durch eine zuständige Behörde eines Mitgliedstaates. Nach ihrem Art. 27 Abs. 1, der nach dem Vorbild des Art. 99 Abs. 1 SDÜ verfasst wurde, dürfen Daten der genannten Kategorien *„nur zum Zweck der Feststellung und Unterrichtung, der verdeckten Registrierung oder der gezielten Kontrolle“* in das EG-ZIS aufgenommen werden. Damit wird das EG-ZIS der Sache nach als **Ausschreibungsdatei** gekennzeichnet.

Bei einer Speicherung zum Zweck einer *gezielten Kontrolle* soll beispielsweise einem deutschen Zollbeamten an einer EG-Außengrenze ermöglicht werden, festzustellen, ob ein anderer Mitgliedstaat das Kraftfahrzeugkennzeichen eines Lkw im EG-ZIS gespeichert hat, dessen Fahrer gerade einen Zollantrag vorlegt. Ist dies der Fall, kann der deutsche Zollbeamte aus dem EG-ZIS entnehmen, dass z. B. die niederländische Zollverwaltung eine gezielte Überprüfung der mitgeführten Warenmenge erbeten hat. Dann führt er die erforderliche Kontrolle durch, stellt möglicherweise eine nicht angemeldete Mindermenge an Waren fest und unterrichtet hierüber die ersuchende Zollverwaltung. Bei einer *verdeckten Registrierung* sollen die Feststellungen unauffällig getroffen werden.

Andere Mitgliedstaaten und die Kommission halten Speicherungen für andere Zwecke als „Ausschreibung“, wie z. B. auch für einen spontanen Informationsaustausch, für zulässig. So wird derzeit bereits in den EG-Mitgliedstaaten ein von der Kommission an diese verteiltes Software-Programm erprobt, das es u. a. ermöglicht, komplexe Sachverhalte bildlich darzustellen und Querverbindungen zu anderen Sachverhalten aufzuzeigen. Damit können zusätzliche Informationen über bereits abgeschlossene und laufende Fälle von Unregelmäßigkeiten in das EG-ZIS eingegeben werden, die gegebenenfalls auch für andere Zollstellen nützlich sind.

Die Bundesregierung wendet sich nicht dagegen, dass den Mitgliedstaaten solche weitergehenden Informationen zur Verfügung gestellt werden, soweit dies erforderlich und angemessen ist. Nur sieht sie in der EG-Amtshilfeverordnung hierfür zu Recht keine ausreichende Rechtsgrundlage. Sie hat ihre rechtlichen Bedenken zuletzt im Dezember 1999 in einem mit mir abgestimmten Schreiben an die Europäische Kommission und an alle Mitgliedstaaten geäußert. Die Frage, in welchem Umfang die EG-Amtshilfeverordnung Datenspeicherungen zulässt, muss geklärt werden, nicht zuletzt auch, weil jeder ZIS-Partner für die Rechtmäßigkeit der Dateneingabe verantwortlich ist. Für die eingebenden Stellen muss ersichtlich sein, welche Daten sie für welche Zwecke eingeben dürfen, ohne das Persönlichkeitsrecht der Betroffenen zu verletzen.

Einige Mitgliedstaaten teilen grundsätzlich die deutschen Überlegungen. Die Kommission beabsichtigt, die Arbeiten, die sich aus kommissionsinternen Gründen verzögert haben, nunmehr beschleunigt voranzubringen.

8 Wirtschaft und Informationsgesellschaft

8.1 Novellierung des Teledienstedatenschutzgesetzes

Das Teledienstedatenschutzgesetz (TDDSG) aus dem Jahr 1997 hat seine erste Bewährungsprobe bestanden. Die Evaluierung, die mit Inkrafttreten des Gesetzes begann und im Juni 1999 mit einem Evaluierungsbericht der Bundesregierung an den Deutschen Bundestag (BT-Drs. 14/1191) abgeschlossen wurde, hat jedoch ergeben, dass das TDDSG aufgrund der Erfahrungen und Entwicklungen präzisiert und angepasst werden muss. Ein weitgehend abgestimmter Novellierungsentwurf (Stand: Dezember 2000) liegt inzwischen vor.

8.1.1 Klarstellungen und Ergänzungen

Die vorgenommenen Änderungen betreffen im wesentlichen Konkretisierungen und Klarstellungen, die für eine bessere Handhabung in der Praxis der Aufsichtsbehörden sorgen sollen. Denn in einigen Fällen hatten die Formulierungen des TDDSG einen nicht gewollten Auslegungsspielraum eröffnet und dadurch zu Rechtsunsicherheiten geführt. So wird im Entwurf der Geltungsbereich dahingehend konkretisiert, dass das TDDSG nur im Verhältnis von Anbietern und natürlichen Personen als Nutzern von Telediensten gilt und somit z. B. die Verarbeitung personenbezogener Daten, die zu ausschließlich beruflichen Zwecken innerhalb eines Arbeitsverhältnisses erfolgt, nicht erfasst wird. Weiterhin wird durch entsprechende Änderungen klargestellt, dass sich die Einwilligung des Nutzers als Erlaubnistatbestand für eine weitergehende Verarbeitung auch auf seine Nutzungsdaten bezieht.

Ergänzt werden die bestehenden Vorschriften außerdem um Regelungen für den Fall einer missbräuchlichen Nutzung von Telediensten und um Sanktionsmöglichkeiten bei Pflichtverletzungen durch den Teledienstean-bieter. So sind Befugnisse zum Speichern von Nutzungsdaten im Einzelfall vorgesehen, um dem Anbieter die Aufklärung und Rechtsverfolgung eines vermuteten Missbrauchs zu ermöglichen. Der Bußgeldkatalog des Entwurfs, der noch an den des neuen BDSG angepasst werden soll, muss aus meiner Sicht aber auch noch auf einige materiell-rechtliche Bereiche des TDDSG ausgedehnt werden. Damit gäbe man den Aufsichtsbehörden ein Instrument an die Hand, das der Umsetzung des TDDSG durch die Dienste-anbieter den erforderlichen Nachdruck verleiht, was nach den Erfahrungen geboten ist (s. u. Nr. 8.2).

Die Novellierung des TDDSG verfolgt als weiteres Ziel, mehr Transparenz zu schaffen und diese bereichsspezifische Regelung so mit dem allgemeinen Datenschutzrecht abzustimmen, dass sie die allgemein geltenden Vorschriften des BDSG lediglich durch Spezialregelungen für den Bereich der Teledienste ergänzt bzw. modifiziert. So werden im Rahmen der Novellierung des BDSG die bisher im TDDSG verankerten Grundsätze der Datenvermeidung und -sparsamkeit in das BDSG aufgenommen, weshalb sie im TDDSG nicht mehr erwähnt werden sollen. Dasselbe gilt für die anlassfreie Kontrolle durch die Aufsichtsbehörden. Ob der „normale“ Anwender die Tranzparenz, die durch diese Systematisierung angestrebt ist, auch wirklich durchschaut, wird sich erst in der Praxis erweisen.

8.1.2 Vertrauen schaffen: Audit für E-Commerce

Dass die Transparenz dort an ihre Grenze stößt, wo die Grenze zwischen Online- und Offline-Welt verwischt oder besser gesagt: nicht für jeden verständlich und nachvollziehbar verläuft, zeigen die Praktiken von Internet-Kaufhäusern, die vor allem im Jahr 2000 die Nutzer verunsichert haben. Macht nämlich ein Nutzer von der Online-Bestellmöglichkeit eines solchen Kaufhauses Gebrauch, so gilt für die Daten, die im Online-Teil dieses Handels beim Versenden des Bestellformulars anfallen, das strenge TDDSG, das die Weitergabe dieser Nutzungsdaten an Dritte verbietet. Die Daten der Bestellung selbst, d. h. die Lieferadresse und die Bezeichnung der bestellten Ware, fallen unter das weniger strenge BDSG. Denn diese Daten sind für die Abwicklung des Handels außerhalb der Online-Welt – für die korrekte Zulieferung – erforderlich. Hierfür erlaubt das BDSG die Weitergabe für Werbezwecke, solange der Kunde dem nicht ausdrücklich widersprochen hat.

Weil der Verbraucher das Einkaufen über das Internet aber oft als einen einheitlichen Dienst ansieht, wird er auch eine beruhigende Zusicherung von Vertraulichkeit auf den gesamten Vorgang – von der Online-Bestellung bis zur Auslieferung der gewünschten Ware bei ihm zu Hause – beziehen. Und weil auch meistens verschwiegen wird, dass diese Zusicherung nur für den Online-Teil des Handels gemeint ist, sieht der Kunde keinen Anlass, der weiteren Verwendung seiner Daten zu widersprechen. Der Täuschung folgt dann die Enttäuschung, wenn er die nicht erwartete Nutzung seiner Daten dadurch bemerkt, dass er Direktwerbung erhält. Der damit erzeugte Vertrauensschaden trifft nachher nicht nur die Anbieter, die solche Verfahren praktizieren, sondern den gesamten Bereich des E-Commerce.

Hier kann ein Datenschutzaudit abhelfen, das die Redlichkeit der gegenüber dem Kunden abgegebenen Erklärungen nicht am gesetzlichen Minimum misst, sondern am Verständnis der Kunden.

Dass die rechtliche Grundlage für ein freiwilliges Datenschutzaudit (vgl. 17. TB Nr. 8.1) nicht im TDDSG, sondern durch eine entsprechende Vorschrift im neuen BDSG geschaffen wird, belegt zweierlei: ein solches Instrument wird nicht nur im Internet, sondern auch in vielen anderen Bereichen als wirksames Mittel zur Förderung des Datenschutzes angesehen, und gesetzliche Rahmenbedingungen als ordnende Hand im Dschungel der vielfältigen Selbstregulierungsaktivitäten im Internet sind dringend erforderlich. Denn derweil sind deren Art und Anzahl kaum überschaubar. Vor allem für den Bereich des E-Commerce werden Gütesiegel angeboten, die dem Verbraucherschutz insgesamt dienen sollen und somit die Einhaltung von Datenschutz-Mindeststandards nur als eine von vielen „Eigenschaften“ eines Online Shops bestätigen. Beispielhaft seien hier nur *Trusted Site* des TÜViT (www.trusted-site.de), *Geprüfter Online Shop* des Europäischen Handelsinstituts (www.shopinfo.net) und *Trusted Shops* des Gerling-Konzerns (www.trusted-shops.de) genannt.

Da bei solchen Siegeln die Aussage zur überprüften Qualität auf ein entsprechendes Logo reduziert ist, benötigt man eine gesetzliche Garantie als wesentlichen vertrauensbildenden Faktor. Im Interesse der Nutzer und zur Förderung des – immer noch erhofften – Wachstums des neuen Marktes erscheint es mir daher umso wichtiger, möglichst zeitnah zur Novellierung des BDSG auch Rahmenbedingungen für ein Datenschutzaudit festzulegen.

Ich unterstütze ein Audit, das anhand von definierten Kriterien und Verfahren die Datenschutzkonzepte und deren praktische Umsetzung bei den Unternehmen prüft, wobei praktische Umsetzung hier sowohl die organisatorischen als auch die technischen Maßnahmen meint. Und damit das durch Audit und Gütesiegel dem Nutzer gegebene Versprechen auch wirklich Vertrauen bildet und erhält, muss der Bruch dieses Versprechens spürbar sanktioniert sein. Benötigt wird deshalb u. a. eine Vorschrift wie: „Wer personenbezogene Daten anders verarbeitet, als er es versprochen hat, handelt rechtswidrig.“

Zu wünschen wäre, dass ein solches Modell Schule macht und von anderen Ländern übernommen wird. Wenn dann auch noch die Vergleichbarkeit der Ergebnisse sichergestellt wird, d. h. die Aussage der Gütesiegel sich an gemeinsamen Kriterien orientiert, könnte so ein einheitliches Datenschutzniveau im globalen Netz erreicht werden.

8.2 ... und nun endlich erwacht?

Eigentlich hätte man erwarten können, dass das Teledienstedatenschutzgesetz inzwischen allseits bekannt ist und von denen, die es verpflichtet, auch umgesetzt wird. Vor allem weil kein Tag vergeht, an dem nicht in den Druckmedien zum Thema Internet geschrieben und auch oft auf die dort vorhandenen Probleme und Risiken hingewiesen wird. Und oft genug wird auch das Teledienstedatenschutzgesetz erwähnt. Aber offensichtlich hinterlassen nicht einmal die Berichte über Vorbehalte der Internet-Nutzer, die sich zu einem großen Teil auf Defizite im Bereich des Datenschutzes zurückführen lassen, keinen so bleibenden Eindruck bei den Providern, dass sie Veränderungen initiieren. Mit anderen Worten: zu wenige der Provider ziehen den folgerichtigen Schluss, dass ihr Angebot für die Nutzer auch und vor allem durch den Qualitätsfaktor Datenschutz – im wahrsten Sinne des Wortes – anziehend wird.

Der Eindruck auf Seiten der Nutzer muss hingegen bleibend schlecht sein:

- Datenschutzerklärungen im Sinne einer *privacy policy* sind selten. Wenn die oft mühselige Suche nach einem Hinweis auf den Datenschutz jedoch mal erfolgreich ist, dann findet man ihn versteckt in den AGB, oft inhaltlich sehr dürftig oder allgemein, oft mit einem Verweis auf die „falsche" Rechtsgrundlage.
- Eine Unterrichtung der Nutzer über den Umfang und Zweck der Datenerhebung, -verarbeitung und -nutzung durch Zugangsprovider, die eine Online-Anmeldung vorsehen, ist ebenso selten. Die Vermutung liegt nahe, dass diese Verpflichtung durch die genannten allgemeinen Hinweise auf „Konformität mit den Datenschutzgesetzen" als erledigt angesehen wird.
- Dem Grundsatz der Datenvermeidung wird oft dadurch „gefolgt", dass in Anmelde- oder Bestellformularen die Felder für Angaben, die über das Erforderliche hinausgehen, unauffällig als optional gekennzeichnet werden.
- Angaben zum Anbieter (Name, Adresse) sind vielfach schwer zu finden, unvollständig oder in einigen Fällen gar nicht vorhanden – auch trotz der „Konvention zur Anbieterkennzeichnung", der sich mehrere Verbände angeschlossen haben. So ist der Name im Logo der Website oft der einzige und wenig hilfreiche Hinweis auf die Identität des Anbieters. Die im Teledienstegesetz festgeschriebene „Impressumspflicht" wirkt als Beitrag zur Transparenz für den Verbraucher – gerade auch im Bereich des Datenschutzes – aber nur dann vertrauensbildend, wenn man sie befolgt.

Was nun meinen Eindruck angeht: nach zwei weiteren Jahren ist die Bilanz enttäuschend! Trotz der von den Aufsichtsbehörden durchgeführten Kontrollen der Provider, die allerdings aufgrund fehlender Personalkapazitäten oftmals – anders als im TDDSG vorgesehen – nur anlassbezogen vorgenommen werden, ist eine „flächendeckende" Änderung der schon in meinem 17. TB (Nr. 8.2.1) dargestellten Situation bisher nicht erkennbar. Angesichts der Vielzahl der Provider – und jeden Tag werden es mehr – käme die Überprüfung jedes einzelnen Providers zudem wohl einer Sisyphusarbeit gleich.

Offensichtlich müssen verstärkt auch andere Wege gewählt werden, die Provider und Nutzer gleichermaßen erreichen. Ein Weg ist eine breitere Öffentlichkeitsarbeit mit dem Ziel der Sensibilisierung, die ja durch die Präsenz der Datenschutzbehörden im Internet schon begonnen wurde. Dort sind mittlerweile Anleitungen für Datenschutzerklärungen und Orientierungshilfen für Provider und Nutzer verfügbar. Einen wesentlichen Beitrag wird sicherlich auch das Datenschutz-Portal „Virtuelles Datenschutzbüro" leisten, das deutsche und einige ausländische Datenschutzbeauftragte gemeinsam seit Anfang Dezember 2000 anbieten (s. u. Nr. 33.2). Hier können sich Interessierte informieren und in Diskussionsforen über aktuelle Datenschutzthemen zur Entwicklung beitragen.

Eine weitreichende Sensibilisierung der Provider für die Belange des Datenschutzes wird wohl in vielen Fällen auch auf dem „Umweg" über die Nutzer erfolgen müssen, d. h. die Nutzer können durch ihr Verhalten die Provider „auf den richtigen Weg bringen". Wenn sich nichts ändert, dann dürfte es bei der Diskrepanz zwischen Wunsch und Wirklichkeit im E-Commerce bleiben, die durch die Weigerung der Nutzer entsteht, sich in eine – virtuelle – Welt zu begeben, wo der Schutz ihrer Daten noch nicht Normalität ist.

8.3 Diskret indiskret: die andere Informationssuche im Internet

Mit personenbezogenen Daten lässt sich Geld machen. Das ist in der realen Welt hinlänglich bekannt und wird entsprechend praktiziert. Und dass das Internet – wegen der zahlreichen Informationen, die jeder Nutzer im Netz hinterlässt, wenn er dort für ihn interessante Informationen sucht – eine ergiebige Fundgrube für Nutzerdaten sein kann, liegt eigentlich auf der Hand. Dennoch ist der Trend, die kommerziellen Angebote im Internet durch personalisierte Werbung zu finanzieren, unerwartet. War man doch noch bei der Entstehung des TDDSG davon ausgegangen, dass die Finanzierung auf herkömmlichem Weg – durch eine Nutzungsgebühr für einzelne Angebote in „harter" Währung – erfolgen würde oder allenfalls durch das Einblenden von Anzeigen, die für alle Nutzer gleich sind.

Weil die auf den jeweiligen Nutzer zugeschnittene Werbung, das sog. One-to-One-Marketing, besonders erfolgsträchtig ist, macht die Online-Werbebranche sich die sowieso vorhandenen Nutzungsdaten, die des Surfers Interessen und Vorlieben widerspiegeln, zunutze: sie werden ausgewertet und zu seinem Profil zusammengeführt. So hat sich das Datensammeln als Voraussetzung für die Plazierung von „passenden" Werbebannern als eigenständiges Gewerbe im Internet entwickelt, wogegen – zumindest prinzipiell – nichts einzuwenden ist. Leider lässt aber die Art und Weise, in der man sich unaufgefordert Eintritt in die Privatsphäre des Nutzers verschafft, nicht nur die eigentlich gebotene Zurückhaltung vermissen, sondern diese Indiskretion geht in vielen Fällen auch sehr diskret vonstatten, denn *„sie* [die Kunden] *wollen nicht das Ge-*

fühl haben, durchschaut zu werden", wie kürzlich aus der Branche zu vernehmen war. Diese Erklärung kann aber wohl kaum die Heimlichkeit rechtfertigen, in der man Nutzer mit Hilfe von *cookies* und *web-bugs* ausforscht oder das Herunterladen von Daten an den Hersteller des benutzten Multimedia-Programms melden lässt. Vor allem nicht, wenn man ihr die Ergebnisse aus Nutzer-Umfragen gegenüberstellt, die belegen, dass die nur verhaltene Teilnahme am E-Commerce in erheblichem Maße auf ein Defizit in der Vertrauensdisziplin „Datenschutz" zurückzuführen ist.

Möglicherweise macht eben wegen des von vielen Bürgern geäußerten Unbehagens in den USA die Strategie des *marketing by permission* Schule, die ganz bewusst auf eine offene Handhabung setzt, indem sie dem Kunden die Entscheidung über das Ob und Wie der Verwendung seiner Daten für Werbezwecke überlässt, und sich so – das sollte kaum überraschen – zur erfolgreichsten Form des Marketing entwickelt hat. Wenn sich dort jetzt noch die Erkenntnis durchsetzt, dass man sich an die Entscheidung des Kunden und damit an sein eigenes Versprechen stets halten muss, wird der Erfolg nicht nur dauerhaft, sondern auch noch größer werden.

Diese Strategie entspricht den Vorschriften des TDDSG und geht sogar, soweit unter Pseudonym erstellte Nutzerprofile verwendet werden, darüber hinaus. Zu hoffen ist, dass das novellierte Gesetz durch die klarstellenden Formulierungen auch an dieser Stelle die nötige Transparenz vor allem für die „Datensammler" schafft. Fraglich bleibt aber, ob die bestehenden Vorschriften auch weitere noch nicht abzusehende, aber im Interesse der Nutzer zu richtende Entwicklungen in diesem Bereich abdecken können. Deshalb habe ich mich beim Bundestagsausschuss für Wirtschaft und Technologie dafür eingesetzt, dass die Erfahrungen im Zusammenhang mit der Anwendung und Umsetzung des TDDSG weiterhin beobachtet und in einem erneuten Evaluierungsbericht der Bundesregierung vorgestellt werden. Hierzu lag bis Redaktionsschluss noch kein Votum des Ausschusses vor.

8.4 Auf dem Prüfstand: Zahlungssysteme im Internet

Keines der im Markt angebotenen Systeme für die Bezahlung im Internet hat sich bis heute durchsetzen können. Auch dem einzigen anonymen System *eCash*, über das ich in meinem 17. TB (Nr. 8.3) berichtet habe, blieb der große Durchbruch bisher versagt. Allerdings bieten ca. 50 Firmen über das *eCash*-Portal der Deutschen Bank auch die Bezahlung mit den digitalen Münzen an, und – anders als in der Pilotphase – wird *eCash* inzwischen zunehmend – auch vom „normalen" Nutzer – eingesetzt. Zur weiteren Akzeptanz und Verbreitung dieses datenschutzfreundlichen Systems kann sicherlich die Werbe-Kampagne beitragen, die an 18 deutschen Universitäten durchgeführt wurde und damit in einem Bereich angesetzt hat, in dem viele – technikoffene – Kunden zu gewinnen sind.

Aber noch ist alles beim alten: immer noch werden die konventionellen Zahlungsverfahren (Nachnahme, Lastschrift, Kreditkartenzahlung) im Netz verwendet, wobei aber – was ein gewisser Fortschritt ist – die Zahlungsinformationen zunehmend über eine sichere Verbindung (SSL) übertragen werden. Aber was nutzt das dem Nutzer, wenn der Empfänger der Daten ein Betrüger ist oder die Daten missbraucht!

Inzwischen werden auch Systeme angeboten, die solche konventionellen Verfahren mit anderen Kommunikationstechniken so kombinieren, dass keine Konto-Informationen über das Internet übertragen werden müssen:

Im Bezahlsystem *paybox* der Firma paybox.net wird der Zahlungsauftrag per Mobiltelefon erteilt. Nachdem der Händler den Kaufbetrag und die angegebene Mobiltelefonnummer an *paybox* übersandt hat, holt *paybox* durch einen automatischen Rückruf beim Nutzer die Bestätigung des Auftrags ein, wobei dieser durch Eingabe seiner persönlichen *paybox*-PIN ein Lastschriftverfahren „freischaltet". paybox.net zieht dann den Betrag vom Konto des Nutzers ein und leitet ihn an den Händler weiter. Dieses System wird auch in der „realen" Welt von mobilen Dienstleistern (z. B. Taxifahrern) eingesetzt.

Mit dem Verfahren *net900* der Deutschen Telekom AG kann das Abrufen kostenpflichtiger Inhalte im Internet über die Telefonrechnung bezahlt werden. Dabei trennt eine spezielle Software für kurze Zeit die bestehende Modemverbindung zum Internetanbieter und baut über eine 0190er-Rufnummer eine Verbindung zu den kostenpflichtigen Inhalten auf, über die diese Inhalte übertragen und „bezahlt" werden. Nach der Übertragung wird die ursprüngliche Verbindung zum Internetanbieter wieder hergestellt. *net900* eignet sich aber wohl eher für Kleinbeträge und ist von Rechnern ohne Modem (z. B. in Firmennetzen) oder außerhalb von Deutschland nicht einsetzbar.

Die Datenschutzbeauftragten werden sich eingehend mit der datenschutzrechtlichen Bewertung von Zahlungssystemen beschäftigen und die Anbieter verschiedener Systeme zu einer Anhörung im Februar 2001 einladen. Bei der Bewertung steht die Frage im Vordergrund, inwieweit ein System anonymes oder pseudonymes Bezahlen ermöglicht. Da aber nur ein sicheres System dies leisten kann, spielen auch die technischen Maßnahmen eine entscheidende Rolle, mit denen die Integrität und Verbindlichkeit und nicht zuletzt die Vertraulichkeit der Zahlungsvorgänge sichergestellt werden.

Eines lässt sich schon jetzt sagen: Auf Dauer werden sich gerade im Internet nur solche Systeme durchsetzen, die dem Nutzer – bei ausreichender Transparenz des Verfahrens – das sichere Gefühl geben, dass seine Daten in keinen oder zumindest in guten Händen sind.

8.5 Mit Kryptographie mehr Sicherheit

8.5.1 Es wird immer noch unzureichend verschlüsselt

Bei meinen Kontrollen musste ich leider feststellen, dass sogar bei hochsensiblen personenbezogenen Daten (z. B. Gesundheitsdaten) kein ausreichender Schutz gegen

unberechtigten Zugang zu den Daten vorhanden ist. Auch werden solche Daten nicht verschlüsselt. Die Daten werden in manchen Behörden zwar auf organisatorisch abgeschotteten Rechnern bearbeitet, die Sicherung der Daten erfolgt dann aber häufig auf einem zentralen Server, der in einem anderen Bereich bzw. Gebäude oder gar in einer anderen Liegenschaft steht. Dabei werden die Daten in der Regel von einem Anwender-PC über ein Local-Area-Network (LAN) oder eine ISDN-Leitung ungeschützt zum Server übertragen. Dort werden die Daten mit anderen, nicht personenbezogenen Daten auf einem Datenträger gesichert. In einem Fall wurde am PC zwar ein Zugriffsschutz durch den Einsatz von Wechselplatten geschaffen – die nach Dienstende in einem Tresor gesichert wurden –, allerdings war dieser Rechner auch über einen Netzanschluss mit einem zentralen Server in einer anderen Liegenschaft verbunden. Auf diesem Server erfolgte eine zusätzliche Datensicherung, die Daten wurden somit dort gespiegelt, eine Verschlüsselung der Daten erfolgte auch hier nicht.

Unverschlüsselte Daten können auf vielen Wegen in die Hände von unbefugten Personen gelangen. Dies gilt sowohl für Arbeiten in der Systemverwaltung, bei Wartungs- oder Reparaturarbeiten durch internes wie externes Personal – im Gewährleistungsfall werden eventuell sogar die Festplatten an die Herstellerfirma geschickt (vgl. dazu meine Hinweise im 17. TB Nr. 8.11) – als auch bei der Übertragung dieser Daten auf einem ungesicherten Übertragungsweg, zu dem auch die Telefon- und Datennetze gehören.

Hier sehe ich nach wie vor dringenden Handlungsbedarf. Kann durch geeignete Maßnahmen der Zugriff oder die Kenntnisnahme der mit der Systempflege beauftragten Personen auch ohne Verschlüsselung noch eingeschränkt werden, so ist bei der Datenübertragung vor allem besonders schützenswerter Daten Verschlüsselung zwingend notwendig.

Auch möchte ich auf die beim BSI entwickelte Verschlüsselungssoftware für PC „Chiasmus für Windows“ hinweisen. Damit ist es möglich, einzelne Dateien oder gesamte Verzeichnisse zu verschlüsseln. Da es sich hier um ein symmetrisches Verfahren handelt, eignet sich Chiasmus nur für kleine (feste) Nutzergruppen. Die notwendigen Schlüssel können vom Anwender selbst mit dem eingebauten Zufallsgenerator erzeugt werden; sie müssen anschließend auf einem sicheren Weg zum Kommunikationspartner transportiert werden. Des weiteren können Dateien mit Hilfe des Programms „physikalisch“ von der Festplatte gelöscht werden. Das heißt, es wird nicht nur der Eintrag aus dem Inhaltsverzeichnis gelöscht, sondern die Datei wird byteweise (mehrfach) überschrieben.

Die öffentliche Verwaltung kann Chiasmus für Windows beim BSI anfordern.

8.5.2 PGP „ganz schön sicher“?

Alle Daten, die im Klartext über das Internet transportiert werden, sind ungeschützt. Sie können beim Transport oder durch Zugriff auf Knotenrechner mitgelesen oder verfälscht werden. Der Absender weiß in der Regel nicht, welchen Weg seine Nachrichten nehmen und er hat auch keine Einflussmöglichkeit auf diesen Weg. Sollen Informationen so geschützt werden, dass nur der berechtigte Empfänger sie zur Kenntnis nehmen kann, ist dies derzeit am sichersten durch Verschlüsselungsverfahren zu bewerkstelligen. Deshalb hat der Arbeitskreis „Technische und organisatorische Fragen des Datenschutzes“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder beschlossen, PGP (Pretty Good Privacy) für die gesicherte Kommunikation zwischen den Dienststellen zu nutzen. Diese Entscheidung fiel auch aufgrund der Tatsache, dass das Programm im Internet sehr verbreitet ist und für die private Nutzung eine „Freeware“-Version zur Verfügung steht.

Mit PGP wird ein sogenanntes asymmetrisches Verschlüsselungsverfahren eingesetzt, das nach derzeitigen Erkenntnissen bei entsprechend großem Schlüssel (bis zu 2048 Bit) als ausreichend sicher angesehen werden kann. Da es das am weitesten verbreitete Verschlüsselungsverfahren ist, wird es inzwischen als de-facto-Standard angesehen.

Die lizenzrechtlichen Voraussetzungen für die Nutzung durch LfD und BfD wurden vom LfD Saarland geschaffen; dort liegt auch der Quelltext der eingesetzten Version vor. Die Datenschutzbeauftragten haben ihre öffentlichen Schlüssel ausgetauscht bzw. auf der eigenen Homepage im Internet bekannt gegeben. Auf dieser Grundlage können sie E-Mail sicher – also vertraulich und integer – austauschen. Auch externe Anwenderinnen und Anwender können den öffentlichen Schlüssel von meiner Homepage (siehe http://www.datenschutz.bund.de/technik/bfd_pgd.html) herunterladen, um mit mir verschlüsselte Nachrichten auszutauschen.

8.6 Kontrollen – auch der Datensicherung – sind nötig

8.6.1 Das „Rechenzentrum der offenen Tür“

Im Januar 1999 lenkten Pressemeldungen wie „Reporter hacken Internet-Zugang“ oder „Netradio deckt Datenskandal auf – Telefongesellschaft will Kunden entschädigen“ mein Interesse auf einen Telekommunikationsdiensteanbieter, der über das Internet auch einen kostenlosen E-Mail-Dienst anbot. Ich nahm die besorgniserregenden Pressemeldungen zum Anlass, mir die Situation vor Ort genauer anzuschauen.

Kunden, die die Dienste des Anbieters in Anspruch nehmen wollten, insbesondere das kostenlose E-Mail-Postfach, wählten sich einfach in das Netz des Telekommunikationsdiensteanbieters ein. Anhand der gewählten Rufnummer stellte die Teilnehmervermittlungsstelle des Anbieters fest, dass ihr E-Mail-Dienst angefordert wurde. In diesem Falle wurde der Ruf dann an eine Tochterfirma weitervermittelt, die den Dienst technisch realisierte. Dabei wurde die Rufnummer des Kunden von der Vermittlungsstelle an die Tochterfirma weitergereicht. Die Ruf-

nummer diente neben einer frei wählbaren Kennung und einem Passwort der Identifizierung des Kunden. Der Kunde wurde über die Weiterleitung seiner Rufnummer nicht informiert. Die Rechner der Tochterfirma übernahmen die Verwaltung und Speicherung aller E-Mails, die der Kunde sendete und empfing. Die Rechner waren in einem Gebäude untergebracht, in dem auch noch eine Firma für Badezubehör sowie eine Krawatten- und Seidentücherhandlung residierten. Eine räumliche Trennung der Firmen war nicht vorhanden, d. h. die Firmenmitarbeiter aller Firmen waren über einen gemeinsamen Flur erreichbar; zum Teil gehörten nebeneinanderliegende Büroräume unterschiedlichen Firmen. Ein wahrlich krasser Sicherheitsmangel war der Hinweis „**Bitte Tür nicht schließen!“** an und neben der Tür zu dem Büroraum, in dem die Server untergebracht waren, auf denen die E-Mails der Kunden verarbeitet und gespeichert wurden. Der Grund für diesen Hinweis war bald gefunden: Die Stromversorgung reichte im vermeintlichen „Server-Raum“ für die Vielzahl der Server nicht mehr aus, so dass – über Verlängerungskabel – die Steckdosen der Nachbarräume herhalten mussten. Das Schließen der Tür hätte unweigerlich dazu geführt, dass die Stromversorgung von mehreren Rechnern unterbrochen worden und der E-Maildienst für einige Minuten ins Stocken geraten wäre. Aus Datensicherheitssicht ein nicht tragbarer Zustand, den ich sofort monierte. Immerhin unterliegen auch E-Mails dem Schutz des Fernmeldegeheimnisses und verlangen deshalb nach besonderen Sicherungsmaßnahmen, die in solch einem „Rechenzentrum der offenen Tür“ natürlich gar nicht zu realisieren waren.

Auch in anderen Bereichen musste ich feststellen, dass es mit den notwendigen Maßnahmen der Datensicherung nicht gut bestellt war. So lagen in einem Bereich mit Publikumsverkehr Datenträger (Festplatten, Disketten und Bänder) mit personenbezogenen Daten offen herum, die jederzeit unbemerkt hätten entwendet werden können. Die Büros waren zum Teil oft unbesetzt oder standen wegen der vorstehend genannten Stromversorgungsprobleme ständig offen. Auch die Entsorgung von Papier, beispielsweise von Listen mit Kundendaten, war nicht geregelt. Papier wurde nämlich über den normalen Hausmüll entsorgt. Die Aufbewahrung der Sicherungsbänder war ebenfalls äußerst mangelhaft. Insgesamt gesehen konnte man den Eindruck erhalten, dass Sicherheitsmaßnahmen nur dann ergriffen wurden, wenn Sicherheitslücken in der Öffentlichkeit offenbart wurden. Die Bedeutung des Fernmeldegeheimnisses war den Mitarbeitern nicht bekannt. Vor dem Hintergrund, dass auch die geringsten Maßnahmen zum sicheren Umgang mit den Daten fehlten, wäre es angemessen gewesen, den Betrieb des E-Maildienstes gemäß § 25 BDSG aufgrund der fehlenden technisch-organisatorischen Maßnahmen nach § 87 Abs. 1 TKG und § 9 BDSG zu beanstanden. Da die Mitarbeiter der Firma jedoch ankündigten, umgehend Maßnahmen zur Sicherung des Fernmeldegeheimnisses zu ergreifen und dies von der Muttergesellschaft auch angeordnet wurde, habe ich auf eine formelle Beanstandung verzichtet. Nach meiner Kontrolle wurden die Rechner in ein anderes sicheres Gebäude verlegt und die Organisation und Technik meinen Empfehlungen angepasst.

8.6.2 Immer noch mangelhafte Benutzerverwaltung

Die Aufgaben der Mitarbeiter bestimmen grundsätzlich, auf welche Daten sie in welcher Form – etwa lesend und/oder schreibend – Zugriff haben. Bei der Einstellung neuer Mitarbeiter oder der Zuweisung neuer Aufgaben werden die dazu erforderlichen Nutzerrechte i. d. R. festgelegt. Jede personelle oder organisatorische Veränderung hat anschließend zur Folge, dass die Zugriffsberechtigungen nochmals überprüft und ggf. neu festgelegt werden müssen. Ohnehin empfiehlt sich, Zugriffsberechtigungen regelmäßig zu überprüfen. Eine sachgerechte Benutzerverwaltung – insbesondere bei großen Netzwerken –, hängt also auch vom organisatorischen Zusammenspiel zwischen Personalverwaltung und Systemverwaltung ab.

Bei meinen Kontrollen habe ich wiederholt festgestellt, dass bei Behörden mit großen Netzwerken die Systemverwaltung, die u. a. die Zugriffsrechte auf Dateien und Daten vergibt, häufig nicht über Personalveränderungen informiert wurde. So konnten Mitarbeiter, die bereits in andere Abteilungen versetzt waren, weiterhin auf Daten zugreifen, für die sie nicht mehr hätten berechtigt sein dürften. In einigen Fällen waren Mitarbeiter bereits mehrere Monate ausgeschieden, die Nutzerkennungen und Zugriffsberechtigungen waren aber immer noch aktiv. Hier liegt ein klarer Verstoß nach § 9 BDSG – Nrn. 5 und 10 der Anlage zu § 9 Satz 1 – vor.

Insbesondere Personalveränderungen müssen der Systemverwaltung zeitnah mitgeteilt und dort dann umgesetzt werden. Ausgeschiedene – unter Umständen auch unzufriedene – Mitarbeiter, so Erfahrungswerte vor allem der Privatwirtschaft, können einen erheblichen Schaden verursachen. Hier sehe ich bei den Bundesbehörden noch Bedarf für zügig greifende Organisationsvorgaben, um Datenschutz- oder Sicherheitsprobleme von vornherein zu vermeiden. Darüber hinaus empfehle ich dringend den Einsatz von Unterstützungssoftware für die Benutzerverwaltung. Diese spezielle Software ist für fast alle Netzwerkprodukte auf dem Markt verfügbar. Ohne eine solche Software ist eine ordnungsgemäße Benutzerverwaltung bei großen Netzwerken kaum durchführbar.

8.6.3 Firewalls schützen nicht immer!

Das Internet hat sich zum weltgrößten und mächtigsten globalen Informations- und Kommunikationsmedium entwickelt. Dieser Boom hat auch vor der Bundesverwaltung nicht halt gemacht. Seit geraumer Zeit nimmt die Zahl der Bundesbehörden ständig zu, die das Internet sowohl zur Informationsgewinnung als auch zur Bereitstellung eigener Informationen benutzen wollen. Der Anschluss an das Internet ist allerdings mit erheblichen Gefährdungen und Risiken verbunden. Die Rechner und Übertragungswege des weltweiten Computernetzes sind nicht kontrollierbar. 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, manipulieren oder zerstören. Ich habe bereits im 16. TB darüber berichtet (Nr. 8.2.3) und dort auf eine „Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“ verwiesen, die im Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erstellt wurde. Aufgrund der Zunahme der Internetanschlüsse habe ich im Berichtszeitraum drei Stellen in meinem Zuständigkeitsbereich unter dem Aspekt der Datensicherheit des Internetanschlusses kontrolliert. Als Ergebnis dieser Kontrollen ist folgendes hervorzuheben:

Erfreulich bewerte ich die Tatsache, dass alle kontrollierten Stellen nicht ohne den Schutz einer Firewall den Schritt ins Internet gewagt haben. Allerdings habe ich doch einige Mängel beim Betrieb der Firewall feststellen müssen. In einem Fall wurde eine Firewall eingesetzt, die völlig veraltet war. Die Herstellerfirma existierte bereits nicht mehr, das Produkt selbst wurde auch nicht mehr durch eine andere Firma gewartet. Aktuelle „Updates“ standen nicht mehr zur Verfügung. Der Schutz, den diese Firewall leistet, ist aus der Sicht der Datensicherheit mit einem Verfallsstempel versehen, d. h. in absehbarer Zeit wird der Schutz nicht mehr ausreichen, neueren Angriffsmethoden aus dem Internet nachhaltig standhalten zu können. Firewallsysteme bedürfen einer ständigen Aktualisierung, um den Angriffen aus dem Internet auf Dauer widerstehen zu können. Mit der bloßen Inbetriebnahme eines Firewallsystems ist es daher nicht getan. Der Aufwand sowohl in finanzieller als auch in personeller Hinsicht, die Firewall in einem sicheren aktuellen Zustand zu betreiben, sollte nicht unterschätzt werden. Im aktuellen Fall hat die Behörde zugesagt, das „alte Modell“ umgehend durch ein neueres zu ersetzen. Ich habe außerdem empfohlen, die Expertenmeinung des Bundesamtes für Sicherheit in der Informationstechnik vor der Auftragsvergabe beizuziehen.

Als weiteren Mangel wurden bei allen Kontrollen die fehlenden Regelungen für die Auswertungen der umfangreichen Protokolldaten in der Firewall festgestellt. Firewalls speichern zum Teil sehr detailliert das Surf-Verhalten der angeschlossenen Benutzer. Diese Daten werden in Form von Protokolldaten zur Auswertung von Angriffsversuchen und zur Sicherstellung eines ordnungsgemäßen Betriebs der Firewall benötigt. Die datenschutzrechtliche Speicherbefugnis ergibt sich aus § 9 BDSG, insbesondere Nrn. 3, 4 und 6 der Anlage hierzu. Allerdings reicht diese Speicherbefugnis nicht aus, diese Protokolldaten über einen übermäßig langen Zeitraum zu speichern. Im Informationsverbund Berlin-Bonn (IVBB) wurde in Absprache mit mir eine 6-monatige Speicherungsdauer vereinbart. Darüber hinausgehende Speicherfristen sind nicht erforderlich. In allen Stellen, die ich im Kontrollzeitraum kontrolliert habe, wurde diese Frist bei weitem überschritten. Auch wurde nicht festgelegt, wer auf diese Protokolldaten zu welchem Zweck zugreifen darf. Die Beteiligung des Personalrats nach dem Personalvertretungsgesetz war ebenfalls nicht erfolgt.

In diesem Zusammenhang wurde auch wiederholt an mich die Frage der Benutzung des Internetanschlusses zu privaten Zwecken und der damit verbundenen datenschutzrechtlichen Problematik der Speicherung der Protokolldaten gerichtet. Aus technisch-organisatorischer Sicht ist es für eine Firewall unmöglich, zwischen privater und dienstlicher Nutzung des Internetanschlusses bzw. des Datenabrufes zu unterscheiden (s. auch Nr. 18.10). Aus Sicht der Datensicherheit könnte zwar ein Dienstherr auf die Protokollierung verzichten; er setzt sich dann allerdings der Gefahr aus, dass ein Benutzer die Firewall als Schutzschild für strafbare Handlungen im Internet missbraucht. Alle Ermittlungsversuche würden letztendlich an der Firewall enden und den Dienstherrn somit in den Ruf der Deckung von Straftätern bringen. Ich halte aus diesem Grund an meiner Auffassung zur Protokollierung der Surf-Daten in der Firewall fest. Das Argument, dass das Persönlichkeitsrecht der Mitarbeiter höher zu bewerten ist als die Sicherheit, ist auch nicht überzeugend, da es Methoden – beispielsweise die Pseudonymisierung der Protokolldaten für eine datenschutzgerechte Verarbeitung – gibt, die diesem Anliegen entgegenkommen.

Das Internet bildet heute das Hauptverteilmedium für Schadensprogramme, wie beispielsweise „Trojanische Pferde“, indem entweder ausführbare Programme direkt über sogenannte aktive Inhalte (Java-Applets, ActiveX-Programme) verteilt oder ausführbare Programme per E-Mail mit Anlage passiv an den Benutzer gesendet werden. Gerade das Unterbinden von aktiven Inhalten in einer Firewall stößt in vielen Fällen bei den Benutzern auf Unmut, da ein Großteil der verfügbaren Seiten im Internet auf aktive Inhalte nicht verzichten möchte. Das automatisierte Unterbinden von aktiven Inhalten führt daher häufig zu einer sehr starken Einschränkung der Nutzung des Internets. Deshalb werden in den meisten Fällen die aktiven Inhalte nicht in der Firewall unterbunden. Das Problem ist derzeit nicht befriedigend abschließend lösbar, so dass ich bislang meine grundsätzlichen Bedenken gegen die Zulassung von aktiven Inhalten zurückgestellt habe. Allerdings empfehle ich allen Verantwortlichen für Internetangebote, aktive Inhalte auf ein Minimum zu beschränken. Weiter müssen die Internet-Nutzer über die mit aktiven Inhalten und E-Mail-Anlagen verbundenen Gefahren regelmäßig informiert werden, denn schließlich können Firewalls nicht alle Risiken (z. B. „Trojanische Pferde“) erkennen und abwehren. Als ergänzende Maßnahme zur Abwehr von Trojanischen Pferden sollte der Einsatz eines Intrusion Detection Systems vorgesehen werden (siehe hierzu Nr. 8.10).

8.6.4 SAP – Einsatz im Personalwesen

In jüngster Vergangenheit werden bei größeren Bundesbehörden verstärkt Anstrengungen unternommen, die bisher genutzten automatisierten Personalinformations- und verwaltungssysteme durch Programme auf Basis der integrierten, branchenunabhängigen Standardsoftware R/3 des

deutschen Softwarehauses SAP zu ersetzen. Dieses in der Privatwirtschaft weit verbreitete Produkt kann alle betriebswirtschaftlichen Anwendungsgebiete (z. B. Rechnungswesen, Logistik oder Personalwirtschaft) abdecken und ist bereits in anderen Bereichen der öffentlichen Verwaltung – so z. B. auf Länderebene – in vielfacher Weise im Einsatz. Als Version R/3 ISH wird es in vielen großen Krankenhäusern und Universitätskliniken für die Personal- und Patientenverwaltung und -abrechnung eingesetzt. Es ist inzwischen in der Wirtschaft so weit verbreitet, dass man ohne Übertreibung von einem de-facto-Standard sprechen kann. Trotzdem gleicht kaum ein im praktischen Einsatz befindliches R/3-System dem anderen. Den eigentlichen Erfolg macht die Flexibilität aus, mit der R/3-Systeme an Betriebs- bzw. Verwaltungsstrukturen angepasst werden können.

Diese hohe Flexibilität und Skalierbarkeit birgt aber auch die Gefahr der Unübersichtlichkeit in sich, wenn bestimmte Größenordnungen überschritten werden. Das R/3-Berechtigungskonzept erscheint an sich geeignet, die datenschutzrechtliche Zielvorstellung zu realisieren, dass jeder Benutzer exakt die Berechtigungen bekommt, die er für seine Aufgaben benötigt. Die vorhandenen und aus Sicht des Datenschutzes grundsätzlich zu begrüßenden sehr feinen Rechtestrukturen können aber auch bewirken, dass die Transparenz der Rechtevergabe schnell verloren geht und damit eine Revision der Zugriffs- und Benutzerkontrollen im Sinne des § 9 BDSG faktisch unmöglich wird. Dies betrifft dann nicht nur außenstehende Prüfer, wie z. B. den lokalen Datenschutzbeauftragten oder die Datenschutzbehörden; selbst mit dem System vertraute Personen – wie etwa die Administratoren – können Sicherheitslücken leicht übersehen oder gar unbewusst verursachen.

Aus datenschutzrechtlicher Sicht steht deshalb insbesondere die Ausgestaltung des Berechtigungskonzepts im Vordergrund des Interesses. Die Standardversion von SAP R/3 beinhaltet etwa 700 Berechtigungsobjekte, daneben können je Benutzerstammsatz nochmals ca. 1 300 Berechtigungseinträge vorgenommen werden. Da verwundert es nicht, dass es Fälle gegeben hat, in denen überforderte Administratoren zur Gewährleistung eines reibungslosen Betriebs den Benutzern mehr Rechte zugewiesen haben, als tatsächlich erforderlich gewesen wären. Hierin, nämlich den Nutzern mehr als die notwendigen Rechte zuzuweisen, besteht eine grundsätzliche Gefahr. Die Ausarbeitung eines guten Berechtigungskonzepts muss daher bereits in der Projektierungsphase vorbereitet werden, denn wenn seine Erstellung erst mit der Installation des Systems beginnt, sind Fehler fast unvermeidlich. Dies setzt natürlich umfassende Kenntnisse über die Funktionalität von R/3 und die Unternehmens- bzw. Verwaltungsgegebenheiten sowie sehr viel Erfahrung bezüglich der Implementierung voraus. Der sichere Umgang mit R/3-Systemen setzt eine hochwertige Qualifikation und Spezialisierung voraus, die nur durch praktische Erfahrung, Fortbildung und einen stetigen Fluss von Informationen zu Sicherheitshinweisen, Fehlermeldungen usw. aufrecht erhalten werden kann. Es sind also in der öffentlichen Verwaltung – ebenso wie in den privaten Unternehmen – alle Qualifikationsanstrengungen zu erbringen, die die sichere Beherrschung solcher Systeme überhaupt erst ermöglichen. Ähnlich wie bei Unix-Systemen (s. u. Nr. 8.12.2) halte ich den Einsatz von Tools zur Prüfung und Revision des Berechtigungskonzeptes für dringend erforderlich. Solche ergänzenden Tools sind am Markt erhältlich und sollten beim Einsatz von SAP R/3 unbedingt berücksichtigt werden.

Die mir bekannten Vorhaben auf Ebene der Bundesbehörden befinden sich allesamt noch in der Planungs- bzw. Konzeptionsphase; erste Realisierungen sind aber möglicherweise bereits im laufenden Jahr 2001 zu erwarten. Bei den Beratungsgesprächen für eine automatisierte Personaldatenverarbeitung – denen ich aus meiner Sicht eine besondere Bedeutung beimesse – habe ich darauf hingewiesen, dass in diesem Bereich für die Bundesverwaltung im Vergleich zur Privatwirtschaft besondere Rechtsvorschriften gelten. So sind etwa die gesetzlichen Vorgaben des Bundesbeamtengesetzes (§§ 90 ff, insbesondere § 90g BBG) zu beachten und auch bei einem Einsatz von SAP-R/3-Produkten sicherzustellen bzw. umzusetzen. Dies wurde mir von den betroffenen Bundesbehörden zugesichert.

8.7 Computerviren – auch eine Gefahr für den Datenschutz

8.7.1 Gefahr durch einen „Liebesbrief“

Im Mai 2000 wurden durch eine „nichtssagende, aber vielversprechende“ E-Mail Millionen von Frauen und Männern ihrer Illusionen beraubt und damit nicht genug, auch noch durch Ausfälle der Informationstechnik ein Millionenschaden angerichtet. Verursacht wurden diese Probleme durch einen Computer-Virus, der unter dem Namen ILOVEYOU-Virus weltweit für Aufsehen und Aufregung sorgte. Computer-Viren sind nicht neu, schon vor einigen Jahren machte ein anderer Virus – MELISSA – Schlagzeilen. „ILOVEYOU“ hatte jedoch einige neue besondere Aspekte:

1. Die rasante Geschwindigkeit, mit der sich der Virus verbreitet hat.

2 Die Methodik der Verbreitung, die auf der Kenntnis der vereinheitlichten Softwarestrukturen beruhte.

3 Die fehlenden Notfallpläne in vielen IT-Bereichen.

4. Die zum Teil kläglichen Versuche von verschiedenen Stellen, dem Virus Herr zu werden.

5 Die „unvernünftige“ Reaktion von vielen Anwendern.

Der Schaden, den der Virus anrichtete, äußerte sich in vielen Fällen darin, dass die elektronische Post der betroffenen Stellen tagelang nicht erreichbar war, weil das Leitungsnetz total überlastet war.

Bei dem „ILOVEYOU“-Virus handelte es sich um einen einfachen sogenannten E-Mail-Wurm. Er war in einer Macrosprache programmiert, die das Handling des Virus vereinfachte. Die schnelle Verbreitung erfolgte über

E-Mail und nutzte die Kenntnis der weiten Verbreitung und einheitlichen E-Mail-Strukturen eines bestimmten E-Mailprodukts gnadenlos derart aus, indem die betroffenen Adressbücher wiederum zur weiteren Verbreitung benutzt wurden. Die Vorgehensweise des Virus war schlichtweg einfach und enthielt in verschiedenen Varianten grundsätzlich folgende Merkmale:

Betreff:	ILOVEYOU
Inhalt:	LOVELETTER coming from me.
Anhang:	LOVE-LETTER-FOR-YOU.TXT.vbs

Die Dateiendung „TXT“ im Anhang sollte der E-Mail einen unverfänglichen Anschein geben, um dem Benutzer vorzugaukeln, sie hätten es nur mit einer – harmlosen – Textdatei zu tun. In Wirklichkeit war der Anhang aber ein gefährliches Programm, das, einmal ausgeführt, die Kontrolle über einen Teil des Betriebssystems übernahm. Nach Öffnung des Anhangs stellte der Virus Kontakt mit dem E-Mail-Programm her und sendete an alle Einträge im Adressbuch eine E-Mail mit dem entsprechenden LOVE-LETTER-FOR-YOU-Anhang. Dadurch wurde er garantiert weiterverbreitet und konnte sich in einem solch enormen Tempo über die globale Internetwelt verbreiten.

Das Erschreckende an diesem Virus war nicht nur die Verbreitungsgeschwindigkeit, sondern auch das Verhalten etlicher Benutzer. Das böse Wort vom „DAU“ – dem dümmsten anzunehmenden User – machte allenthalben die Runde. Trotz Warnungen öffneten Benutzer nämlich den „Loveletter“ und lösten damit das Chaos im betroffenen Netzwerk aus. Hier zeigte sich wiederum, dass Anwenderschulung eine wesentliche Voraussetzung für ein sicheres Funktionieren einer IT-Landschaft ist.

Die von mir immer wieder beklagte Laissez-faire-Haltung vieler Behörden und Unternehmen in Fragen der IT-Sicherheit führte ferner dazu, dass der Virus den „Nährboden“ fand, den er für seine Verbreitung brauchte. Diejenigen, die die Schuld allein auf den von „ILOVEYOU“ betroffenen Softwarehersteller Microsoft schieben wollten, machen es sich zu einfach. Immerhin benötigte der Virus Schwachstellen im Sicherheitskonzept, um sich in diesem Umfang verbreiten zu können. Die Schädigung schlug auch auf die Kommunikationspartner über, indem deren Mail-Server und Leitungen restlos überlastet wurden. Die Mail-Lawinen solcher unsicherer Internet-Teilnehmer schädigten somit auch Dritte mitunter in ganz erheblichem Maße. Die Behörden, die über ein Notfallkonzept verfügten und kurze Alarmwege organisiert haben, blieben von einer größeren Attacke verschont.

Auch die Reaktionszeit von verschiedenen Institutionen, die sich mit Sicherheitsfragen befassen, muss nach diesem Angriff überdacht werden, insbesondere die Vorwarnzeiten müssen im erheblichen Umfang verkürzt werden.

Vielleicht war „ILOVEYOU“ auch schlichtweg überfällig, um vielen Verantwortlichen die Fahrlässigkeit und fehlenden Konzepte, solchen Fällen zu begegnen, vor Augen zu führen.

8.7.2 Notfallkonzept statt Hektik!

Der „ILOVEYOU“-Virus (s. o. Nr. 8.7.1) brachte es an den Tag: In vielen Behörden und Unternehmen existieren zwar Sicherheitskonzepte, doch für den „Fall der Fälle“ ist man nicht gewappnet. Erfolgt eine Attacke, z. B. durch einen Virus, weiß niemand so genau, was zu tun ist. Unkoordiniertes Handeln bestimmt dann den weiteren Ablauf, mit der Folge, dass planlos gehandelt wird, ohne die Konsequenzen zu überlegen. Auch Regressforderungen an den Verursacher können nicht erhoben werden, weil der Schaden nicht in ausreichendem Maße dokumentiert wird. Eine Notfallplanung existiert in vielen Fällen nicht. In der Folge weiß beispielsweise der Anwender nicht, an wen er sich wenden soll, wenn bei ihm ein Virus auftritt. In vielen Fällen kennt die Systemverwaltung weder eine Telefonnummer noch eine Internetadresse, um sich bei einem Virenbefall oder einem Angriff etwa aus dem Internet Rat zu holen. Aktuelle Virenwarnmitteilungen in den Internetseiten des Computer Emergency Response Teams (CERT) oder des Computer Emergency Response Teams des Bundesamtes für Sicherheit in der Informationstechnik (BSI-CERT) werden oft auch nicht gelesen. Dies ist deshalb zu bedauern, weil es gerade in diesen kritischen Situationen auf Schnelligkeit ankommt, um größere Schäden zu verhindern.

Aufgrund der Erfahrungen mit dem „ILOVEYOU“-Virus empfehle ich deshalb dringend, ein Notfallkonzept aufzustellen und dieses ständig der technologischen Entwicklung und der Veränderung der Systeme anzupassen.

Das Notfallkonzept sollte in jedem Fall folgende Teile enthalten:

1. Eine interne Hotline-Nummer, an die sich Anwender wenden können, wenn ein Virus aufgetreten ist, unplausibles Systemverhalten vorliegt oder eine Attacke aus dem Internet erkannt wird.
2. Die externe Hotline-Telefonnummer des für die Behörde oder das Unternehmen zuständige CERT; für Stellen in meinem Zuständigkeitsbereichs ist dies das Bundesamt für Sicherheit in der Informationstechnik, Referat V2/BSI-CERT, Postfach 20 03 63, 53133 Bonn, Tel. 0228 9582 444, FAX: 0228 9582 427
3. Sinnvoll ist auch, die Internetadresse des BSI-CERT in die Planungen mit aufzunehmen (www.bsi-cert.de).
4. Festlegung der Alarmmeldewege, die bei einem Virusbefall und/oder Eindringen eines Hackers zu beachten sind.
5. Genaue Festlegung, wer in einem System welche Entscheidung – beispielsweise das Herunterfahren von Systemteilen – treffen darf. Auch sollte festgelegt werden, wie die Benutzer über das Beenden des Systembetriebs unterrichtet werden.
6. Das Starten des Systems ist ebenso an Bedingungen zu knüpfen, damit beispielsweise sichergestellt ist, dass der Virus in einem Netz vollständig beseitigt wurde.

7. Sicherstellung des Virus und/oder der Protokolldaten, die einen Einbruch in das System dokumentieren.
8. Schadensermittlung, um eventuell Regressansprüche stellen zu können.

Das Notfallkonzept sollte allen Mitarbeitern, die mit PC arbeiten, bekannt gegeben und es sollte erprobt werden. Behörden und Organisationen, die kein Notfallkonzept haben, sollten umgehend mit den Planungen beginnen, damit sie im Fall der Fälle gerüstet sind.

8.8 Programme aus „offenen Quellen“

Jeder, der im Internet surft oder E-Mails schreibt, benutzt – wenn auch vielleicht unbewusst – kostenlose Software. Wer sich mit Computern beschäftigt, wird mit kostenloser Software auf CDs, in Zeitschriften oder durch „kostenlose“ Angebote zum Herunterladen im Internet konfrontiert.

Die Datenschutzbeauftragten des Bundes und der Länder haben in ihrer Entschließung vom 25./26. März 1999 (s. **Anlage 10**) die Hersteller von Informations- und Kommunikationstechnik aufgefordert, Software so zu entwickeln und herzustellen, dass Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen überzeugen können. Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder hat dazu im November 2000 die Empfehlung „Transparente Software – eine Voraussetzung für datenschutzfreundliche Technologien“ veröffentlicht (siehe http://www.bfd.bund.de/technik/aktech1.html).

Mit dem Begriff Software wird nahezu alles bezeichnet, was auf einem Computer ausgeführt wird. Das sind sowohl fertige, nur in einer bestimmten Systemumgebung (Architektur) ausführbare Programme (Binary) als auch vom Programmierer geschriebene Programmtexte (Source oder Quelltexte). Die aus Sicht des Datenschutzes notwendige Transparenz von Software kann nur gewährleistet werden, wenn Quelltexte von Programmen nicht geheim gehalten werden, sondern für Prüf- und Revisionszwecke zugänglich sind. Solche Kontrollen sind unerlässlich, weil komplexe Software praktisch nie fehlerfrei ist – und sich auch nicht hundertprozentig austesten lässt –, die Qualitätskontrollen der Hersteller in der Regel somit auch nicht ausreichen und die Überprüfung (durch unabhängige Dritte) bei sicherheitskritischen Komponenten etwa zur Erzeugung einer Digitalen Signatur verpflichtend ist.

Ein Ansatz, um transparente, datenschutzfreundliche Technologien bereit zu stellen, ist die Evaluierung und Zertifizierung von Software durch unabhängige Fachleute. Dieses Modell kann – obwohl die breite Anwendung der Evaluierung und Zertifizierung immer noch aussteht – als anerkannt betrachtet werden. Auch die dazu geschaffenen Grundlagen, wie die europäischen „Information Technology Security Evaluation Criteria“ oder die „Common Criteria“ haben sich bereits bewährt.

Ein weiterer Ansatz für Transparenz stellt das Entwicklungsmodell „Open Source“ dar. Der Begriff Open Source wurde zunächst geprägt, um einen gemeinsamen Namen für die Lizenzen benutzen zu können, die für jedermann zugänglich sind. In der Praxis sind schon vor der Entstehung des Open Source Modells andere Lizenzmodelle entstanden, die alle das Ziel haben, Programmierern wie Anwendern Software mit möglichst wenigen Einschränkungen zur Verfügung zu stellen und gleichzeitig deren Fortbestand und Weiterentwicklung zu sichern oder zumindest zu vereinfachen. Sowohl bei kommerzieller Software als auch im Bereich der freien Software gibt es fast so viele verschiedene Lizenzbedingungen wie Programme. Für Open Source Software gelten insbesondere folgende Lizenzbedingungen:

- BSD License
- GNU General Public License (GPL)
- GNU Library General Public License (LGPL)
- QPL
- NPL
- Public Domain.

Seit 1998 gibt es eine Open Source Definition (OSD), die im Internet unter http://www.opensource.org/osd.html veröffentlicht ist.

Beispiele für Open Source – Projekte

GNU	**DNS, BIND**	**Samba**	**Tcl/Tk**	**GIMP**
Free BSD	**Sendmail**	**Perl**	**KDE**	**GnuPG**
Linux	**Apache**	**Python**	**GNOME**	**Jade**

Open-Source-Software ist transparent und erfüllt damit eine Basisforderung datenschutzfreundlicher Technologien. Anhand des Quelltextes ist eine Prüfung durch unabhängige IT-Experten prinzipiell uneingeschränkt möglich, was auch die Revisionsfähigkeit der Software maßgeblich erhöht.

Allerdings ist nicht garantiert, dass die Prüfung auch tatsächlich stattfindet – in der Praxis findet eine unabhängige Überprüfung eher nicht statt – und dass der Quelltext verständlich ist. Generell gilt daher, dass auch Programme, die unter Open-Source-Bedingungen veröffentlicht werden, Fehler enthalten können, von denen möglicherweise lange Zeit niemand Notiz nimmt. Darum ist es besonders wichtig, dass formalisierte Verfahren für Prüfung und Evaluierung von Software genutzt werden. In der Regel ist hierfür zusätzlich die Spezifikation der Software nötig, leider verlangt die OSD nicht, dem Quellcode eine Dokumentation oder gar eine Spezifikation beizulegen. Beides ist aber zur Evaluation zwingend erforderlich. Die OSD verbietet lediglich absichtlich verwirrend geschriebenen Code.

Open-Source-Produkte haben den Vorteil, dass sich Anwender weitgehend selbst gegenüber Sicherheitslücken schützen können, sofern sie sich regelmäßig die erforderlichen Informationen – normalerweise aus dem Internet – beschaffen. Open-Source-Entwickler unterstützen dieses Vorgehen, indem Fehler im Internet in der Regel mit entsprechenden Fehlerbeseitigungsmaßnahmen publiziert werden. Die aktive Beteiligung vieler IT-Experten an der Fehlerbeseitigung kann dazu beitragen, dass Sicherheitslücken wesentlich schneller geschlossen werden, als das bei herkömmlicher Software möglich ist.

Derzeit scheint sich das Open Source Entwicklungsmodell neben dem herkömmlichen Softwareentwicklungsmodell als Alternative zu etablieren. Es zeichnet sich ab, dass einige große kommerzielle Unternehmen ihre Entwicklungen (wenigstens teilweise) als Open Source veröffentlichen werden. Nach den Open Source Entwicklungen in den Bereichen Toolentwicklung (z. B. GNU), Betriebssystem (z. B. Linux) und graphischen Desktopanwendungen (z. B. KDE, KOffice) wird zukünftig an Entwicklungen im Bereich der Embedded Systems gearbeitet werden.

In der Vergangenheit stellten fehlende Support- und Dienstleistungsangebote ein wesentliches Hindernis für den kommerziellen Einsatz von Open Source Anwendungen dar. Heute bieten viele Hardwarehersteller Dienstleistungsunternehmen und Distributoren gleichen Support an, wie für vergleichbare kommerzielle Systeme.

Ein Ziel des Datenschutzes – mehr Transparenz von Software – kann nur erreicht werden, wenn

- die Quellprogramme von vertrauenswürdigen Stellen kommen und überprüft sind,
- die lauffähigen Programme aus diesen Quellen erzeugt werden,
- die Verteilung / Bereitstellung von Quellprogrammen und lauffähigen Programmen sicher erfolgt und
- Betreuung, Fehlerbeseitigung sowie Weiterentwicklung in angemessener Weise sichergestellt wird.

Mit dem Open Source Modell ist man auf dem richtigen Weg.

8.9 Die nächste Generation des elektronischen Telefonbuchs: Verzeichnisdienste!

Jeder kennt die Situation bei Konferenzen, Tagungen und sonstigen Treffen mit Kunden oder interessanten Gesprächspartnern: der Austausch der Visitenkarten! Auf der Visitenkarte sind nämlich die wichtigsten Informationen wie Name, Vorname, Titel, Anschrift, E-Mail-Adresse, Telefonnummer, Faxnummer und selbstverständlich die Stellung innerhalb der Organisation, mehr oder weniger übersichtlich angeordnet und griffbereit. Doch jeder kennt auch die Situation, die auftritt, wenn er die Information der Visitenkarte sucht, weil er sie verlegt hat, oder wenn die Informationen darauf nicht mehr stimmen, weil sich die Daten geändert haben. Schön wäre deshalb ein elektronisches Telefonbuch, auf das man von überall und jederzeit zugreifen kann, z. B. über das Handy, und die gewünschte Adresse, Telefonnummer oder anderes mit ein paar einfachen Klicks finden könnte. Gute Dienste könnte ein solches System auch dann liefern, wenn man vertrauliche Informationen an einen Kommunikationspartner schicken möchte und hierzu einen vertrauenswürdigen „öffentlichen Schlüssel“ zum Verschlüsseln der E-Mail benötigt. Unter Zuhilfenahme eines solchen Dienstes bekäme man immer den gültigen öffentlichen Schlüssel des Kommunikationspartners und könnte somit vertrauliche Informationen problemlos austauschen. Um ein Höchstmass an Effizienz und Sicherheit in der täglich anfallenden Kommunikation mit einem Gesprächspartner zu erreichen, wäre also ein übergeordnetes globales „elektronisches Telefonbuch“ durchaus von Nutzen, aus datenschutzrechtlicher Sicht sogar zu begrüßen.

Programme mit der Bezeichnung „Verzeichnisdienste“ bieten solche Dienste an. In internen Netzen mit mehreren hundert Benutzern in der öffentlichen Verwaltung, aber auch im Internet, halten Verzeichnisdienste in neuester Zeit Einzug. Sie bieten aus datenschutzrechtlicher Sicht einige Vorzüge, aber werfen auch einige Fragen auf.

Die wichtigsten bei Beratungen zu diesem Thema an mich gerichteten Fragen betrafen folgende Punkte:

- Rechtliche Einordnung von Verzeichnisdiensten:
  Soweit ein Verzeichnisdienst nur in einem Intranet einer datenverarbeitenden Stelle – beispielsweise im Informationsverbund Berlin Bonn (IVBB) – eingesetzt wird, handelt es sich weder um einen Tele- noch um einen Mediendienst. Die Zulässigkeit derartiger Verzeichnisdienste richtet sich daher in einem abgeschlossenen internen Netz nach den allgemeinen da-

tenschutzrechtlichen Bestimmungen für Dienst- und Arbeitsverhältnisse.

- Veröffentlichung von Klarnamen:
  Grundsätzlich sollte allen Bediensteten, die keine herausgehobene Funktion innehaben, ein Wahlrecht dahingehend eingeräumt werden, ob sie mit ihrem Klarnamen oder mit einem selbstgewählten Pseudonym – beispielsweise „Pforte 1“ – in ein über das Intranet abrufbares Verzeichnis eingestellt werden wollen. Auf diese Weise kann auch das Risiko einer unkontrollierten Sammlung personenbezogener Informationen durch Suchmaschinen begrenzt werden.

- Beschäftigtendaten in Verzeichnisdiensten:
  Da es bisher keine speziellen Regelungen gibt, kommt lediglich eine Anlehnung an die Regelungen über die Datenerhebung und den Umgang mit Personalaktendaten sowie das BDSG in Betracht, wonach Beschäftigtendaten nur verarbeitet werden dürfen, wenn dies zur ordnungsgemäßen Aufgabenerfüllung der öffentlichen Stelle erforderlich ist. Um hier die notwendigen gesetzlichen Regelungen zu schaffen, bietet sich das von der Bundesregierung angekündigte Arbeitnehmerdatenschutzgesetz an. Soweit auf den Verzeichnisdienst nur Mitarbeiterinnen/Mitarbeiter der eigenen Verwaltung zugreifen können, dürfen die erforderlichen Angaben über sämtliche Mitarbeiterinnen/Mitarbeiter zur Verfügung gestellt werden. Bestehen auch andere Zugriffsmöglichkeiten, dürfen Familienname, dienstliche Telefonnummer und Hinweise auf den Aufgabenbereich sowie öffentliche Schlüssel zur sicheren Kommunikation nur von solchen Personen in den Verzeichnisdienst aufgenommen werden, die den Anschluss aus dienstlichen Gründen nutzen müssen und bei denen die Erreichbarkeit zu ihrer dienstlichen Aufgabe gehört, beispielsweise Mitarbeiter der Pressestelle. Hinsichtlich der Bediensteten, die in der Regel keinen unmittelbaren Kontakt außerhalb der eigenen Dienststelle haben, beispielsweise Angehörige des Schreib- oder Botendienstes, ist die Bekanntgabe ihrer Daten nicht erforderlich. Deren Aufnahme wäre nur mit Einwilligung zulässig. Zur Veröffentlichung von Personaldaten im Internet s. u. Nr. 18.10.

- Organisatorisch-technische Sicherungsmaßnahmen:
  Für alle Komponenten, auf die der Verzeichnisdienst aufsetzt, sind mindestens Maßnahmen entsprechend dem BSI-Grundschutzhandbuch vorzusehen. Für Unix-Systeme wäre der Einsatz eines Administrationstools wünschenswert (s. u. Nr. 8.11.2). Die Zugriffsregelungen sind möglichst eng zu fassen.

Mit dem Betrieb von Verzeichnisdiensten hat sich auch eine Arbeitsgruppe des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder befasst und eine Orientierungshilfe erarbeitet, die auf meiner Homepage unter „Datenschutz und Technik“ zum Abruf bereit steht. Neben den oben aufgeführten Grundsätzen finden sich dort weitere hilfreiche Tipps zum datenschutzgerechten Betrieb eines Verzeichnisdienstes.

8.10 „Intrusion Detection“ – ein zweischneidiges Schwert

Die zunehmende Vernetzung einzelner Systeme, die Vernetzung lokaler Netzwerke zu Weitverkehrsnetzwerken, der Anschluss von bisher isolierten Netzwerken an das Internet oder der Anschluss von Intranetstrukturen an das Internet ist heute unabdingbare Voraussetzung für eine erfolgreiche Unternehmensstrategie oder für eine bürgernahe öffentliche Verwaltung. Allerdings wachsen damit auch die Risiken, denen die Systeme ausgesetzt sind.

Für die öffentliche Verwaltung des Bundes und der Länder haben deshalb die Datenschutzbeauftragten des Bundes und der Länder vor einiger Zeit eine Orientierungshilfe herausgegeben, die sich mit Sicherheitsfragen beim Anschluss von Netzwerken an das Internet befasst und entsprechende Empfehlungen zur Minimierung der Risiken ausspricht. Ich habe mich zu diesen Empfehlungen in meinem letzten Tätigkeitsbericht geäußert (s. 17.TB. Nr. 8.9.2); die Orientierungshilfe ist unter meiner Homepage abrufbar (URL: http://www.bfd.bund.de/technik/Ori_int/ohint_iv.html).

In der Regel wird die Sicherheit der Systeme durch die Abschottung gegenüber dem Internet mittels Firewalls zu erreichen versucht. Die Erfahrungen mit Firewalls zeigen allerdings, dass diese keine 100 %-ige Sicherheit bieten können. Verbesserte Angriffsmethoden können auch Firewalls überwinden, beispielsweise durch Einsatz von „Trojanischen Pferden“. **Intrusion Detection Systeme (IDS)** sollen diese Lücke schließen. Unter einem IDS versteht man eine Analysemethode zur Erkennung von Angriffen auf Rechnersysteme hinter einer Firewall. Ein IDS ist also nichts anderes als eine Art Videosystem zur Raumüberwachung. Die „Raumüberwachung“ geht dabei von folgenden Szenarien aus (s. Abb. 3):

Ein IDS basiert auf folgenden Komponenten:

- **Datensammelkomponente**
  Sammlung aller Daten über den Systemzustand, herangezogen werden dabei auch Protokolldaten, Sniffer-Daten etc.

- **Datenanalyse**
  Auswertung der gesammelten Daten im Hinblick auf Angriffe.

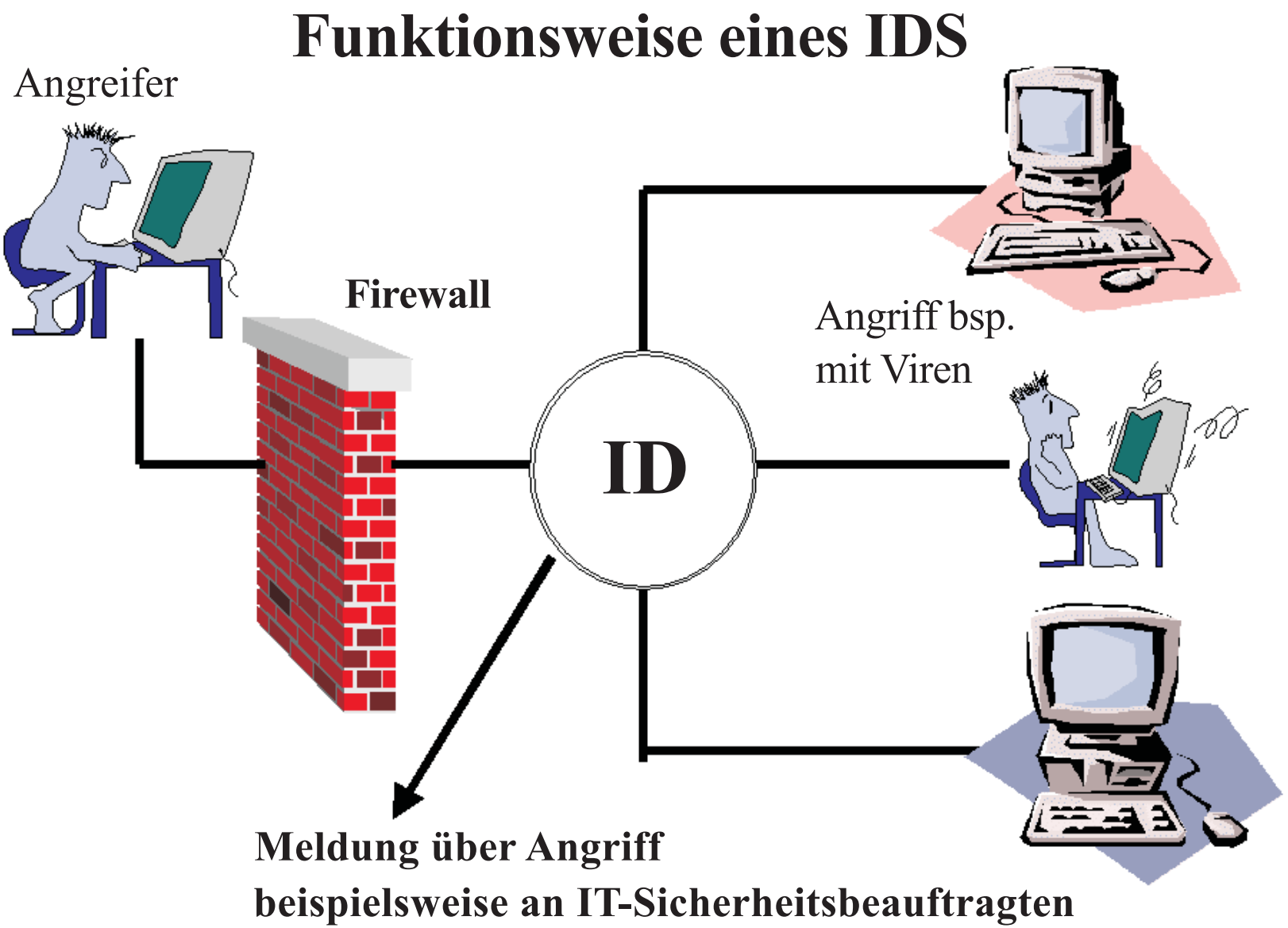
- **Präsentation**
  Benutzergerechte Darstellung der Ergebnisse der Datenanalyse, eventuell Übergabe der Ergebnisse an Intrusion Response Systeme (Abwehrprogramme).

Der Einsatz eines Intrusion Detection Systems ist auch deshalb notwendig, weil folgende Änderungen des IT-Umfeldes in den letzten Jahren zu verzeichnen sind:

- Der Einsatz von objektorientierten Techniken ermöglicht ohne große Umstände die sofortige Ausführung von übermittelten Programmen und/oder aktiven Dokumenten auf Zielsystemen (Verteilung von Viren, Trojanischen Pferden etc.).

- Die Konzentration auf wenige den Markt beherrschende kommerzielle Softwareprodukte führt zu einem

Abbildung 3 (zu Nr. 8.10)



weitgehend einheitlichen Produktspektrum und einer im wesentlichen einheitlichen Verzeichnisstruktur (gleiche/ähnliche Angriffsziele, der Angreifer weiß wo er welche Lücken findet).

- Sicherheitsaspekte werden bei der Entwicklung von Softwareprodukten nicht in ausreichendem Maße beachtet.
- Hohe Fehlerrate bei Neuentwicklungen (Bananenprodukte = reifen beim Kunden)
- Billige Shareware mit hohem Verbreitungsgrad (und Unterhaltungswert) führen zur einer leichten Verbreitung von „Hilfsprogrammen“ (Ausspionierung).
- Browser-Plug-In-Technik (Plug-In sind Erweiterungen für den Browser, um z. B. Grafikformate oder Videoclips anzeigen zu können) reizt zum ungeprüften Übernehmen von neuen Features.
- Effektivität der Hacker steigt.
- Publikationen von Angriffen nehmen ständig zu.
- Angriffe setzen nicht mehr Fachwissen voraus, sondern den Besitz von Angriffsskripten und/oder Hack- und Cracksoftware.

Der Erfolg eines IDS hängt häufig zum großen Teil von der Quelle der Daten zur Intrusion-Erkennung, der Qualität der Daten und der Speicherdauer der Datensammlungen ab.

Aus datenschutzrechtlicher Sicht sind die **Datenquellen und deren Qualitäten** von besonderer Bedeutung. Als Datenquellen kommen dabei in Frage:

- **Auditdaten aus den Systemkomponenten wie Betriebssystem, Firewallsysteme, Anwendungsprogrammen etc.**
  Wer hat sich angemeldet?
  Gibt es Schutzverletzungen und wenn ja, welcher Art?
  Wer greift wann auf welche Daten?
  Welche Programme werden gestartet?
- **Betriebsmittelvergabe durch das Betriebssystem**
  Prozessor-Auslastung
  Anzahl der Netzverbindungen
  Art der Netzverbindungen
- **Netzwerkprotokoll und Nutzungsdaten**
  Quell- und Zieladresse einer Verbindung
  Welche Protokolle werden verwendet?

Der eigentliche Verarbeitungsprozess in einem IDS wird in der Datenanalyse durchgeführt. Die am Markt erhältlichen Produkte lassen sich dazu in folgende zwei Kategorien einteilen:

1. Missbrauchserkennungssysteme:
   Ähnlich wie bei Virenscannern werden hier die Auditdaten mit Blick auf bekannte typische (Angriffs-) Muster analysiert, d. h. die vorhandenen Auditdaten werden auf ein bestimmtes vorhandenes und bekanntes Angriffsmuster untersucht. Hierfür ist Voraussetzung, dass die Angriffsmuster hinreichend bekannt und beschrieben sind, das IDS die Muster beispielsweise in einer Datenbank zugänglich gespeichert hat und die Datenbank manipulationssicher ist.

2 Anomalieerkennung:
   Jeder Angriff erzeugt nach einer gewissen Zeit ein atypisches Systemverhalten, wodurch ein Angriff letztendlich erkannt wird. Das Abweichen eines Systems von einem Normalzustand setzt allerdings voraus, dass der Normalzustand eines Systems bekannt ist. Die Erkennung des Normalzustandes erfolgt dabei auf der Basis eines **statistischen** (das System ermittelt den Normalzustand aus den Systemparametern CPU-Auslastung, Seitenwechselrate etc.) und eines **logischen Ansatzes** (anhand von zeitlichen Abfolgen von Ereignissen wird der Normalzustand festgehalten).

Weicht das System vom Normalzustand ab, führt dies zu einem IDS-Alarm. Der Einsatz von ID-Systemen steckt noch in den Kinderschuhen, so dass bislang kaum Erfahrungswerte vorliegen. Grundsätzlich kann man aber feststellen, dass der Erkennungsaufwand mit der Effektivität der Angriffe steigt.

Die Datenschutzprobleme ergeben sich aufgrund der notwendigen umfangreichen Speicherung von Protokolldaten. Die einschlägigen Rechtsnormen sind § 14 Abs. 4 BDSG für den öffentlichen Bereich und in § 31 BDSG für den nicht-öffentlichen Bereich (= Privatwirtschaft). Beide Vorschriften bestimmen die Zweckbindung von Protokolldaten zur Datenschutzkontrolle, zur Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage. So sind nach Nr. 6 der Anlage zu § 9 Satz 1 BDSG bei der automatisierten Verarbeitung von personenbezogenen Daten beispielsweise Maßnahmen zu treffen, die geeignet sind *„zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können.*“ Diese Vorschriften des BDSG müssen bei Inbetriebnahme eines IDS herangezogen werden. Man könnte sich nämlich auf den Standpunkt stellen, dass die Rohdaten für die Komponente „Datensammlung“ eines IDS im gewissen Umfang erhoben und gespeichert werden dürfen, um auch den Anforderungen nach § 9 BDSG zu entsprechen. Ich empfehle beim Einsatz von IDS-Systemen folgende Maßnahmen zu beachten:

1. Personenbezogene Auditdaten sind nur solange wie absolut notwendig zu speichern und umgehend nach der Nutzung zu löschen.
2. Nutzungsdaten sind unbedingt zu pseudonymisieren. Das Verfahren muss geeignet und sicher sein. Die Re-Pseudonymisierung sollte nur unter 4-Augen-Prinzip stattfinden können. Aufgedeckte Pseudonyme dürfen nicht mehr verwendet werden.
3. Authentizität der Audit- und Nutzungsdaten ist sicherzustellen. Dies kann zum einen durch die Zertifizierung des IDS erfolgen, zum anderen durch den Einsatz von sicherer Hardware (beispielsweise WORM-Medien) und digitalen Signaturen.

Vorsicht:
Bei Verwendung vom WORM-Speichermedien ist die Löschung der nicht mehr benötigten Daten sicherzustellen.

4. Entkopplung der IDS-Anwendung von der Systemadministration, beispielsweise in dem das IDS auf einer abgesetzten Hardware mit eigener Administration läuft.
5. Erstellen einer Dienstanweisung, die auch den Verfahrensablauf bei interner Missbrauchserkennung regelt.
6. Die Beteiligung der Personalvertretung/des Betriebsrates ist sicherzustellen.

8.11 BSI hilft beim Datenschutz

8.11.1 Verbesserungen im IT-Grundschutzhandbuch

Da die Informationstechnik überaus innovativ ist und sich ständig weiterentwickelt, muss auch das IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ständig aktualisiert und erweitert werden. Der aktuelle Sachstand zum IT-Grundschutz – die neueste Version ist vom Oktober 2000 – kann über die Seite http://www.bsi.bund.de/gshb abgerufen werden.

Mit den Empfehlungen zur Implementierung von Standard-Sicherheitsmaßnahmen bietet das IT-Grundschutzhandbuch unmittelbare Hilfe zur Umsetzung der IT-Sicherheit. Darüber hinaus stehen weitere Hilfsmittel für die tägliche Arbeit, wie

– das BSI-Tool zum IT-Grundschutz,

– das BSI-Tool USEIT (s. Nr. 8.11..2),

– Chiasmus für Windows (s. Nr. 8.5.1),

– Formblätter z. B. für die IT-Grundschutzerhebung oder

– Muster z. B. für die Dienstanweisung des IT-Sicherheitsbeauftragten

zur Verfügung.

Mit dem IT-Grundschutztool wird die gesamte Vorgehensweise bei der Erstellung eines Sicherheitskonzepts, der Soll-Ist-Vergleich, die Umsetzung der Maßnahmen und die anschließende Sicherheitsrevision unterstützt. Darüber hinaus kann aus dem Tool elektronisch auf die Texte des Handbuchs zugegriffen werden. Ein individuell anpassbares Berichtswesen unterstützt den IT-Sicherheitsbeauftragten dabei, IT-Grundschutz umzusetzen.

Nach § 18 Abs. 2 Satz 1 BDSG sind öffentliche Stellen verpflichtet, ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen zu führen. Nach § 18 Abs. 2 Satz 2 haben öffentliche Stellen eine Übersicht über ihre Dateien, nach dem BDSG-Entwurf ihrer automatisierten Verarbeitungen zu führen. Mit Blick auf die rechtliche Verpflichtung, diese Verzeichnisse führen zu müssen, habe ich dem BSI empfohlen, bei der Überarbeitung des IT-Grundschutztools Hilfen zur Erstellung dieser Verzeichnisse vorzusehen. Für die Dateienübersicht, das Verzeichnis der automatisierten Verarbeitungen sollte dabei bereits auf den Datenkatalog des BDSG-Entwurfs abgestellt werden (s. § 18 i. V. mit § 4e BDSG-Entwurf).

8.11.2 Automatisierter IT-Sicherheitscheck

Immer wieder stelle ich bei Kontrollen fest, dass mit der Vernetzung, der steigenden Anzahl von Clients und Servern im Netz die Komplexität eines Netzwerkes derart steigt, dass eine sichere Administration nur unter Zuhilfenahme eines Software-Werkzeuges möglich ist. Für Netzwerke, die unter dem Betriebssystem Novell Netware laufen, habe ich bereits in meinem 16. TB (Nr. 33.2) über meine Erfahrungen mit dem Einsatz eines solchen Audit-Tools berichtet und ihn empfohlen. Da sich zwischenzeitlich die Produktpalette im Bereich der Netzwerke um einige Unix-Produkte erweitert hat, habe ich jetzt auch den Betrieb von Netzwerken auf Unix-Basis genauer untersucht.

Der Einsatz von Unix-Systemen bringt für den Administrator eine Menge Aufgaben mit sich, die sich von der Installation über den Betrieb bis zur Wartung und Pflege sowie den Test des Systems erstreckt. Aufgrund der Kenntnis dieser schwierigen Situation, hat sich das BSI vor einiger Zeit entschlossen, ein Administrationstool zu entwickeln, das die Arbeit der Systemverwaltung beim Einsatz von Unix-Systemen unterstützt und erleichtert. Dieses Tool – **„Sichere Unix-Administration (USEIT)“** –, das jetzt in einer stabilen Version für eine Vielzahl von verschiedenen Unix-Systemen vorliegt, wird leider im Bereich der Bundesverwaltung viel zu wenig genutzt. Gerade in großen Netzwerken, in denen mehrere hundert Server unter dem Betriebssystem Unix laufen, sehe ich hierfür notwendige Einsatzmöglichkeiten, denn die Sicherheit eines Unix-Systems ist grundlegend von der Erkennung systembedingter Sicherheitslücken und der Nutzung der systemeigenen Sicherheitsfunktionen abhängig. Die Überprüfung, ob Grundschutz im System eingestellt ist, ist erfahrungsgemäß sehr aufwendig und eigentlich nur automatisiert zufriedenstellend zu erreichen. Diese Aufgabe sollte deshalb einem Tool übertragen werden. Das vom BSI entwickelte Tool führt automatisierte oder manuelle sicherheitsrelevante Prüfungen durch, die insgesamt zu einem sicheren Betrieb führen. Schwachstellen werden analysiert und mit einer Handlungsanweisung zu deren Behebung an die Systemadministration versehen. Ferner kann mit Hilfe dieses Tools der Schutz im Unix-System so eingestellt werden, dass definierte Angriffe auf das System erkannt werden können. Auch in diesem Fall wird die Systemverwaltung mit einer Liste von ausführlichen Hinweisen, wie diesen zu begegnen ist, alarmiert.

Aufgrund meiner Anregungen wird das Tool nunmehr im Bereich der Bundesfinanzverwaltung eingesetzt; die Bundesanstalt für Arbeit prüft derzeit noch den Einsatz. Ich empfehle allerdings den Einsatz dieses Tools in allen Behörden der Bundesverwaltung, in denen Unix-Systeme verwendet werden. Das Tool unterstützt auch meine Kon-

trollen in erheblichen Umfang, da über entsprechende Reports der Sicherheitszustand eines Servers sehr schnell und einfach festgestellt werden kann.

8.12 Ausschluss unzuverlässiger Unternehmer

In meinem 17. TB (Nr. 8.15) habe ich über den Beschluss der Bundesregierung berichtet, Maßnahmen gegen unzuverlässige Unternehmen einzuleiten. Gegenüber ersten Überlegungen ist der Katalog der Verfehlungen, die eine Unzuverlässigkeit begründen, zwischenzeitlich ausgeweitet worden. Dazu gehören nunmehr u. a. Verstöße gegen das Tarifvertragsgesetz, das Gesetz zur Bekämpfung der Schwarzarbeit, das Gesetz zur Regelung der gewerbsmäßigen Arbeitnehmerüberlassung, das Gesetz über zwingende Arbeitsbedingungen bei grenzüberschreitenden Dienstleistungen und verschiedene Regelungen des Sozialgesetzbuches, des Strafgesetzbuches und des Gesetzes gegen Wettbewerbsbeschränkung, wenn diese als Ordnungswidrigkeit bzw. Straftat geahndet wurden. Die Bundesregierung will derart unzuverlässige Unternehmen künftig von der Vergabe öffentlicher Aufträge ausschließen. Darüber hinaus wird eine Vertragspartnerschaft der öffentlichen Hand mit einem Unternehmen, das durch Korruption oder Preisabsprachen Einfluss auf die Vergabeentscheidung zu nehmen versucht hat, für grundsätzlich nicht zumutbar gehalten.

Um als unzuverlässig erkannte Unternehmen tatsächlich von der Vergabe öffentlicher Aufträge ausschließen zu können, soll ein zentrales Register über diese Unternehmen eingerichtet werden. Dazu sollte zunächst von allen Unternehmen mit den Ausschreibungsunterlagen eine entsprechende Einwilligungserklärung in die Registerspeicherung verlangt werden. Gegen eine solche Lösung habe ich Einwände vorgetragen: Zum einen ist es ein bedenklicher Umgang mit dem Recht auf informationelle Selbstbestimmung, wenn man den Betroffenen gesetzlich zu seiner Einwilligung zwingt, und zum anderen könnte der Betroffene seine gegebene Einwilligung jederzeit gegenüber den zuständigen Stellen widerrufen, mit dem Ergebnis, dass jede weitere Verarbeitung seiner Daten – mit Ausnahme der Löschung – unzulässig wäre. Deshalb ist nunmehr eine gesetzliche Regelung dieser Datenverarbeitung geplant. Denn es liegt im Allgemeininteresse, dass Aufträge der öffentlichen Hand nur an zuverlässige Unternehmen vergeben werden.

Die Ressortabstimmung über den Gesetzentwurf war bei Redaktionsschluss noch nicht abgeschlossen.

9 Chipkarten

Weil die Miniaturisierung elektronischer Bauteile weiter Fortschritte macht, können mehr Speicherplatz und mehr Prozessorleistung auf einem Chip untergebracht werden. Chips in Chipkarten sind heute programmierbar, können Daten verschlüsseln und entschlüsseln und die dazu benötigten Schlüssel so speichern, dass sie weder ausgelesen noch verändert werden können. Weil das alles zu vertretbaren Kosten möglich ist, entwickeln sich Chipkarten zu leistungsfähigen und nützlichen Funktionsträgern.

Zu den realistisch scheinenden und zum Teil schon realisierten Funktionen gehören u. a.:

- Chipkarten als Datenträger, die jede Datenanforderung prüfen und je nach dem Ergebnis bestimmte – oder eben auch keine – Daten herausgeben,
- Signaturkarten, mit denen man eine elektronische Signatur leisten kann (s. dazu 17. TB Nr. 8.7),
- Berechtigungsnachweise, z. B. für die Nutzung von Geldautomaten und Mobiltelefonen,
- Personalausweis, Firmenausweis, Führerschein u. ä.,
- Schlüssel(ersatz) für Wohnungen, Häuser oder Autos,
- Lkw-Fahrerkarte zur Überwachung der Lenkzeiten,
- Kundenkarten mit Kredit- oder Rabattfunktionen,
- Wertträger, die aus ihrem Bestand Werte „ausgeben“ und bei Bedarf wieder aufgefüllt werden können,
- Träger von „Fahrscheinen“, die zuvor oder beim Besteigen des Verkehrsmittels mit Werten aus demselben Chip bezahlt wurden.

Die Handhabung wird immer einfacher werden, oft muss nur die Karte in ein Kartenlese- und/oder -schreibgerät gesteckt oder – bei berührungslos einsetzbaren Karten – nahe genug daran vorbeigeführt werden, und alles Weitere erfolgt automatisch. Zu diesem Weiteren gehören möglicherweise Änderungen und Ergänzungen der Daten auf der Karte und nachfolgende Verarbeitungen von der Karte gelesener und anderer Transaktionsdaten im System „hinter dem Lesegerät“. Weil das alles dem Karteninhaber nicht unbedingt bewusst ist, wäre es unredlich, das Verwenden einer Chipkarte als Einwilligung ihres Inhabers in jedwede Art der damit angestoßenen Verarbeitung seiner Daten zu werten. Bei der Novellierung des BDSG (s. o. Nr. 2.1) sollte deshalb eine klare Regelung u. a. für Transparenz sorgen.

Der Bürger, der mit der Chipkarte seine eigenen Daten in der Hand hat, kann nur dann wirklich über deren Nutzung bestimmen, wenn er weiß, was aus dem Einsatz seiner Chipkarte folgt.

9.1 Chipkarten im Gesundheitswesen

9.1.1 Gesundheitsdatenkarten

Schon vor geraumer Zeit wurden wesentliche Festlegungen für Chipkarten, die Gesundheitsdaten ihres Inhabers für Zwecke seiner zukünftigen medizinischen Betreuung enthalten sollen, sowohl national als auch international getroffen (s. 16. TB Nr. 9.2 und 17. TB Nr. 9.1). Damals wurde auch in verschiedenen lokalen Feldversuchen mit ermutigendem Erfolg erprobt, ob und wie solche Karten

in der Praxis die Bereitstellung wichtiger Gesundheitsinformationen zu Gunsten der Patienten verbessern können. Und es gab – und gibt es noch immer – einen breiten Konsens über die Prinzipien, insbesondere über die Entscheidungsrechte der Betroffenen, die zur Wahrung des hier besonders wichtigen Datenschutzes einzuhalten sind (s. 16. TB Nr. 9.2.2). Damit war eine Reihe wesentlicher Voraussetzungen geschaffen, um die Chipkarten-Technik, die mit der schon seit sechs Jahren als Versicherungsnachweis dienenden Krankenversicherten-Karte (s. dazu u. a. 15. TB Nr. 12.4) in die Praxis eingeführt worden war, nicht nur für die Verwaltungsarbeit, sondern auch für die Behandlung der Patienten zu nutzen.

Bei der Umsetzung des viel versprechenden Konzeptes in die breite Anwendung gibt es jedoch kaum relevante Fortschritte. Die Gründe dafür sind unterschiedlich und liegen keineswegs überwiegend im Bereich des Datenschutzes. Ein großes Problem ist z. B., dass für die Nutzung einer Gesundheitsdatenkarte in Arztpraxen, Krankenhäusern und beim Apotheker sowie bei anderen Leistungserbringern im Gesundheitswesen erhebliche Investitionen in Programme und Geräte erforderlich sind. Zwar nimmt man allgemein an, dass die zu erreichenden Einsparungen und andere Vorteile diesen Aufwand weit überwiegen. Wenn jedoch zu befürchten ist, dass eine Gruppe, beispielsweise die niedergelassenen Ärzte, einen wesentlichen Teil der Kosten tragen müsste, während der Nutzen fast ausschließlich bei den Patienten und den Krankenkassen zu Buche schlüge, dann wird kaum jemand die Vorlauf-Investitionen tragen wollen. Denn ohne konkrete Aussicht auf eine alle beteiligten Gruppen motivierende Verteilung der Vorteile ist der Erfolg höchst ungewiss. Hier sind Konzepte der großen Kostenträger, insbesondere der Krankenkassen gefragt und, weil vieles in diesem Bereich gesetzlich geregelt ist, der Gesetzgeber.

Eine politische Lösung ist auch für den Schutz der Gesundheitsdaten auf der Chipkarte (und bei anderen Speicherungen außerhalb einer Arztpraxis und des Gewahrsams einer Krankenanstalt) geboten, um Risiken für die Betroffenen und Hindernisse für die Entwicklung abzubauen. Würde man nämlich – was die Redlichkeit gebietet – die Patienten darauf hinweisen, dass ihre Gesundheitsdatenkarte anders als ihre Unterlagen beim Arzt der Beschlagnahme unterliegen und dass sie mit dem Mitführen ihrer Gesundheitsdaten diese aus dem Schutzbereich des Arztgeheimnisses heraus tragen, so wäre deren Interesse in vielen Fällen gedämpft. Um dieses Hindernis für die Akzeptanz und damit auch für die Entwicklung auszuräumen, hat der Deutsche Bundestag wiederholt, zuletzt in seinem Beschluss vom 24. Juli 1998 zu BT-Drs. 13/11168, die Bundesregierung aufgefordert, „*eine Gesetzesinitiative zu ergreifen, um beim Einsatz moderner Informationstechnik im Gesundheitswesen den gebotenen Schutz dieser Daten auch außerhalb von Arztpraxen und Krankenhäusern sicherzustellen*."

Aus Gesprächen mit dem BMG und dem BMJ habe ich zwar den Eindruck gewonnen, dass jetzt dort entsprechende Überlegungen angestellt werden, ein konkretes Ergebnis stand bei Redaktionsschluss aber noch aus. Konkreter scheinen die Vorstellungen des BMG über eine zur großflächigen Erprobung realitätsnaher Modelle notwendige Öffnungsklausel im SGB V zu sein, mit der für Zwecke der Entwicklung neuer Informationswege von den bislang geltenden Festlegungen abgewichen werden darf. Ohne flankierende Schutzmaßnahmen für die dann an anderen Stellen verarbeiteten Gesundheitsdaten könnte dabei ein erhebliches Vertrauensdefizit entstehen.

Neue Impulse dürfte diese Entwicklung ebenso wie andere Nutzungen moderner Informations- und Kommunikationstechnik von dem Aktionsforum Telematik im Gesundheitswesen (ATG) erhalten (s. dazu unten Nr. 25.1.1).

9.1.2 Ausweiskarten für Heilberufe

Zur automatisiert auswertbaren Legitimation von Ärzten und anderen Angehörigen von Gesundheitsberufen wird schon seit einiger Zeit die Verwendung von Chipkarten als sog. Health Professional Cards (HPC) geplant (s. auch 16. TB Nr. 9.1.2 und 17. TB Nr. 9.1.1). Auf der Basis des novellierten Signaturgesetzes (s. Nr. 33.6) sollen die HPC ihren jeweiligen Inhaber authentifizieren und in Form von sog. Attributzertifikaten seine berufliche Stellung, wie etwa Arzt einer bestimmten Fachrichtung oder Apotheker, verbürgen. Außerdem sollen die Karten die elektronische Signatur für von ihrem Inhaber zu verantwortende Daten leisten und die kryptographische Übertragung von Daten unterstützen. Weil es damit möglich sein wird, z. B. Patientenkarten nur von Personen lesen zu lassen, die sich der Karte gegenüber als zum Lesen bestimmter Daten berechtigt ausgewiesen haben, und von Kommunikationspartnern im Netz nicht nur die Verschlüsselung des Datenverkehrs, sondern zuvor auch eine zuverlässige Authentifikation zu verlangen, werden diese Karten ein wichtiges Element einer datenschutzgerechten Kommunikations-Infrastruktur für das Gesundheitswesen bilden.

Nachdem wesentliche Probleme technischer und organisatorischer Art gelöst sind, ist zu erwarten, dass im Jahr 2001 die Ausgabe solcher Karten an Ärzte beginnt, wobei die Ärztekammern jeweils die Einzelheiten des Verfahrens für ihren Zuständigkeitsbereich festlegen. Aus Kostengründen wird erwogen, einige der möglichen Funktionen lediglich als Optionen anzubieten. Das kann die Einführung erleichtern, der Verzicht auf die in der Zukunft durchweg nützlichen oder gar notwendigen Funktionen wird aber allenfalls eine Übergangserscheinung sein.

9.2 Wenig Neues von der GeldKarte

Es ist im Prinzip eine schöne Idee, eine Chipkarte als Geldbörse zu verwenden, aus der man das darauf geladene elektronische Guthaben in beliebigen Beträgen ausgeben kann, ohne sich um passende Münzen für Automaten oder zu viel Kleingeld im Portemonnaie kümmern zu müssen. Weniger gelungen ist eine Ausführung dieser Idee in Form eines nicht überziehbaren Kontos, über dessen in der Chipkarte nachgewiesenen Stand man durch elektronische Einzugsermächtigungen zu Gunsten des Akzeptanten verfügen kann. Das hat nämlich zur Folge, dass die Daten eines jeden Bezahlvorganges in einem Clearingverfahren zu dem gesondert angelegten Konto

der Karte – dem sog. Schattenkonto – geführt werden müssen. Dort bleiben sie aus handels- und steuerrechtlichen Gründen dann mit Datum, Uhrzeit, Betrag, Akzeptanz und ggf. einer Kennung zur Unterscheidung mehrerer Kassenterminals eines Akzeptanten noch für mindestens sechs Jahre gespeichert. Sie weisen damit einen mehr oder minder großen Teil des Ausgabeverhaltens des Nutzers nach.

Diese wenig datenschutzfreundliche Lösung wurde für die sog. GeldKarte (mit großem „K“) des deutschen Kreditwesens gewählt, und Millionen von Bankkunden haben schon seit Jahren in ihrer Geldautomaten-Karte einen Chip mit dieser Funktion. Weil die Banken es unterlassen hatten, die Kunden über die Datenverarbeitung zu informieren, die dem Bezahlen mit der GeldKarte folgt, habe ich das in meinem 17. TB (Nr. 9.2.1) erläutert.

Um wenigstens eine Abkürzung der unverhältnismäßig langen Speicherungsdauer der einzelnen Nutzungsdaten zu ermöglichen – etwa bis zum Ende der notwendigen Prüfungen auf Korrektheit des Ablaufs – hatte ich mich an das BMF gewandt (s. 17. TB Nr. 9.2.2). Auch in seiner Antwort auf mein zweites Schreiben hält das BMF daran fest, dass die Daten über alle Einzelzahlungen als Grundlage der Ermittlung der steuerpflichtigen Einnahmen nicht früher gelöscht werden dürfen.

Beim Informationsverhalten der Bankenseite gab es beinahe ebenso wenig Neues. Noch immer wird den Kunden nicht erläutert, welche Verarbeitungen personenbezogener Daten durch den Einsatz der GeldKarte angestoßen werden. Mitunter wird auch einfach bestritten, dass ein Schattenkonto zu jeder GeldKarte geführt wird, und besonders betont, dass lediglich ein Schattensaldo gespeichert werde, um dem Kunden bei einem Defekt seiner Karte den nicht genutzten Betrag auszahlen zu können. Die angesichts der Sachlage verständliche Scheu, hier Klartext zu bieten, führt in der Diskussion zwischen dem Zentralen Kreditausschuss (ZKA) und den Aufsichtsbehörden der Länder, die sich im Rahmen ihrer datenschutzrechtlichen Zuständigkeit um Klarheit bemühen, gelegentlich zu schwer nachvollziehbaren Äußerungen. So steht in einer Stellungnahme des ZKA vom September 2000: „*Bei den einzelnen Evidenzzentralen werden nur Schattensalden geführt, die lediglich Auskunft über den noch auf der Karte bestehenden Geldwert, aber nicht über einzelne Nutzungsvorgänge geben*“. Und schon im nächsten Satz wird angemerkt, „*dass die Evidenzzentrale mit der GeldKarte getätigte Transaktionen entsprechend den gesetzlichen Vorgaben über einen längeren Zeitraum nachweisen kann*“.

Hinsichtlich der Darstellung der Fakten ist das zwar ein gewisser Fortschritt. Bedenkt man aber, dass der Nachweis der getätigten Transaktionen das ist, was ein Konto ausmacht, und dass die einzelnen Nutzungsvorgänge nichts anderes als Transaktionen sind, so wird deutlich, dass bis zu für jedermann verständlichen und zugleich zutreffenden Erklärungen wohl noch ein weiter Weg ist. Möglicherweise gibt die zu erwartende Umsetzung der Transparenzforderungen der Datenschutzrichtlinie der EU (s. o. Nr. 2.1) hier einen neuen Impuls, diesen Weg zu gehen. Vielleicht ist das aber auch nicht mehr nötig. Denn mit gut fünf Jahren ist das System der GeldKarte – gemessen am Entwicklungstempo der Informationstechnik – schon recht alt, und sein bisheriger Erfolg war jedenfalls nicht so groß, als dass man nicht über ein verbessertes Design nachdenken könnte, das dann hoffentlich mehr Rücksicht auf den Datenschutz für die Nutzer nimmt.

9.3 Ein digitaler Dienstausweis für die Bundesbediensteten

In der 83. Sitzung des Ausschusses für Organisationsangelegenheiten (AfO) der obersten Bundesbehörden am 10. August 1998 wurde ein Vorschlag des BMI zur einheitlichen Gestaltung neuer Dienstausweise in der Bundesverwaltung angenommen. Diese Dienstausweise in Form einer Chipkarte sollen unterschiedliche Funktionalitäten enthalten, wobei bestimmte Funktionen optional sind. Ein beim BMI eingerichteter Arbeitskreis, dem auch Vertreter des BSI, BKA und BVA angehörten, erarbeitete bis Dezember 1998 hierzu ein Konzept; ich war beratend beteiligt.

Nach Fertigstellung des Konzeptes wurde das BVA vom BMI beauftragt, das Muster eines neuen Dienstausweises zu entwickeln und die Dienstausweisregelung zu überarbeiten. Angesichts der hohen Anforderungen an die Sicherheit der Lösung wurde das BSI mit der technischen Umsetzung des Konzeptes beauftragt.

Der digitale Dienstausweis soll für folgende Funktionen genutzt werden können:

- Herkömmliche Ausweisfunktion mit Lichtbild, Personalien, äußere Sicherheitskennzeichen;
- Speicherung der Merkmale für die Prüfbarkeit der Echtheit des Ausweises;
- Erzeugung digitaler Signaturen unter Speicherung und Anwendung des privaten Signaturschlüssels;
- Authentisierung, z. B. beim Zugang zu Rechnern;
- Speicherung der Schlüssel zum Ver- bzw. Entschlüsseln von Daten;
- „Elektronische Geldbörse“ und
- Berechtigungsnachweis für bestimmte Leistungen.

Für die Bediensteten wird kein Zwang bestehen, sämtliche angebotenen Funktionen zu nutzen. Welche Funktionen tatsächlich benötigt werden, hängt vom Einzelfall ab. Ressortspezifisch können weitere Angaben (z. B. der Dienstgrad im Bereich des BMVg) hinzugefügt werden.

Besonders folgende Vorteile sind mit der Einführung dieser multifunktionalen Chipkarte verbunden:

- Praktisch vollständige Fälschungssicherheit für die herkömmliche Ausweisfunktion sowie einfache und zuverlässige Nachprüfbarkeit der Echtheit des Ausweises über die digitale Signatur;
- Zuverlässige Identifikation und Authentisierung des Inhabers der Ausweiskarte, auch über Kommunikationsnetze.

10 Telekommunikation

Gegen Ende des Berichtszeitraumes, am 21. Dezember 2000, ist die Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV 1996) durch die Telekommunikations-Datenschutzverordnung (TDSV 2000) ersetzt worden. Soweit nichts anderes erwähnt ist, wird in diesem Kapitel die nunmehr gültige TDSV 2000 zitiert.

10.1 Telekommunikationsrecht

Mit Verabschiedung der Telekommunikations-Datenschutzverordnung konnte gegen Ende des Berichtszeitraumes das Datenschutzniveau im Bereich der Telekommunikation weiter gesteigert werden. Dabei hat die von der Bundesregierung mit Zustimmung des Bundesrates erlassene Rechtsverordnung zum einen die EG-Telekommunikations-Datenschutzrichtlinie 97/66/EG umgesetzt. Darüber hinaus galt es, unterschiedliche nationale Datenschutzregelungen zu harmonisieren, um für die Betroffenen Rechtssicherheit und Rechtsklarheit sicherstellen zu können.

Seit Sommer 2000 liegt nunmehr ein von der EG-Kommission erarbeiteter Entwurf für eine Neufassung der EG-Telekommunikations-Datenschutzrichtlinie vor. Damit sollen die bisherigen Bestimmungen an neue und vorhersehbare Entwicklungen auf dem Gebiet elektronischer Kommunikationsdienste und -technologien angepasst werden. Der Entwurfstext wird derzeit auf europäischer Ebene erörtert. Wann die Richtlinie in Kraft treten wird bzw. bis zu welchem Zeitraum die Mitgliedstaaten diese umzusetzen haben, steht derzeit noch nicht fest. Begleitend hierzu hatte ich auf meiner Website ein Forum eingerichtet, um allen Interessierten die Möglichkeit zur Diskussion der Kommissionsvorlage offen steht (s. auch u. Nr. 33.1).

Bedauerlicherweise ist es der Bundesregierung nicht gelungen, im Berichtszeitraum die nach § 88 Abs. 2 Telekommunikationsgesetz dringend erforderliche Telekommunikations-Überwachungsverordnung zu verabschieden. Nach Auskunft des hierfür federführenden BMWi sollen die hierzu notwendigen Arbeiten im Jahr 2001 durchgeführt werden (s. u. Nr. 10.1.3).

10.1.1 Fortschreibung des EG-Telekommunikationsdatenschutzrechts

Die europäische Telekommunikations-Datenschutzrichtlinie 97/66/EG vom 15. Dezember 1997 (Abl. Nr. L. 24/1 v. 30. Januar 1998, 1ff) sollte von den Mitgliedstaaten bis zum 24. Oktober 1998 in nationales Recht umgesetzt werden (vgl. 17. TB Nr. 10.1.4). In Deutschland ist dies mit zweijähriger Verspätung durch den Erlass der neuen Telekommunikations-Datenschutzverordnung erfolgt (s. nachfolgend Nr. 10.1.2). Auch in anderen europäischen Ländern wurden mittlerweile entsprechende Regelungen geschaffen.

Wegen der rasanten Entwicklung im Bereich der modernen Kommunikationsmöglichkeiten hat die Europäische Kommission im Juli 2000 einen Entwurf für eine EG-Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vorgelegt. Diese soll die bestehende Richtlinie vom Dezember 1997 ersetzen.

Dabei sollen keine wesentlichen inhaltlichen Änderungen an der geltenden Richtlinie vorgenommen werden, sondern lediglich die bisherigen Bestimmungen an neue und vorhersehbare Entwicklungen auf dem Gebiet elektronischer Kommunikationsdienste und -technologien angepasst werden. Der Anwendungsbereich der Richtlinie soll nicht mehr nur die Telekommunikationsdienste umfassen, sondern auf alle elektronischen Kommunikationsnetze und -dienste ausgedehnt werden. So sind beispielsweise die Begriffe „Anruf“ (= Telefonanruf) und „Nachricht“ (= E-Mail) neu definiert worden. Außerdem wird insbesondere der Bereich der Internetnutzung mit einbezogen.

Neu aufgenommen wurden auch Regelungen über die Verarbeitung sog. Standortdaten. Damit soll eine Schutzvorschrift zugunsten der Nutzer von Mobilfunkgeräten und Telematikdiensten geschaffen werden. Damit der Bürger in Zukunft nicht nur vor unerbetenen Anrufen, sondern auch gegen unerwünschte E-Mails geschützt ist, wurde der Anwendungsbereich der entsprechenden Vorschrift erweitert.

Ein wichtiger Punkt für das deutsche Datenschutzrecht ergibt sich aus den Erwägungsgründen der Richtlinie. Danach soll sich u. a. die Harmonisierung auf die Anforderungen beschränken, die notwendig sind, um zu gewährleisten, dass die Entstehung und die Weiterentwicklung neuer elektronischer Kommunikationsdienste und -netze zwischen Mitgliedstaaten nicht behindert werden. Diese Formulierung entspricht im wesentlichen der geltenden Rechtslage, so dass der deutsche Gesetzgeber auch weiterhin nicht den hohen Datenschutzstandard im deutschen Telekommunikations- bzw. Teledienstrecht senken muss.

Die neue Richtlinie könnte zum Anlass genommen werden, entsprechend den Vorgaben der EG, auch im nationalen Recht den Datenschutz in der Telekommunikation und bei den Telediensten in einem einheitlichen Gesetz zu regeln. Dies würde der „zusammenwachsenden“ Technik in beiden Bereichen entsprechen, den Anbietern von Komplettlösungen Rechtssicherheit und -klarheit verschaffen sowie den Nutzern dieser Dienste ein einheitliches und damit für sie durchschaubares Regime anbieten.

Vom Herbst letzten Jahres an hatte ich auf meiner Website ein Diskussionsforum zu den Vorschlägen der Kommission eingerichtet (s. Abb. 4). Auf diese Weise sollte allen interessierten Kreisen und jedem Bürger die Möglichkeit gegeben werden, Stellungnahmen zu dem vorgelegten Entwurf abzugeben, um diese ggf. in meiner Stellungnahme zum Entwurf der Fortschreibung des EG-Telekommunikationsdatenschutzrechts berücksichtigen zu können.

10.1.2 Die neue Telekommunikations-Datenschutzverordnung

Am 21. Dezember 2000 ist die Telekommunikations-Datenschutzverordnung (TDSV 2000) in Kraft getreten.

Abbildung 4 (zu Nr. 10.1.1)

Damit konnte ein für den Datenschutz im Bereich der Telekommunikation wichtiges Rechtssetzungsvorhaben abgeschlossen werden, dessen Geschichte sich über mehrere Jahre verfolgen lässt.

Vorläufer der neuen TDSV 2000 war die Telekommunikationsdienstunternehmen-Datenschutzverordnung vom 12. Juli 1996 (TDSV 1996), die seinerzeit aufgrund von § 10 Abs. 1 des Gesetzes über die Regulierung der Telekommunikation und des Postwesens (PTRegG) von der Bundesregierung erlassen worden war. Wie ich in meinem 17. TB (Nr.10.1.3) berichtet habe, wurde bereits kurz nach Inkrafttreten des Telekommunikationgesetzes und dem Außerkrafttreten des PTRegG deutlich, dass die TDSV 1996 an die für die Verordnung verbindlichen Vorgaben des Telekommunikationgesetzes dringend angepasst werden muss.

Dies betraf insbesondere die unterschiedlichen Kreise der Normadressaten. So richtete sich die TDSV 1996 entgegen ihrem Wortlaut nicht nur an die dort genannten öffentlichen Telekommunikationsdiensteanbieter. Da das Telekommunikationsgesetz im Verhältnis zur TDSV 1996 sowohl das höherrangige als auch das jüngere Regelwerk war, galt es, die Bestimmungen der TDSV 1996 im Lichte des Telekommunikationsgesetzes auszulegen. In bezug auf den Anwendungsbereich der Rechtsverordnung bedeutete dies, dass auch die Betreiber von sogenannten geschlossenen Benutzergruppen, d. h. von Telekommunikationsdiensten, die nur für bestimmte Dritte und nicht für jedermann angeboten werden, vom Regelungsbereich der TDSV 1996 erfasst waren.

Neben Problemen bei der Bestimmung der von Verordnung und Gesetz verpflichteten Normadressaten galt es, die für die Verarbeitung personenbezogener Daten einschlägigen, aber zum Teil unterschiedlich ausgestalteten Zulässigkeitsvoraussetzungen in Gesetz und Verordnung zu harmonisieren. So ist nach § 89 TKG in bestimmten Fällen die Datenverarbeitung und -nutzung nur zulässig, wenn der Betroffene zuvor seine Einwilligung hierzu erklärt hat. In einigen dieser Fälle ging die TDSV 1996 dagegen davon aus, dass dem betroffenen Kunden nur ein

Widerspruchsrecht gegen eine entsprechende Nutzung seiner personenbezogenen Daten zustehen sollte. Somit musste ein gleichartiger Datenschutzstandard gefunden werden.

Obwohl früh erkannt, wurden die hierzu erforderlichen Arbeiten erst aus Anlass der EG-Telekommunikations-Datenschutzrichtlinie 97/66/EG vom 15. Dezember 1997 aufgenommen, mit der innerhalb der Europäischen Gemeinschaft ein einheitliches Datenschutzniveau im Bereich der Telekommunikation geschaffen werden soll. Auch die Entwicklungen auf dem rasant wachsenden deutschen Telekommunikationsmarkt zeigten seit dem Ende des Sprachtelefondienstmonopols am 31. Dezember 1997 den Bedarf für neue, die Gegebenheiten dieses Marktes berücksichtigende Datenschutzregelungen. So waren beispielsweise die rechtlichen Rahmenbedingungen für die sogenannten Call-by-Call-Dienste (d. h. die freie Wahl des TK-Unternehmens bei jedem Anruf) in den einschlägigen Bestimmungen nicht berücksichtigt. Es war notwendig geworden, zugunsten der Nutzer von Telekommunikationsdienstleistungen Rechtssicherheit und für die von den Regelungen betroffenen TK-Unternehmen Rechtsklarheit zu schaffen. Diesem Anspruch ist die TDSV 2000 in weiten Teilen gerecht geworden.

Gleichwohl sind in die TDSV 2000 auch Bestimmungen aufgenommen worden, die für den Datenschutz im Bereich der Telekommunikation nicht förderlich sind. So haben sich die Telekommunikationsdiensteanbieter nach § 3 Abs. 4 TDSV 2000 zwar an dem Ziel der Datenvermeidung und Datensparsamkeit auszurichten. Eine über diesen Programmsatz hinausgehende Regelung enthält die Vorschrift jedoch nicht. Die Bundesregierung hat sich nicht entschließen können – wie von mir wiederholt gefordert – eine Verpflichtung der TK-Unternehmen vorzusehen, einen anonymen Zugang zu öffentlichen Telekommunikationsdienstleistungen anzubieten. Hier hätte der Verordnungsgeber eine Anleihe an § 4 Abs. 1 TDDSG machen können. Danach sind die Teledienstеanbieter verpflichtet, die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen. Diese Ungleichbehandlung zwischen Telediensten und Telekommunikationsdiensten ist angesichts des Zusammenwachsens von Informations- und Kommunikationsmedien kaum nachvollziehbar.

Datenschutzrechtlich bedenklich ist auch die in § 7 Abs. 3 Satz 3 TDSV 2000 geregelte Speicherfrist für entgeltrelevante Verbindungsdaten von einem halben Jahr nach Versendung der Rechnung. Sinnvoll wäre es gewesen, die Speicherfrist mit dem Ende der jeweiligen Verbindung beginnen zu lassen. Damit wäre ein eindeutiger und nicht im Belieben der TK-Unternehmen stehender Fristbeginn bestimmt worden. Nach gegenwärtiger Rechtslage hängt der Beginn der Speicherfrist dagegen von der Rechnungspraxis des einzelnen TK-Unternehmens ab. Eine Speicherung dieser Daten von mehr als einem Jahr nach Beendigung der Verbindung ist durchaus vorstellbar und wäre nach § 7 Abs. 3 Satz 3 TDSV 2000 auch zulässig. Im übrigen erscheint die Speicherdauer von einem halben Jahr grundsätzlich datenschutzrechtlich bedenklich.

Gleiches gilt für § 9 TDSV 2000. Diese Vorschrift betrifft die datenschutzgerechte Gestaltung von Verfahren, mit denen die Telekommunikationsunternehmen eine missbräuchliche Inanspruchnahme ihrer Leistungen durch Dritte verhindern bzw. aufdecken. Gemäß § 9 Abs. 2 Satz 1 TDSV 2000 darf für derartige Ermittlungen auf bis zu sechs Monate alte Verbindungsdaten zurückgegriffen werden. Nach bisherigem Recht durften hierfür nur diejenigen Verbindungsdaten herangezogen werden, die nicht älter als zwei Monate waren. Aufgrund meiner Erkenntnisse bei der Kontrolle von Missbrauchserkennungssystemen hatte ich der Bundesregierung gegenüber deutlich gemacht, dass eine Ausweitung des Datenbestandes für die Wirksamkeit und Tauglichkeit derartiger Systeme nicht erforderlich ist. Bedauerlicherweise wurden meine Argumente nicht berücksichtigt.

Als positives Beispiel möchte ich die datenschutzgerechte Ausgestaltung der sogenannten Fangschaltung in § 10 TDSV 2000 nennen. Danach hat das TK-Unternehmen auf Antrag seinem Kunden Auskunft über bedrohende oder belästigende Anrufe zu erteilen, damit sich der Betroffene hiergegen zur Wehr setzen kann. Datenschutzrechtlich problematisch waren in der Vergangenheit insbesondere die Fälle, bei denen das TK-Unternehmen einen bedrohenden oder belästigenden Anruf aus einem anderen als dem eigenen Netz ermittelte. Hierzu hatte ich in meinem 17. TB (Nr. 10.2.7.1) Stellung genommen und ein datenschutzgerechtes Verfahren vorgeschlagen. Diese Anregungen hat die Bundesregierung aufgegriffen. Nach § 10 Abs. 3 TDSV 2000 sind nunmehr alle an der Verbindung mitwirkenden Diensteanbieter verpflichtet, dem TK-Unternehmen des bedrohten oder belästigten Kunden die erforderlichen Auskünfte zu erteilen. Durch das nunmehr verbindlich vorgeschriebene Verfahren werden unnötige Datenübermittlungen vermieden.

Ob die TDSV 2000 länger in Kraft bleibt als ihre Vorgängerregelung, erscheint eher fraglich, nachdem die EG-Kommission im Juli 2000 den Entwurf für eine neue EG-Telekommunikations-Datenschutzrichtlinie vorgelegt hat (s. o. Nr. 10.1.1). Die Halbwertzeit von Datenschutzvorschriften im Bereich der modernen Informations- und Kommunikationsmedien scheint sich weiter zu reduzieren. Vor diesem Hintergrund appelliere ich an den Gesetz- und Verordnungsgeber, nicht nur reaktiv auf die Entwicklungen der Telekommunikationstechnik und die Gegebenheiten des Telekommunikationsmarktes zu antworten, sondern diese im Vorfeld aufzugreifen und mitzugestalten.

10.1.3 Die neue Telekommunikations-Überwachungsverordnung

Mit § 88 TKG gibt es seit Juli 1996 eine Ermächtigungsgrundlage zum Erlass einer Verordnung für die technische Umsetzung von Überwachungsmaßnahmen im Bereich der Telekommunikation. Da die Bundesregierung eine entsprechende Verordnung bislang noch nicht verabschiedet hat, werden solche Maßnahmen derzeit noch aufgrund der Fernmeldeverkehrs-Überwachungs-Verordnung (FÜV) vom 18. Mai 1995 durchgeführt.

§ 88 TKG sah in der Fassung von 1996 noch vor, dass alle Betreiber von Telekommunikationsanlagen die für die Durchführung von Maßnahmen zur Telekommunikationsüberwachung notwendigen technischen Einrichtungen auf eigene Kosten vorzuhalten haben. Diese Vorschrift wurde ein Jahr später im Rahmen des TKG-Begleitgesetzes vom 17.Dezember 1997 dahingehend geändert, dass die Betreiber von Telekommunikationsanlagen in bestimmten Fällen nach Maßgabe der noch zu erlassenden Rechtsverordnung von dieser Verpflichtung befreit werden können. Diese Ausnahme kann nach § 88 Abs. 2 S. 2 Nr. 3 TKG aus grundlegenden technischen Erwägungen oder aus Gründen der Verhältnismäßigkeit gegeben sein. Die genauen Einzelheiten sollten in der Verordnung geregelt werden. Außerdem kann von der Erfüllung einzelner technischer Anforderungen bei den Telekommunikationsanlagen abgesehen werden, bei denen ein technisch begründeter Ausnahmefall vorliegt (§ 88 Abs. 2 S. 3 TKG).

Bereits im Mai 1998 wurde der erste Entwurf für eine „Verordnung über die technische und organisatorische Umsetzung von Überwachungsmaßnahmen in der Telekommunikation (Telekommunikations-Überwachungsverordnung – TKÜV)" vorgelegt. Diese sollte die FÜV ersetzen. Der Entwurf wurde in der Öffentlichkeit sehr kontrovers diskutiert und daraufhin vom federführenden BMWi kurzfristig zurückgezogen (s. 17. TB Nr. 10.1.5.1). Das Verordnungsverfahren wurde für eine erneute Überarbeitung gestoppt. Grund für die Proteste insbesondere auf Seiten der Telekommunikationsbranche waren die im Verordnungsentwurf nur in sehr begrenztem Umfang vorgesehenen Ausnahmen von der Verpflichtung der Unternehmen, die Überwachungstechnik vorzuhalten (s. 17. TB Nr. 10.1.5.1). Es wäre wichtig und richtig gewesen, im Rahmen der Verordnung die Möglichkeit zu nutzen, großzügige Ausnahmeregelungen zu schaffen.

Im Frühjahr 1999 wurden dann vom BMWi die „Eckpunkte für den Regelungsrahmen der Rechtsverordnung nach § 88 TKG" vorgelegt. Dadurch sollten zunächst die wichtigsten Bereiche geklärt werden, die nach den Vorgaben des Gesetzes im Rahmen der Verordnung geregelt werden sollen. Gleichzeitig hat das BMWi auf die materiellen Rechtsgrundlagen zur Überwachung der Telekommunikation hingewiesen und betont, dass es die materielle Rechtslage durch die technische Verordnung nicht ändern könne.

Aus dem Eckpunktepapier ergab sich zunächst, dass man die Ausnahmemöglichkeiten, die das Gesetz bietet, in größerem Umfang nutzen wollte, als dies im Vorentwurf aus dem Jahr 1998 der Fall gewesen war. In einer Auflistung, die den Kreis der Verpflichteten und den Umfang der Pflichten aufzählte, hat das BMWi angedeutet, dass nur die öffentlichen Telekommunikationsdiensteanbieter, die ihre Leistungen jedermann gegenüber anbieten, verpflichtet sind, alle technischen Einrichtungen zur Umsetzung von Überwachungsmaßnahmen ständig vorzuhalten.

Anfang 2001 wurde der Öffentlichkeit ein neuer Entwurf einer TKÜV zur Diskussion vorgestellt. So gehören zum Kreis der Verpflichteten nur die Unternehmen, die gewerblich Telekommunikationsdienstleistungen für die Öffentlichkeit anbieten (§ 3 Nr. 19 TKG). Die Betreiber sog. Nebenstellenanlagen, unternehmensinterner Telekommunikationsanlagen und Corporate Networks gehören nicht zu dieser Gruppe. Diese müssen nach bisheriger Planung nur im möglicherweise eintretenden Einzelfall einer Abhörmaßnahme bestimmte, vor allem sicherheitsrelevante Grundsätze einhalten. Mit diesem ersten Schritt wurde ein wesentliches Anliegen des Datenschutzes berücksichtigt.

10.2 Telefonüberwachung in Deutschland

Das Thema der Telefonüberwachung war auch in den letzten Jahren von besonderem Interesse für die Öffentlichkeit, sowohl was die Überwachung durch deutsche Behörden betrifft (s. Nr. 6.4.2), als auch die mögliche Überwachung durch Geheimdienste aus dem Ausland (s. Nr. 16.4). Dabei fiel auf, dass die Zahl der Anordnungen für Überwachungsmaßnahmen in den letzten Jahren in Deutschland kontinuierlich gestiegen ist. Umso wichtiger ist es für den Schutz des Fernmeldegeheimnisses, dass die technischen Verfahren, die hier eingesetzt werden, sicher sind und von mir kontrolliert werden kann, wie die vorgelegten Beschlüsse von den Telekommunikationsunternehmen ausgeführt werden.

10.2.1 Verfahren, die der Telekommunikationsüberwachung dienen, müssen sicher sein!

Die gemäß Art. 10 GG garantierte Unverletzlichkeit des Fernmeldegeheimnisses verlangt bei der Durchführung der Telekommunikationsüberwachung eine sorgfältige Behandlung durch alle Beteiligten und eine sichere Übermittlung ausschließlich an die dazu berechtigte Stelle. Um dieser grundlegenden Anforderung gerecht zu werden, wurde für die Überwachung der Telekommunikation in Telekommunikationsnetzen zwischen den Telekommunikationsunternehmen und den Bedarfsträgern der Telekommunikationsüberwachung eine geschlossene Benutzergruppe (GBG) eingerichtet. Damit sollte verhindert werden, dass über die berechtigten Stellen hinaus Dritte von dem abgehörten Telekommunikationsvorgang Kenntnis erhalten. Gleichzeitig werden die in die GBG einzubeziehenden Anschlüsse der berechtigten Stellen vor Fehlbelegungen (Anrufblockaden) geschützt. Nach einer Übergangsfrist sollten bis zum 1. Januar 2000 alle Anschlüsse der GBG für Außenverkehre gesperrt werden.

Im letzten Quartal 1999 wurde mir bekannt, dass ein Mobilfunkunternehmen wegen Verzögerungen beim Systemlieferanten nicht termingerecht die an die GBG gestellten funktionalen Sicherheitsanforderungen erfüllen konnte. Da durch diese „Lücke im Gesamtsystem" das Grundrecht des Fernmeldegeheimnisses nicht umfassend gewährleistet werden konnte, habe ich mich dafür eingesetzt, dass die RegTP nachdrücklich auf das Mobilfunkunternehmen einwirkt, damit dieses die Sicherheitskriterien der GBG schnellstmöglich in vollem Umfange erfüllt. Bis zur Realisierung dieser Forderung galt es, eine

Lösung zu finden, die einerseits dem berechtigten Schutzinteresse der Betroffenen gerecht wurde, andererseits den eingeschränkten technischen Möglichkeiten des besagten Mobilfunkunternehmens Rechnung trug. Ich habe daher eine Übergangslösung unterstützt, nach der zwischen den Bedarfsträgern und den technisch hierzu in der Lage befindlichen Telekommunikationsunternehmen die GBG unter Erfüllung aller Sicherheitsanforderungen zeitgerecht in Betrieb genommen werden konnte. Lediglich für das eine Mobilfunkunternehmen wurden übergangsweise gewisse Abweichungen hingenommen. Dies war vertretbar, weil dieser Zeitraum voraussehbar nur sehr kurz war.

Seit Mitte 2000 erfüllt auch das betreffende Mobilfunkunternehmen alle Sicherheitsanforderungen der GBG, so dass die übertragungstechnische Sicherheit bei der Telekommunikationsüberwachung gewährleistet ist.

10.2.2 Kontrolle der Telekommunikationsüberwachung

Über den Umfang meiner Kontrollkompetenz nach § 91 Abs. 4 Satz 1 TKG i. V .m. § 24 BDSG im Zusammenhang mit TK-Überwachungsmaßnahmen, die im Auftrag von Strafverfolgungs- oder Sicherheitsbehörden durchgeführt werden, bestanden zwischen mir und einem TK-Unternehmen unterschiedliche Rechtsauffassungen.

Ein Bürger hatte in einer Eingabe den Verdacht geäußert, dass sein Telefon überwacht werde. Im Rahmen der Bearbeitung dieser Eingabe habe ich das TK-Unternehmen um Mitteilung gebeten, ob eine Maßnahme zur Überwachung der Telekommunikation gemäß § 100a StPO durchgeführt worden ist. Eine entsprechende Auskunft wurde jedoch unter Hinweis auf Art. 3 § 10 des Gesetzes zu Artikel 10 Grundgesetz (G 10) verweigert. Danach sei den für die Durchführung der Überwachungsmaßnahme in Anspruch genommenen TK-Diensteanbietern die Mitteilung der Tatsache der Überwachung des Fernmeldeverkehrs nach § 100a StPO an andere untersagt; eine Zuwiderhandlung werde mit Strafe bedroht.

Ich habe demgegenüber auf meinen Anspruch auf Auskunftserteilung beharrt. Nach § 91 Abs. 4 Satz 1 TKG i. V. m. § 24 BDSG bin ich berechtigt, den Umgang von TK-Diensteanbietern mit den von ihnen im Bereich der Telekommunikation erhobenen und verarbeiteten Daten umfassend zu kontrollieren. Dies erlaubt es mir, auch die Datenerhebung und -verarbeitung in Bezug auf durchgeführte Überwachungsmaßnahmen nach § 100a StPO im konkreten Einzelfall zu prüfen. Gegenstand der Kontrolle ist dabei nicht der zugrunde liegende Gerichtsbeschluss, sondern die datenschutzgerechte Umsetzung der Maßnahme durch das TK-Unternehmen. Um feststellen zu können, ob in einem Einzelfall eine Kontrolle notwendig ist, bin ich darauf angewiesen, von dem Diensteanbieter auf Nachfrage Informationen darüber zu erhalten, ob eine Telefonüberwachung – wie vermutet – überhaupt stattgefunden hat. Ohne eine solche Information könnte ich mein Kontrollrecht nicht ausüben und nicht überprüfen, ob das TK-Unternehmen und dessen Mitarbeiter Überwachungsmaßnahmen ordnungsgemäß auf der Grundlage und im Rahmen von gerichtlichen Anordnungen durchführen.

Da es nicht möglich war, mit dem TK-Unternehmen zu einer Einigung zu kommen, habe ich mich an die RegTP gewandt, der nach § 91 Abs. 1 TKG ebenfalls Kontrollbefugnisse für diesen Bereich zustehen. Die RegTP hat meine Rechtsauffassung bestätigt und darauf hingewiesen, dass es nicht Sinn und Zweck der Regelung des Art. 3 § 10 Abs. 1 G 10 sei, die Kontrolle durch die Aufsichtsbehörden gerade bezüglich der datenschutzgerechten Umsetzung von Überwachungsmaßnahmen nach § 100a StPO einzuschränken. Anderenfalls wäre der Umgang mit personenbezogenen Daten bei TK-Diensteanbietern im Falle von Überwachungsmaßnahmen mangels Zuständigkeit einer anderen Aufsichtbehörde einer Datenschutzkontrolle vollständig entzogen. Auch das für die Auslegung des G 10 zuständige BMI hat meine Rechtsauffassung geteilt, dass sich nicht strafbar macht, wer als Mitarbeiter eines TK-Unternehmens mir im Rahmen meiner Kontrollbefugnis Mitteilung über die Tatsache einer Überwachungsmaßnahme im Sinne des Art. 3 § 10 Abs. 1 G 10 macht. Das in dieser Bestimmung enthaltene Geheimhaltungsgebot werde durch die spezielle gesetzliche Übermittlungspflicht nach § 91 Abs. 4 Satz 1 TKG i. V. m. § 24 Abs. 4 BDSG durchbrochen, so dass die Strafbewehrung keine Anwendung finde.

Ich habe das TK-Unternehmen über die Bestätigung meiner Rechtsauffassung durch die vorgenannten Stellen unterrichtet und aufgefordert, mir in Zukunft in allen Fällen, in denen sich aus Eingaben mir gegenüber mögliche Zweifel an der ordnungsgemäßen Durchführung einer Überwachungsmaßnahme ergeben, entsprechende Auskünfte zu erteilen. Ich sehe die umstrittene Rechtsfrage nunmehr als geklärt an und gehe davon aus, dass das Unternehmen künftig seiner Auskunftspflicht nachkommen wird.

In dem konkreten Einzelfall lagen letztendlich keine Erkenntnisse vor, die mir Veranlassung zu einer Überprüfung der ordnungsgemäßen Durchführung einer TK-Überwachungsmaßnahme hätten geben können.

10.3 Das automatisierte Auskunftsverfahren nach § 90 Telekommunikationsgesetz

Mit dem automatisierten Auskunftsverfahren nach § 90 TKG können Sicherheitsbehörden bei der RegTP zu einer Rufnummer den Anschlussinhaber und zu einer Person die Telefonanschlüsse abfragen. Ich habe dieses Verfahren bereits im Vorfeld begleitet (s. 16. TB Nr. 10.4.14, 17. TB Nr. 10.1.5.3 sowie nachfolgend Nr. 34, dort Nrn. 9 und 10). Mit Aufnahme des Wirkbetriebs haben sich jedoch neue Probleme ergeben, die ich im Folgenden darstellen möchte.

10.3.1 Prepaid-Cards und die Begehrlichkeiten des Staates

Die sogenannten Prepaid-Cards sind nicht nur im Weihnachtsgeschäft der Renner bei den Mobilfunkunternehmen. Immer mehr Handy-Nutzer wollen sich nicht mehr

langfristig an ein TK-Unternehmen binden und wechseln zu einem Prepaid-Card-Angebot. Der Anteil dieser Verträge liegt bei einigen TK-Unternehmen mittlerweile bei mehr als 50 Prozent.

Die Prepaid-Card-Verträge zeichnen sich dadurch aus, dass der Kunde die Telekommunikationsdienstleistungen im voraus bezahlt. Zudem verzichtet das TK-Unternehmen auf die im Mobilfunkbereich sonst übliche Vereinbarung einer bestimmten Vertragslaufzeit, die in der Regel zwei Jahre beträgt. Da mit der Prepaid-Card nur im Rahmen des eingezahlten Guthabens telefoniert werden kann, besteht beispielsweise bei Jugendlichen mit geringem Einkommen nicht die Gefahr, die Telefonrechnung nicht bezahlen zu können. Dies macht die Prepaid-Card gerade für diesen Nutzerkreis so attraktiv. Ist die Prepaid-Card abtelefoniert, kann sie wieder aufgeladen werden. Aufgrund dieses Zahlungsverfahrens treten die TK-Unternehmen den Kunden gegenüber nicht in Vorleistung und benötigen daher auch keine persönlichen Angaben ihrer Kunden wie Name, Adresse oder Bankverbindung. Um den Verwaltungsaufwand bei der Abwicklung der Verträge zu reduzieren, würden sie gerne auf die Erhebung und Speicherung dieser Daten verzichten.

Aufgrund entsprechender verbindlicher Vorgaben seitens der RegTP ist ihnen dies aber nicht möglich. Die TK-Unternehmen sind vielmehr verpflichtet, die Identität des Käufers mittels Personaldokument festzustellen und den Namen, die Adresse sowie die Rufnummer des Kunden zu erheben. Diese Daten haben sie in ihren Kundendateien zu speichern und sie gemäß § 90 TKG für einen unmittelbaren Zugriff durch die RegTP bereitzustellen. Damit soll die RegTP in die Lage versetzt werden, bei Anfragen von Strafverfolgungs- und Sicherheitsbehörden den abfrageberechtigten Stellen Auskünfte über die dort gespeicherten Daten geben zu können. Diese Daten werden beispielsweise im Vorfeld von TK-Überwachungsmaßnahmen nachgefragt, um ausreichende Informationen für den Antrag auf Erlass eines richterlichen Überwachungsbeschlusses nach den Vorschriften der Strafprozessordnung zu erhalten (zu meinen ersten Erfahrungen mit dem Auskunftsverfahren nach § 90 TKG s. u. Nr. 10.3.2).

Gegen die Vorgaben der RegTP haben einige TK-Unternehmen vor dem Verwaltungsgericht Köln geklagt. Mit Urteil vom 22. September 2000 hat das Verwaltungsgericht Köln den Klagen stattgegeben. Danach sind die Anbieter von Mobilfunkdiensten nicht verpflichtet, bei Verträgen über Prepaid-Cards den Namen, die Adresse und die Rufnummer des Kunden zu erheben und in ihren Kundendateien für einen Abruf durch die RegTP zu speichern. Das Urteil des Verwaltungsgerichts Köln ist jedoch noch nicht rechtskräftig, da die RegTP beim Oberwaltungsgericht Münster Berufung hiergegen eingelegt hat. Zudem hat das Verwaltungsgericht Köln den Antrag auf Wiederherstellung der aufschiebenden Wirkung des Widerspruchs gegen die Auflage der RegTP abgelehnt. Es bleibt daher derzeit beim bisherigen Zustand, wonach die Diensteanbieter im Rahmen der Prepaid-Card-Verträge Bestandsdaten ihrer Kunden zu erheben und zu speichern haben.

Das Urteil des Verwaltungsgerichts Köln begrüße ich, da das Gericht damit eine anonyme Nutzung von Telekommunikationsdiensten zugelassen hat, wie ich sie seit langem fordere. Insbesondere bei der Novellierung der Telekommunikations-Datenschutzverordnung habe ich mich der Bundesregierung gegenüber für eine entsprechende Regelung eingesetzt (s. o. Nr. 10.1.2). Diese hat sich jedoch nicht entschließen können, die TK-Unternehmen zu verpflichten, ihren Kunden einen anonymen Zugang zu öffentlichen Telekommunikationsdienstleistungen anzubieten. Nach Auffassung von Strafverfolgungs- und Sicherheitsbehörden werden Prepaid-Cards auch im kriminellen Umfeld genutzt. Würde man eine anonyme Nutzung von Prepaid-Card-Produkten zulassen, würde dies nach Meinung der Bundesregierung die Arbeit von Strafverfolgungs- und Sicherheitsbehörden behindern.

Hinweisen möchte ich in diesem Zusammenhang darauf, dass es für die Teledienste bereits eine entsprechende datenschutzgerechte Regelung gibt. Nach § 4 Abs. 1 TDDSG sind die Teleddiensteanbieter verpflichtet, die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen. Auf europäischer Ebene hat sich dieser Gedanke auch für den Bereich der Telekommunikation durchgesetzt. So sieht die EG-TK-Datenschutzrichtlinie vom 15. Dezember 1997 in Erwägungsgrund 18 die Einführung eines anonymen Zugangs zu öffentlichen Telekommunikationsdiensten vor. Vor diesem Hintergrund und im Hinblick auf das weitere Zusammenwachsen von Informations- und Kommunikationsmedien wird die Bundesregierung ihre Haltung zu überprüfen haben.

10.3.2 Verfahrensdarstellung und erste Erfahrungen beim Wirkbetrieb

Das automatisierte Auskunftsverfahren nach § 90 TKG wurde Anfang des Jahres 2000 in Betrieb genommen. Die RegTP bearbeitet derzeit wöchentlich etwa 15 000 bis 20 000 Anfragen von den abfragenden Behörden. Die Netzbetreiber und Diensteanbieter werden Zug um Zug in das Verfahren aufgenommen.

Die Anfragen der berechtigten Stellen werden elektronisch mittels Datenübertragung (File Transfer), per Fax (gesichert und ungesichert) oder per Brief an die RegTP gesandt. Anfragen per File Transfer mit der höchsten Prioritätsstufe werden innerhalb von 3 Minuten beantwortet. Anfragen per Brief oder ungesichertem Fax werden nur in der niedrigsten Prioritätsstufe bearbeitet und mit einem Brief beantwortet. Jede Anfrage per Brief und Fax wird am Computer erfasst, während Anfragen mit File Transfer in Stichproben geprüft und automatisch über gesicherte Verbindungen an die Diensteanbieter übermittelt werden. Alle Telekommunikationsdiensteanbieter, die ihren Kunden eine Rufnummer zuteilen, müssen für die RegTP für diesen Zweck einen Rechner mit den Kundendateien und den dazugehörenden Einrichtungen wie Verschlüsselungsgeräte bereitstellen. Aufgrund der rechtlichen und technischen Vorgaben dürfen und können die Unternehmen nicht Kenntnis von den Abfragen erhalten.

Obwohl für die Behörden die Bereitstellung eines Zugangs für File Transfer mit einem größeren Aufwand verbunden ist, stellt sie sich als sicherste Art der Datenübermittlung dar. Es hat sich nämlich gezeigt, dass die Bearbeitung von Faxen und Briefen fehleranfällig ist. Dadurch werden „Irrläufer“ produziert, bei denen die Behörde eine Antwort erhält und nicht feststellen kann, um welche Anfrage es sich handelt. Dabei liegen die Fehler sowohl bei der RegTP, etwa wenn eine Antwort bei der Dienststelle in Frankfurt an der Oder statt in Frankfurt am Main ankommt, als auch bei den abfragenden Behörden, wenn z. B. das Aktenzeichen schwer lesbar ist und falsch wiedergegeben wird. Deshalb wäre es sinnvoll – soweit dies organisatorisch möglich ist –, Anfragen nicht von einzelnen Dienststellen per Fax, sondern zentralisiert von einer Dienststelle der Behörde mit File Transfer-Zugang zu stellen. Die Zuständigkeit hierfür liegt jedoch für die meisten Behörden bei den Bundesländern.

Bei der RegTP wird das Verfahren mit einem erheblichen Aufwand betrieben. Dies betrifft sowohl die Sicherheit – wovon sich meine Mitarbeiter bereits überzeugt haben – als auch die ständige Verfügbarkeit rund um die Uhr, denn an zwei der drei Standorte wird auch nachts gearbeitet.

10.3.3 Kontrolle des Verfahrens

Um eine Datenschutzkontrolle des Verfahrens zu ermöglichen, hat der Gesetzgeber eine Protokollierung aller Abrufe für ein Jahr vorgesehen (siehe § 90 Abs. 4 Satz 4 bis 6 TKG). Hierfür werden sämtliche Abfragen in einer Datenbank gespeichert, wobei alle Angaben außer dem Datum und einem von der RegTP intern vergebenen Aktenzeichen mit einem aufwendigen Verfahren verschlüsselt werden. Im Rahmen der in § 90 Abs. 4 Satz 4 TKG vorgesehenen Datenschutzkontrolle sind diese Daten zu entschlüsseln. Dies ist mittels zweier Chipkarten möglich, von denen eine bei der Reg TP und eine in meiner Dienststelle aufbewahrt wird. Die Verschlüsselung verhindert zwar einen Missbrauch der Daten, sie macht aber auch deren rechtmäßige Nutzung fast undurchführbar.

Ein weiteres technisches Problem betrifft den Umfang der Datenbank. Diese ist mit den Daten eines ganzen Jahres überlastet. Deshalb ist vorgesehen, die Daten auf CD-ROM zu überspielen, die nach zwölf Monaten vernichtet werden.

Mir sind zwei Fälle bekannt, in denen ein Bürger den Verdacht äußerte, dass jemand mit Verbindungen zur Polizei eine Rufnummer, die nicht in öffentlichen Verzeichnissen eingetragen war, in Erfahrung brachte. Hier war es naheliegend, in dem entsprechenden Zeitraum in der Datei nach dem Namen des Bürgers zu suchen, um prüfen zu können, ob eine solche Abfrage erfolgte und berechtigt war. Da die Entschlüsselung der Daten in den Chipkarten stattfindet und keine Suchkriterien außer dem Datum zur Verfügung standen, dauerte die Entschlüsselung der Daten des betreffenden Tages etliche Stunden. Bei einem zu überprüfenden Zeitraum von zwei Wochen wäre eine Kontrolle damit praktisch nicht durchführbar.

Um hier Abhilfe zu schaffen, habe ich mich mit der Reg TP darauf verständigt, das Datenfeld mit dem Straßennamen nicht mehr zu verschlüsseln. Damit kann ein schnelles Suchkriterium genutzt werden, aus dem allein kein Personenbezug herstellbar ist. Zudem wird die Protokolldatei gesichert gespeichert, so dass ich dieses Verfahren als sicher und datenschutzgerecht bewerte. Da es sich gerade in der Einführungsphase befindet, liegen mir bislang noch keine praktischen Erfahrungen vor. Sollte sich diese Vorgehensweise nicht bewähren, müsste ein anderes Verfahren zur Sicherstellung einer effektiven Datenschutzkontrolle entwickelt werden.

10.4 Neues vom IMSI-Catcher

Der GA 90 – besser bekannt unter der Bezeichnung IMSI-Catcher – hat in den letzten Jahren immer wieder datenschutzrechtliche Diskussionen in der Öffentlichkeit ausgelöst. Dieses Gerät ist in der Lage, die IMSI (International Mobile Subscriber Identity) eines Handys und damit letztlich den Anschlussinhaber festzustellen. Dabei simuliert der IMSI-Catcher eine Funkzelle mit starker Feldstärke, so dass sich alle Handys in einem bestimmten Umkreis nicht bei der echten Funkzelle, sondern bei der des IMSI-Catchers melden. Die Strafverfolgungs- und Sicherheitsbehörden sind an diesem Gerät sehr interessiert, da sie damit auch unbekannte Anschlussnummern ermitteln können, die ein Verdächtiger nutzt.

Der Einsatz des IMSI-Catchers ist ein erheblicher Eingriff in das Fernmeldegeheimnis der Betroffenen, denn auch die Nummern unbeteiligter, sich zufällig in seiner „Funkzelle“ befindender Handy-Nutzer werden zunächst mit erfasst. Ein zulässiger Einsatz des IMSI-Catchers ist nur aufgrund eines Gesetzes möglich. Im Rahmen des TKG-Begleitgesetzes hatten die Länder versucht, eine entsprechende Rechtsgrundlage hierfür zu schaffen (vgl. 17. TB Nr. 10.1.1). Diese Pläne wurden nach heftigen Diskussionen während des Gesetzgebungsverfahrens nicht mehr weiter verfolgt, so dass zur Zeit eine materielle Rechtsgrundlage für den Einsatz des IMSI-Catchers fehlt.

Außerdem ist für den Einsatz des Gerätes die Erteilung einer Lizenz für die Nutzung der entsprechenden Frequenz notwendig. Diese wurde für einen begrenzten Zeitraum für Versuchszwecke durch die RegTP erteilt. Nach Ablauf dieses Zeitraums hat die RegTP entschieden, keine neue Lizenz zu erteilen, weil der IMSI-Catcher Frequenzen nutzt, die den Mobilfunknetzbetreibern zur exklusiven Nutzung zugeteilt wurden.

Ob es von Seiten der Strafverfolgungs- und Sicherheitsbehörden erneut Bestrebungen gibt, eine materielle Rechtsgrundlage für den Einsatz des IMSI-Catchers zu schaffen, ist mir nicht bekannt.

10.5 Verarbeitung von Telekommunikationsdaten im Ausland

Viele in Deutschland tätige TK-Unternehmen nutzen aus wirtschaftlichen Gründen die vorhandenen technischen

Möglichkeiten, die ihnen ihre ausländischen Partnerunternehmen bieten. Bisher gab es keine spezielle Regelung für die Weitergabe von personenbezogenen Daten im Bereich der Telekommunikation an ausländische Stellen (vgl. 17. TB Nr. 10.2.12).

Die neue TDSV (s. o. Nr. 10.1.2) hat jetzt eine entsprechende Regelung in § 3 Abs. 6 getroffen. Danach ist die Übermittlung personenbezogener Daten an ausländische Stellen zulässig, soweit es für die Erbringung von Telekommunikationsdiensten, für die Erstellung oder Versendung von Rechnungen oder für die Bekämpfung des Missbrauchs von Telekommunikationsdiensten erforderlich ist. Dabei sieht der Verordnungsgeber es schon als ausreichend an, wenn z. B. die Erstellung der Rechnung im Ausland kostengünstiger ist. Die TDSV verweist im Übrigen auf die Vorschriften des BDSG in diesem Bereich.

Im Rahmen meiner Beratungs- und Kontrolltätigkeit gebe ich den TK-Unternehmen den Hinweis, dass ihre Kunden über eine Datenverarbeitung im Ausland im Rahmen des Vertragsabschlusses informiert werden sollen.

10.6 Datenschutzprobleme im Mobilfunk

Die weiter steigenden Nutzerzahlen im Mobilfunkbereich zeigen, dass sich das mobile Telefonieren in Deutschland durchgesetzt hat und aus dem alltäglichen Leben vieler Menschen nicht mehr wegzudenken ist. Aufgrund der dabei eingesetzten Technik bestehen auch in Bezug auf den Datenschutz Unterschiede zur Festnetztelefonie. So wird das Handy nicht allein zum Telefonieren genutzt, sondern ist aufgrund seiner vielfältigen Einsatzmöglichkeiten in mancher Hinsicht mit einem Computer vergleichbar. Man denke nur an die Funktionen eines Telefonbuches, eines Terminplaners sowie der Möglichkeit, über WAP (Wireless Application Protocol) den Zugang zum Internet zu eröffnen. Wie die folgenden Beiträge zeigen, führt dies im Ergebnis auch zu spezifischen Datenschutzproblemen.

10.6.1 Einsatz eines Handys als Wanze

Um sich eine Wanze, mit der man einen Raum abhören kann, zu beschaffen und einzusetzen, brauchte man früher einige kriminelle Energie. Dies gilt nicht mehr im Handy-Zeitalter. Mit einem marktüblichen Handy und einer transportablen Freisprecheinrichtung – im Laden für ein paar Mark zu kaufen – kann man sich selbst eine unauffällige Abhöreinrichtung zusammenstellen. Unterdrückt man den Anrufton und aktiviert gleichzeitig das automatische Annehmen eines Anrufes, ist die Wanze fertig.

Wenn dieses so präparierte Handy von einem anderen Telefon aus angerufen wird, schaltet es das Mikrofon ein. Gespräche in dem Raum, in dem sich das Handy befindet, können dann von außen abgehört werden. Dabei ist die Übertragungsqualität überraschend gut.

Es ist zwar strafbar, eine solche Wanze zu verwenden. Da dies aber nicht jeden abschreckt, sollte man bei vertraulichen Besprechungen auf eingeschaltete Handys im Raum achten. Geräte, die zuverlässig anzeigen, ob ein Handy in der Nähe sendet, sind leider nicht für jeden Geldbeutel erschwinglich, im professionellen Umfeld aber zu empfehlen.

An die Hersteller von Mobilfunkgeräten habe ich appelliert, dass Leistungsmerkmale, die ein unauffälliges Abhören mit geringem Aufwand ermöglichen, nicht gleichzeitig aktivierbar sein sollten.

10.6.2 Was hat die Reparatur eines Telefons mit Datenschutz zu tun?

Ein modernes Handy kann man nicht nur zum einfachen Telefonieren verwenden. Viele Handys enthalten Speicher für Telefonnummern oder Adressen, können Kurzmitteilungen speichern, an Termine erinnern, enthalten Bookmarks für häufig besuchte WAP-Seiten – und in manchen Geräten können sogar Telefaxe hinterlegt sein. Ein solches Handy (und nicht nur die darin befindliche Chip-Karte) enthält also jede Menge Informationen über den Besitzer.

Eine Journalistin hatte mich darauf aufmerksam gemacht, dass dadurch eine Reparatur zum Datenschutz-Problem werden kann. Das Handy, das sie von einer Reparatur zurückbekam, enthielt nämlich Daten eines anderen Handybesitzers. Das Gerät war nur getauscht worden, damit sie nicht zu lange auf die Reparatur ihres eigenen Geräts warten musste. Als sie dies feststellte, fragte sie sich, ob ihr altes Gerät, in dem vertrauliche Telefonnummern gespeichert waren, ebenfalls mit den Daten an einen Fremden weitergegeben wurde.

Ich kann somit nur empfehlen, die in einem Handy gespeicherten besonders schützenswerten Daten zu löschen, bevor das Handy zur Reparatur gegeben wird. Ist eine Löschung beispielsweise wegen technischer Probleme nicht mehr möglich, bleibt nur, mit dem Händler über das Problem zu sprechen. Viele Handys können Rufnummern sowohl in der Chip-Karte (SIM) als auch im Gerät selbst speichern. Ist das bei einem Handy möglich, sollten vertrauliche Telefonnummern in der Karte gespeichert und diese bei einer Reparatur aus dem Gerät genommen werden. Über die Verwendung dieser sogenannten „Telefonbuchfunktion“ sollte die Gebrauchsanleitung des Handys Auskunft geben.

Wenn es Probleme mit dem Datenschutz bei Herstellern und Händlern von Handys gibt, kann sich der Betroffene unmittelbar an die zuständige Aufsichtsbehörde für den nicht-öffentlichen Bereich wenden – eine direkte Zuständigkeit des BfD besteht hier nicht. Dennoch habe ich über die Presse an Hersteller und Reparaturbetriebe appelliert, die Datenschutzbelange ihrer Kunden zu berücksichtigen und ggf. die Daten, die in einem Gerät gespeichert sind, zu löschen, wenn es nicht an den Kunden zurückgeht.

10.6.3 Mehr Mobilität – Mehr Daten

Im Festnetz sind die personenbezogenen Daten, die die TK-Unternehmen erheben und verarbeiten, noch sehr übersichtlich. Beim Mobilfunk gibt es zusätzliche Informationen, wie beispielsweise die Standortdaten, von dem aus das Gespräch begonnen wird, oder die Seriennummer

des Endgerätes (IMEI – International Mobile Equipment Identity).

In meinem 17. TB habe ich unter Nr. 10.1.8 bereits auf die Problematik der Erhebung und Verarbeitung von Standortdaten hingewiesen: „*So gibt es bis heute in den Mobilfunknetzen keine Tarife, die tatsächlich von der Entfernung der beiden Kommunikationspartner abhängig sind; gleichwohl wird der Standort des Handy beim Gesprächsbeginn registriert.*“ Inzwischen bieten zwar alle GSM-Netzbetreiber ortsabhängige Tarife an, so dass grundsätzlich eine Nutzung von Standortdaten zulässig ist. Betrachtet man die dabei angewandten technischen Verfahren allerdings genauer, so werden auch heute noch mehr personenbezogene Daten erhoben als für die Tarifierung notwendig ist. So werden auch für Kunden, die keine ortsabhängige Tarifierung gewählt haben, ebenfalls Angaben zum Standort erhoben. In anderen Fällen werden genauere Standortinformationen gespeichert, als für die Abrechnung erforderlich ist.

Obwohl die IMEI für die Ermittlung der Gesprächskosten nicht benötigt wird, speichern einige Netzbetreiber dieses Datum. Dabei wird sie beispielsweise als Parameter im Rahmen von Missbrauchserkennungsprogrammen nach § 9 TDSV genutzt. Ein anderer Nutzungszweck gilt der Implementierung der IMEI in Verfahren zum Diebstahlschutz. Dabei können gestohlene Endgeräte anhand ihrer IMEI auf eine schwarze Liste gesetzt und im Netz gesperrt werden. Zumindest in der Vergangenheit wurde auch der rechtmäßige Eigentümer benachrichtigt.

Eine Speicherung und Nutzung der IMEI nach Beendigung der Verbindung halte ich in jedem Fall für datenschutzrechtlich problematisch. Ob beispielsweise die Nutzung eines gestohlenen und gutgläubig auf einem Flohmarkt erstandenen Handys eine „*rechtswidrige Inanspruchnahme von Telekommunikationsnetzen*“ darstellt, so dass in diesem Fall eine Datenverarbeitung nach § 9 TDSV gerechtfertigt wäre, möchte ich bezweifeln.

Ich werde mich auch in Zukunft dafür einsetzen, dass nur diejenigen Daten gespeichert werden, die aufgrund des konkret mit dem Kunden abgeschlossenen Vertrages genutzt werden dürfen. Eine Umsetzung dieser Vorgaben durch die Unternehmen ist jedoch nicht in allen Fällen kurzfristig möglich, da die hierfür einschlägigen Systeme in der Mehrzahl sehr komplexe und unternehmenskritische Anwendungen sind.

10.6.4 Wer schickt diese SMS?

Kurzmitteilungen oder SMS (Short Message Service) erfreuen sich – gerade bei den jüngeren Mobilfunkkunden – zunehmender Beliebtheit. Es gibt jedoch auch Fälle, bei denen man sich überhaupt nicht über den Erhalt einer Kurzmitteilung freut, etwa wenn diese den Empfänger bedroht oder belästigt. Hier wurde mir die Frage gestellt, ob eine „Fangschaltung“ nach § 10 TDSV auch für Kurzmitteilungen in Frage kommt. Danach kann der TK-Anbieter unter bestimmten Voraussetzungen mitteilen, von wessen Anschluss angerufen wurde.

Dies habe ich verneinen müssen, da in § 10 TDSV nur von bedrohenden oder belästigenden **Anrufen** die Rede ist. Ein Anruf bezeichnet *„eine über einen öffentlich zugänglichen Telefondienst aufgebaute Verbindung, die eine zweigleisige Echtzeit-Kommunikation ermöglicht.“* So jedenfalls definiert der „Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation“ vom 12. Juli 2000 einen Anruf. Eine Kurzmitteilung kann somit nicht als Anruf bezeichnet werden, da sie im Mobilfunknetz zwischengespeichert, also weder zweigleisig noch in Echtzeit übertragen wird.

Dies ist jedoch kein Problem, wenn die Kurzmitteilung von einem anderen Handy gesendet wurde. Dann ist die Rufnummer des Absenders in jedem Fall in der SMS enthalten. Eine Rufnummernunterdrückung ist für SMS technisch nicht vorgesehen. Dies scheint in der Praxis niemanden zu stören, da Kurzmitteilungen anders genutzt werden, als der Telefondienst. Die übermittelte Rufnummer erspart oft sogar die „Unterschrift“. Eine bessere Information der Kunden durch die Anbieter über die Übertragung der Rufnummer halte ich jedoch für angebracht.

Gleichwohl ist ein Mobilfunkteilnehmer auch dann nicht schutzlos, wenn er die übertragene Rufnummer nicht kennt. Bei strafrechtlich relevanten Handlungen haben Strafverfolgungsbehörden die Möglichkeit, den Besitzer einer unbekannten Rufnummer durch das automatisierte Auskunftsverfahren nach § 90 TKG (s. o. Nr. 10.3) zu erfragen.

Andererseits kann eine Kurzmitteilung über das Internet anonym versendet werden. Dabei ist der Absender nicht oder nur mit sehr hohem Aufwand zu ermitteln. Somit sind auch anonyme Belästigungen möglich. Diese Situation jedoch ist nicht neu, auch bei einer Postkarte oder einem Brief kann eine Absenderangabe nicht in jedem Fall überprüft werden. Deswegen sollte keine Kontrollstruktur aufgebaut werden.

Auf eine andere Art belästigender SMS wurde ich von einem Bürger aufmerksam gemacht. Er hatte eine unerwünschte Werbebotschaft auf seinem Handy erhalten, war aber in keinem öffentlichen Verzeichnis eingetragen. Die Befürchtung, dass sein TK-Unternehmen die Nummer weitergegeben habe, bestätigte sich nicht. Es stellte sich vielmehr heraus, dass der Absender mit einem Computer zufällig Rufnummern mit einer bestimmten Mobilfunk-Vorwahl ausgewählt hatte und die Mitteilungen an diese versandte.

10.7 Die neue Mobilfunkgeneration UMTS – Neue Herausforderungen für den Datenschutz

Wenn man sich in wenigen Jahren unterwegs überlegt, ins Kino zu gehen, wird voraussichtlich der erste Griff zum neuen UMTS-Handy führen. Man muss nur „Kino“ eingeben und das Programm des nächstgelegenen Kinos wird angezeigt. Man kann sich das mit Bildern untermalte

Programm ansehen und auch gleich die Karten bestellen und bezahlen. Zur Einstimmung kann man sich dann noch den Titelsong anhören. Selbstverständlich wird auch auf das Angebot des nächstgelegenen Burger-Restaurants aufmerksam gemacht – schließlich ist der Dienst gesponsert – und man kann bei dem Gewinnspiel der Restaurantkette mitmachen.

Viele Möglichkeiten, die heute das Internet bietet, werden aufgrund der schnellen Datenübertragung auf das Handy auch unterwegs verfügbar sein. Oft wird es sogar bequemer sein, da man nicht umständlich eingeben muss, wo man sich gerade aufhält. Gerade bei Notrufen kann es wichtig sein, wenn die Rettungsleitstelle den Aufenthaltsort automatisch mitgeteilt bekommt. Vielleicht wird man die E-Mails auch zuhause mit dem UMTS-Gerät lesen, da man den PC nicht extra hochfahren will. Dabei funktioniert der Ausdruck auf dem Drucker dank der neuen Funkübertragungstechnik „Bluetooth“ ganz unkompliziert ohne Kabel oder PC.

Für den Datenschutz stellen sich hier wichtige Fragen. Soll der Anbieter des TK-Dienstes genau wissen, wo man sich aufhält? Werden die „Gefahren aus dem Internet“ (s. hierzu 17. TB Nr. 8.9.2) auch für Handys drohen, z. B. durch aktive Inhalte? Auch für die Funkübertragung mit „Bluetooth“ sind Sicherheitsprobleme denkbar, wie beispielsweise eine deaktivierte Verschlüsselung. Ein UMTS-Gerät mit vielen zusätzlichen Leistungsmerkmalen wird in der Komplexität und den möglichen Fehlern bei der Konfiguration mit einem PC vergleichbar sein. Eine genaue Aussage dazu ist heute noch nicht möglich, ich möchte aber an die Hersteller und Netzbetreiber appellieren, bei der Entwicklung von Geräten und Diensten auch auf solche Sicherheitsprobleme zu achten. Wenn die Geräte weitere Funktionen übernehmen und beispielsweise als Organizer verwendet werden, enthalten sie auch zahlreiche personenbezogene Daten, die angemessen geschützt werden müssen.

Da ein Teil der erwähnten Dienste unabhängig von UMTS möglich ist, handelt es sich nicht um „Zukunftsmusik“. Bereits heute werden schon mit WAP (Wireless Application Protocol) und seit kurzem mit GPRS (General Packet Radio Service) viele der erwähnten Möglichkeiten angeboten, wenn auch nicht unbedingt mit vielen bunten Bildern. Auch bei der heutigen Mobilfunktechnik GSM (Global System for Mobile Communications) ist eine Anbindung an das Internet und eine – vielleicht etwas ungenauere – Ortung möglich. Eine hohe Datenübertragungsrate und große farbige Displays wird es aber erst in wenigen Jahren geben. Ich hoffe, dass mein Appell an die Hersteller und Entwickler dieser zukunftsweisenden Technik im Interesse des Rechtes der Bürger auf informationelle Selbstbestimmung aber auch des wirtschaftlichen Erfolges aufgenommen wird.

10.8 Spezielle datenschutzrechtliche Fragen beim Call-by-Call

Seit einigen Jahren können die Nutzer von Telekommunikationsdienstleistungen den Verbindungsnetzbetreiber, über den sie telefonieren wollen, durch Telekommunikationsvertrag frei wählen. Wer im Einzelfall nicht über das Verbindungsnetz des Vertragspartners telefonieren will, kann über eine sogenannte Verbindungsnetzbetreiber-Kennzahl, die vor der eigentlichen Rufnummer gewählt wird, die Verbindung über einen anderen Verbindungsnetzbetreiber herstellen (Call-by-Call). Von dieser Möglichkeit wird wegen der dabei regelmäßig angebotenen günstigen Tarife in großem Umfang Gebrauch gemacht. Bei Telekommunikationsverbindungen, die durch Call-by-Call zustande kommen, stellt sich jedoch das datenschutzrechtliche Problem, wann die dabei anfallenden Verbindungsdaten gelöscht werden müssen.

Nach § 6 Abs. 3 TDSV 1996 durften die Verbindungsdaten unter Kürzung der Zielrufnummer um die letzten drei Ziffern zu Beweiszwecken für die Richtigkeit der berechneten Entgelte grundsätzlich bis zu 80 Tage nach Versendung der Rechnung gespeichert werden. Beim Call-by-Call erfolgt nach § 15 TKV die Rechnungsstellung über den Diensteanbieter, der dem Kunden den Zugang zum öffentlichen Telekommunikationsnetz zur Verfügung stellt. Da dies nicht der Call-by-Call-Anbieter ist, kennt er zwar Beginn und Ende der von ihm vermittelten Verbindung. Er weiß aber nicht, wann die Rechnungsstellung durch das TK-Unternehmen erfolgt. Für ihn ist daher der Beginn der Löschungsfrist nicht tagesgenau bestimmbar. Bei Kundenreklamationen ist der Call-by-Call-Anbieter gegenüber dem Kunden beweispflichtig. Er sollte daher nach Rechnungszugang beim Kunden ebenfalls 80 Tage über die gespeicherten Verbindungsdaten verfügen.

Da die damaligen Rechtsvorschriften diesen Sachverhalt nicht erfasst und damit nicht einschlägig waren, hatte ich mit dem BMWi und der RegTP eine datenschutzverträgliche und nachprüfbare Lösung erarbeitet. Diese stellte auf den Zeitpunkt des Endes der Verbindung ab und ging davon aus, dass bis zur Versendung der Rechnung maximal 40 Tage vergehen können. Vor dem Hintergrund der durch § 6 Abs. 3 TDSV 1996 geregelten grundsätzlichen Speicherfrist von höchstens 80 Tagen hatte ich im Ergebnis erreicht, dass die Call-by-Call-Anbieter eine Speicherfrist für Verbindungsdaten von höchstens 120 Tagen seit dem Ende der Verbindung in ihren Unternehmen umgesetzt haben. Nach Ablauf dieses Zeitraumes waren die Verbindungsdaten zu löschen.

Im Rahmen der Novellierung der TDSV hatte ich die Aufnahme einer besonderen Regelung für Call-by-Call-Dienste in den Verordnungsentwurf erreicht. Diese ist jedoch leider im Zuge der Beratungen in den Gremien des Bundesrates gestrichen worden.

Die bis Dezember 2000 nach § 6 Abs. 3 TDSV 1996 geltende Speicherfrist von grundsätzlich 80 Tagen nach Rechnungsversand ist gemäß § 7 Abs. 3 TDSV neuer Fassung zur Berücksichtigung des Zeitbedarfs für die Abrechnung zwischen verschiedenen Netzbetreibern auf 6 Monate ausgedehnt worden. Ob und inwieweit die oben gefundene Lösung auf die neue Rechtslage übertragen werden kann, werde ich mit den beteiligten Stellen erörtern. Bei diesen Gesprächen ist zu berücksichtigen, dass es derzeit Überlegungen gibt, die Call-by-Call-Anbieter

selbst abrechnen zu lassen. Dies hätte die datenschutzfreundliche Wirkung, dass die Regelung des § 7 Abs. 3 TDSV auch für Call-by-Call direkt anwendbar wäre und somit Sonderregelungen entbehrlich würden.

Ein weiteres datenschutzrechtliches Problem beim Call-by-Call besteht darin, dass zwischen Kunde und Call-by-Call-Anbieter kein herkömmliches Vertragsverhältnis besteht. Ich habe insoweit mit § 7 Abs. 4 Satz 1 TDSV eine datenschutzgerechte Regelung erreichen können, nach der ausschließlich der rechnungsstellende Diensteanbieter die Kundenwünsche hinsichtlich vollständiger Speicherung bzw. vollständiger Löschung der Verbindungsdaten zu berücksichtigen hat.

10.9 Neues Verhältnis der TK-Unternehmen zu den Datenschutzinteressen ihrer Kunden

Im Berichtszeitraum haben viele TK-Unternehmen bei mir um datenschutzrechtliche Beratung nachgefragt. Dabei wurden unter anderem geplante Serviceleistungen der Unternehmen, die Einführung von Datenverarbeitungsprogrammen oder der Einsatz von Verfahren zur Auftragsverarbeitung diskutiert. Regelmäßig konnten – gemeinsam mit den Unternehmen – datenschutzgerechte Lösungen gefunden werden. Zudem veranstalte ich zweimal im Jahr einen Jour Fixe Telekommunikation, zu dem ich die TK-Unternehmen einlade. Dieses Angebot, im Expertenkreis wichtige und aktuelle Fragen des Datenschutzes im Bereich der Telekommunikation zu diskutieren, wird sehr gut angenommen. Auch das von mir im September 2000 zum Thema „Datenschutz in der Telekommunikation“ in Bonn durchgeführte Symposium traf auf große Nachfrage. All dies zeigt, dass die TK-Unternehmen die Interessen ihrer Kunden nach einem sicheren Umgang mit ihren personenbezogenen Daten wahrgenommen haben, dieses Anliegen bei ihren Angeboten und Leistungen berücksichtigen und auch damit werben. Datenschutz ist auch für diesen Bereich zu einem Marketingfaktor geworden.

10.9.1 Erarbeitung von Guidelines zur Kundeninformation

Telekommunikationsdiensteanbieter müssen ihre Kunden in angemessener Weise über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten unterrichten. Diese auch schon früher bestehende Informationspflicht wurde in der neuen TDSV konkretisiert und verstärkt. Die Vorschrift des § 3 Abs. 4 TDSV 1996 wurde um Kriterien und Maßstäbe erweitert, nach denen bestimmt werden kann, ob der Kunde in „*angemessener Weise*“ über die Verarbeitung und Nutzung seiner Daten unterrichtet worden ist. § 3 Abs. 5 TDSV 2000 fordert, dass der Kunde in allgemein verständlicher Form Kenntnis von den grundlegenden Verarbeitungstatbeständen der Daten erhält. Die Unterrichtungspflicht erstreckt sich nunmehr auch auf die einzelnen Gestaltungs- und Wahlmöglichkeiten des Kunden und wie bisher auf die Auskunfts- und Berichtigungspflicht nach dem BDSG.

Die neue Rechtslage hat bei den TK-Unternehmen Fragen nach der konkreten Gestaltung und dem notwendigen Umfang der vorgeschriebenen Datenschutzinformationen aufgeworfen. Ich habe dieses Thema deshalb mit den Unternehmen erörtert. Bei den gemeinsamen Überlegungen spielten sowohl die Verhältnisse in den oftmals überlasteten Verkaufsstellen, die eine ausreichende mündliche Information der Kunden kaum zulassen, als auch die Tatsache eine Rolle, dass die Aufnahmefähigkeit der Kunden bei der Vielzahl von Informationen begrenzt ist. Außerdem bestand Einvernehmen, dass die Allgemeinen Geschäftsbedingungen nicht für eine Unterrichtung nach § 3 Abs. 5 TDSV geeignet sind. Es kommen vielmehr nur gesonderte Informationen sowohl im Auftragsformular, als auch in einem zusätzlichen Merkblatt oder auch auf der Website der Diensteanbieter in Betracht. Im Interesse einer einheitlichen Praxis habe ich gemeinsam mit der RegTP Richtlinien bzw. Empfehlungen, sogenannte Guidelines, für die Erfüllung der Pflicht zur Kundeninformation nach § 3 Abs. 5 TDSV erarbeitet. Nach meinen Vorstellungen sollen sie einerseits Hinweise enthalten, welche Kundeninformationen notwendig sind (z. B. die grundlegenden Datenverarbeitungstatbestände, Einwilligungsvoraussetzungen, Wahlmöglichkeiten) oder wo und in welcher Form die Unterrichtung erfolgen soll. Entsprechende Formulierungsvorschläge (Muster) sind ergänzend vorgesehen. Auf der anderen Seite sind aber auch Vorgaben unerlässlich, welche Informationen zwingend in die Auftragsformulare aufgenommen werden müssen, beispielsweise alle mit einer Willenserklärung des Kunden verbundenen Vorgänge.

Einen ersten Entwurf der Guidelines habe ich den TK-Unternehmen noch vor dem Inkrafttreten der neuen TDSV vorgestellt und mit ihnen erörtert. Diese Diskussion ist noch nicht abgeschlossen. Aufgrund der bislang geführten Gespräche gehe ich von einem weitgehenden Einvernehmen zwischen den TK-Unternehmen, der RegTP und mir aus. Mit den Guidelines wird sich der Schutz der Nutzer von Telekommunikationsdienstleistungen entscheidend verbessern und damit auch den Intentionen des Verordnungsgebers bei der Änderung des § 3 Abs. 4 TDSV 1996 weitestgehend Rechnung getragen.

10.9.2 Datenschutzgerechter Auftragsannahmedienst

Vermehrt hatten sich Bürger bei mir über ein Telekommunikationsunternehmen beschwert, weil es die von ihnen geäußerten Wünsche zum Eintrag oder Nichteintrag in öffentliche gedruckte oder elektronische Kundenverzeichnisse und zur Nutzung ihrer persönlichen Daten im Auskunftsdienst, auf deren Berücksichtigung sie nach § 89 Abs. 8, 9 TKG bzw. §§ 13, 14 TDSV einen Rechtsanspruch haben, nicht berücksichtigte. Meine Kontrolle ergab, dass dies vielfach durch Arbeitsfehler verursacht wurde, die möglicherweise durch organisatorische Defizite begünstigt worden waren. Ich habe daraufhin die Arbeitsabläufe im Auftragsannahmedienst dieses Unternehmens untersucht.

Zusammenfassend musste ich feststellen, dass die Nichtberücksichtigung der Kundenwünsche vielfältige Ursa-

chen hatte, die in den Arbeitsbereichen der persönlichen Auftragsannahme im Geschäftslokal, der telefonischen Auftragsannahme, der sachlichen Auftragsbearbeitung, der für die Veröffentlichung maßgeblichen redaktionellen Bearbeitung sowie den organisatorischen und datenverarbeitungstechnischen Prozessen lagen. So verfügte das Personal teilweise nicht über die notwendigen Fachkenntnisse, wie beispielsweise über die dem Kunden nach den telekommunikationsrechtlichen Vorschriften eingeräumten Wahlmöglichkeiten. Damit konnten die Kunden auch nicht datenschutzrechtlich korrekt beraten werden.

Der Fehler setzte sich bei der datenverarbeitungsgestützten Auftragsbearbeitung fort: Dort sah die entsprechende Eingabemaske nicht alle rechtlich vorgesehenen Optionen vor. Besonders bedenklich war, dass das maßgebliche Eingabefeld softwareseitig mit der Kennzeichnung „Standardeintrag“ vorbelegt war. Dies führte dazu, dass vor allem bei der telefonischen Auftragsannahme gerade unter dem Druck hoher Arbeitsbelastung es schnell beim Standardeintrag blieb, der vorsah, dass die Kundendaten in öffentliche Verzeichnisse aufgenommen und für den Auskunftsdienst zur Verfügung gestellt werden konnten. Ich habe daher nachdrücklich – und mit Erfolg – die Aufhebung dieser Vorbelegung erbeten. Ich begrüße es, dass das Telekommunikationsunternehmen darüber hinaus das Eingabefeld mit der Kennzeichnung „Nichteintrag“ vorbesetzt hat. Dies ist besonders datenschutzfreundlich.

Auch musste ich feststellen, dass in einigen Fällen wichtige Kontrollmitteilungen an den Kunden, auf deren Grundlage dieser eine Korrektur bei nicht sachgemäßer Umsetzung seiner Wünsche hätte erwirken können, unterblieben sind, weil für deren automatische Fertigung ein bestimmtes Maskenfeld durch manuelle Eingabe besonders hätte gekennzeichnet werden müssen. Ich habe hierzu vorgeschlagen, das Eingabefeld so vorzubelegen, dass die entsprechende Kontrollmitteilung standardmäßig übersandt wird. Das Unternehmen ist meinem Vorschlag gefolgt und hat jetzt auch sichergestellt, dass die Arbeitsanweisung für die Auftragsbearbeitung der geltenden Rechtslage entspricht.

Darüber hinaus habe ich z. T. eine nicht sachgerechte Entsorgung von Auftragsunterlagen, die Möglichkeit der Einsichtnahme in Bildschirminhalte durch Unbefugte oder das Mithören eines Kundengesprächs durch unbeteiligte Kunden bemängelt.

Das Telekommunikationsunternehmen hat inzwischen weitreichende organisatorische und technische Verbesserungen umgesetzt und die datenschutzrechtliche Ausbildung seines Personals intensiviert.

Im sogenannten Veränderungsdienst, d. h. beispielsweise bei Umzug des Kunden oder Tarifwechsel, konnte aus datenverarbeitungstechnischen Gründen der bestehende Kundendatensatz nicht lediglich in einzelnen Vertragsmerkmalen verändert werden, sondern musste stets neu angelegt werden. Dadurch wurden vom Kunden im Rahmen des bisherigen Vertragsverhältnisses geäußerte und durch das Telekommunikationsunternehmen berücksichtigte Kundenwünsche – auch soweit es andere als die vorgenannten Aspekte betrifft – nicht automatisch auf das geänderte Vertragsverhältnis übernommen, sondern mussten neu abgefragt und eingegeben werden. Dies begünstigte gerade in zeitkritischen Situationen Arbeitsfehler des Personals. Ich halte diese Tatsache für einen datenschutzrechtlich sehr bedenklichen Konzeptionsmangel der Datenverarbeitungs-Organisation. Daher habe ich das Telekommunikationsunternehmen aufgefordert, durch Einführung entsprechender Software dieses Defizit zu beheben. Auch hier hat das Telekommunikationsunternehmen meine Forderung aufgegriffen und wird voraussichtlich noch im Laufe des Jahres 2001 eine korrigierte Programmversion flächendeckend einsetzen.

10.9.3 Übermittlung von Kundendaten für die Einrichtung von Auskunftsdiensten

Eine Informatik-Firma bietet an, die Dateien ihrer Kunden mit Angaben beispielsweise über Bankverbindung, Name, Beruf und Adresse zu pflegen und zu aktualisieren. Zu diesem vorhandenen Service soll ein weiteres Angebot hinzukommen, bei dem die Telefonnummern der Kunden jeweils tagesaktuell auf den neuesten Stand gebracht werden. Wie auch in den übrigen Sachbereichen soll das Angebot auf europaweiten Daten beruhen, um so den international arbeitenden Kunden den Abruf in verschiedenen Ländern zu ersparen. Die Daten aus Deutschland sind dabei ein wichtiger Baustein für dieses System.

Diese Informatik-Firma hatte mich gebeten, die Zulässigkeit der Übermittlung bestimmter Bestandsdaten von Telekommunikationsunternehmen zwecks Realisierung des beabsichtigten Angebots datenschutzrechtlich zu beurteilen. Eine solche Datenweitergabe durch Telekommunikationsunternehmen an die Informatik-Firma richtet sich nach § 12 TKG einerseits und § 28 BDSG andererseits. § 12 TKG sieht die Bereitstellung der Teilnehmerdaten für Dritte ausschließlich zum Zwecke der Aufnahme eines Auskunftsdienstes oder der Herausgabe eines öffentlichen Kundenverzeichnisses vor, während § 28 Abs. 1 Nr. 3 BDSG unter bestimmten Voraussetzungen eine Datenübermittlung zur Erfüllung eigener Geschäftszwecke der speichernden Stelle zulässt.

Nach Beteiligung des BMWi und der RegTP bin ich zu dem Ergebnis gekommen, dass im vorliegenden Fall eine Weitergabe der Daten nach § 12 TKG zulässig ist, wenn bestimmte Voraussetzungen erfüllt werden. Dies ergibt sich daraus, dass die Informatik-Firma mit ihrem Serviceangebot einen Auskunftsdienst aufnehmen will, mit dem sie die Dateien ihrer Kunden gerade im Hinblick auf die Telefonnummer auf den neuesten Stand bringt. Für die Zulässigkeit der Datenweitergabe muss folgendes sichergestellt sein:

- Es dürfen nur Daten von Personen zur Verfügung gestellt werden, die der Auskunftserteilung nach § 89 Abs. 9 Satz 2 TKG nicht widersprochen haben.
- Es darf keine laufende Datenübermittlung von Telekommunikationsunternehmen an die Informatik-Firma, sondern nur eine bedarfsorientierte Abfrage seitens der Informatik-Firma beim jeweiligen Telekommunikationsunternehmen erfolgen.

- Das Angebot darf nicht nur einem geschlossenen Kreis einzelner Nachfrager zugänglich sein, sondern muss grundsätzlich für die Öffentlichkeit angeboten werden.
- Die Verpflichtung zur Anwendung datenschutzrechtlicher Vorschriften muss Bestandteil des Vertrages zwischen der Informatik-Firma und dem jeweiligen Telekommunikationsunternehmen sein.

Wegen der Umsetzung der vorstehenden Forderungen bin ich mit den beteiligten Firmen in Kontakt.

10.9.4 Elektronische Telefonverzeichnisse

Nach wie vor gibt es Telefonkunden, die nicht möchten, dass ihre Telefonnummer nebst Anschrift in einem der zahlreichen CD-ROM-Telefonverzeichnisse eingetragen ist, die mit einem PC gelesen und ausgewertet werden können. Die Problematik hatte ich bereits in zurückliegenden Tätigkeitsberichten (vgl. 16. TB Nr. 10.4.5 und 17. TB Nr. 10.3.3) aufgegriffen. Auch im Berichtszeitraum wurden wieder Fälle an mich herangetragen, in denen Kunden in ein solches elektronisches Telefonverzeichnis eingetragen wurden, obwohl sie dies nicht gewünscht hatten. Die eigentliche Fehlerquelle hierfür lag in der Nichtberücksichtigung des Kundenwunsches durch das TK-Unternehmen infolge eines Arbeitsfehlers bei der Auftragsbearbeitung (s. o. Nr. 10.9.2). Da der Kunde über die vorgesehene Eintragung unterrichtet wird und er die Möglichkeit hat, ihr unverzüglich zu widersprechen oder sie zu korrigieren, könnten die negativen Auswirkungen eines Arbeitsfehlers an sich reduziert und unzulässige Veröffentlichungen noch verhindert werden. Dies würde allerdings voraussetzen, dass die Daten erst nach Ablauf einer – gesetzlich nicht vorgesehenen – „Widerspruchsfrist“ zur Veröffentlichung freigegeben und an CD-ROM-Hersteller weitergegeben werden. Leider wird derzeit in der Praxis nicht so verfahren. Der angelegte Kundendatensatz wird sofort freigegeben und zu vertraglich festgelegten Stichtagen an Dritte für die Aufnahme eines Auskunftsdienstes oder zwecks Herausgabe eines Telefonverzeichnisses übermittelt. Da die Stichtage für die Weitergabe der Daten zeitlich eng an den Produktionsprozess für die CD-ROM gekoppelt sind, können nachträgliche Korrekturen kaum noch berücksichtigt werden. Hierzu besteht noch Erörterungsbedarf mit den TK-Unternehmen.

Ein besonders weitreichender Fall im Zusammenhang mit der Bereitstellung von Teilnehmerdaten nach § 12 Abs. 1 TKG zum Zwecke der Aufnahme eines Auskunftsdienstes oder der Herausgabe eines Verzeichnisses der Rufnummern war folgender:

Ein großes TK-Unternehmen, das Millionen von Bestandsdaten erhebt und speichert, hat an Herausgeber elektronischer Verzeichnisse stets den Gesamtdatenbestand seiner Kunden weitergegeben und im Bestand die Daten der Kunden lediglich markiert, die einer Aufnahme in elektronische Verzeichnisse widersprochen haben. Das TK-Unternehmen konnte nach eigenen Angaben wegen mangelnder Kapazität der Rechenzentren und Umstellung der in diesem Bereich eingesetzten Datenverarbeitungsprogramme den Datenbestand nicht selbst selektieren. Stattdessen wurden die CD-ROM-Hersteller als Auftragnehmer nach § 11 BDSG vertraglich verpflichtet, die Datensätze zu verarbeiten, die nicht gekennzeichnet sind, und ihnen auferlegt, „*die Bestimmungen der TDSV einzuhalten und die datenschutzrechtliche Kennzeichnung eines Datensatzes zu beachten*“.

Diese Verfahrensweise konnte im Hinblick darauf, dass eine Datenübermittlung nur zulässig ist, wenn schutzwürdige Interessen der Betroffenen nicht verletzt werden, nicht hingenommen werden. Wer einer Veröffentlichung seiner Daten in einem elektronischen Verzeichnis widerspricht, muss sich darauf verlassen können, dass seine Daten nicht an Unternehmen weitergegeben werden, die die Herausgabe einer CD-ROM beabsichtigen. Das TK-Unternehmen hat zugesagt, die Möglichkeit für eine eigene Sortierung der Bestandsdaten nach den entsprechenden Kriterien zu schaffen. Da dies nur mit großem finanziellen, technischen und zeitlichen Aufwand möglich ist, habe ich die übergangsweise Beibehaltung des Verfahrens unter der Bedingung toleriert, dass es zeitlich angemessen befristet ist und durch Vereinbarung zusätzlicher Regelungen mit den Vertragspartnern der Charakter der Auftragsdatenverarbeitung stärker betont wird. Um weitgehend sicherzustellen, dass die unselektiert übermittelten Daten nicht missbräuchlich in elektronische Verzeichnisse aufgenommen werden, soll insbesondere die Verpflichtung zur Löschung der nicht zur Veröffentlichung freigegebenen Daten hervorgehoben werden. Die Installation des neuen Verfahrens soll im ersten Halbjahr 2001 abgeschlossen sein.

10.10 Automatisierte Missbrauchserkennung

Eine missbräuchliche Nutzung von Telekommunikationsdiensten kann gerade beim Mobilfunk zu erheblichen wirtschaftlichen Schäden bei Telekommunikationsunternehmen führen. Daher haben diese ein erhebliches Interesse daran, einen eventuellen Missbrauch automatisiert zu erkennen, um diesem schnellstmöglich wirksam zu begegnen. Nach Maßgabe des § 9 Abs. 2 TDSV dürfen die Kommunikationsunternehmen zum Zweck der Missbrauchserkennung die Bestands- und Verbindungsdaten erheben, verarbeiten und nutzen.

Da im Rahmen von automatisierten Missbrauchserkennungssystemen auch die besonders schützenswerten, dem Fernmeldegeheimnis unterliegenden Verbindungsdaten verarbeitet werden, habe ich ein derartiges System bei einem Telekommunikationsunternehmen überprüft. Grundsätzliche datenschutzrechtliche Probleme habe ich nicht festgestellt, aber einige Mängel gefunden

Aufgrund meiner Initiative hat das Telekommunikationsunternehmen u. a. folgende Verbesserungen vorgenommen:

- Das Missbrauchserkennungssystem wurde durch ein Passwort geschützt, das automatisch generiert wurde. Dies ist aus Gründen der Sicherheit nicht akzeptabel.

Das persönliche Passwort wird jetzt manuell eingegeben.

- Die im System abgelegte Liste der Zugriffsberechtigten enthielt Namen von Personen, die in dem betreffenden Fachbereich nicht mehr arbeiteten. Um eine missbräuchliche Anwendung des Systems zu vermeiden, dürfen Zugriffsrechte nur einem engen Kreis von Berechtigten erteilt werden. Die Zugriffsrechte werden nunmehr durch einen hierfür bestimmten Systemadministrator zeitnah vergeben und die Liste entsprechend gepflegt.
- In der systemeigenen Dokumentation, die nur vom Administrator eingesehen werden kann, werden alle Alarme aufgeführt, die angefallen waren bzw. verändert oder gelöscht wurden. Die Dokumentation wies personenbezogene Daten über Alarme aus, die bereits vor über einem Jahr gelöscht wurden. Eine Erforderlichkeit für diese lange Speicherdauer war nicht erkennbar; eine Speicherfrist von maximal 6 Monaten ist ausreichend. Das Telekommunikationsunternehmen hat ältere Alarme inzwischen gelöscht und prüft Möglichkeiten der Etablierung eines manuellen oder automatischen Verfahrens zur Löschung dieser Daten nach spätestens 6 Monaten.
- Zur Transparenz und zum Nachweis der Notwendigkeit der eingestellten Alarmmuster werden die Alarmgenerierungen schriftlich protokolliert. Unter dem Gesichtspunkt des „Vier-Augen-Prinzips“ werden die schriftlichen Protokolle an den betrieblichen Datenschutzbeauftragten weitergeleitet.
- Ferner prüft das Telekommunikationsunternehmen, ob die durch das Missbrauchserkennungssystem gesperrten Kunden bei einem Anrufversuch über eine automatische Ansage statt an die allgemeine Hotline des Unternehmens direkt an den für die Bearbeitung der Risikoprüfung zuständigen Fachbereich verwiesen werden können. Diese Änderung dient dazu, den Kreis der Personen, die Kenntnis von dem gegen einen Kunden bestehenden Missbrauchsverdacht erhalten, möglichst klein zu halten.

Zur Infrastruktur und Vernetzung der Systemkomponenten behalte ich mir eine ergänzende Kontrolle vor. Die weiteren Ausbaustufen des Missbrauchserkennungssystems werden von mir zeitnah begleitet.

10.11 Verfahren zur Bonitätsprüfung

Wegen der hohen wirtschaftlichen Vorleistungen der TK-Unternehmen – Subventionierung des Handys sowie sofortige Freischaltung des Kunden – ist es im Bereich des Mobilfunkes marktüblich, dass sich der Kunde vor Abschluss eines Vertrages über Telekommunikationsdienstleistungen einer Bonitätsprüfung zu unterziehen hat. Es besteht zwar die Möglichkeit, den wirtschaftlichen Risiken der Unternehmen auch durch die Hinterlegung einer entsprechenden Sicherheitsleistung seitens des Kunden zu begegnen. Hiervon wird in der Praxis aber so gut wie kein Gebrauch gemacht. Die Bonitätsprüfung ist zwar das klassische Betätigungsfeld der Wirtschaftsauskunfteien. Es sind aber bei den TK-Unternehmen verstärkt Bestrebungen zu beobachten, eigene Bonitätsprüfungsstellen zu schaffen. Auch in diesem Bereich bin ich um datenschutzrechtliche Beratung gebeten worden.

10.11.1 Neue SCHUFA-Klausel für Telekommunikationsverträge

Bonitätsprüfungen – bei Firmen, die Kredite vergeben, seit langem üblich – sind inzwischen auch bei Telekommunikationsunternehmen gängige Praxis, weil bereits von der Freischaltung des Festnetzanschlusses oder einer Mobilfunkkarte bis zur ersten Abrechnung hohe Verbindungsentgelte entstehen können. In Zusammenhang muss der Betroffene darüber unterrichtet werden, zu welchem Zweck die Speicherung und Übermittlung seiner persönlichen Daten vorgesehen ist und welche konkreten Daten im Rahmen des Bonitätsprüfungsverfahrens an wen übermittelt werden. Zudem ist er auf sein Auskunftsrecht über die gespeicherten Daten hinzuweisen.

Im Hinblick auf diese umfangreiche Informationspflicht hatte die SCHUFA – Schutzgemeinschaft für allgemeine Kreditsicherung – eine Gemeinschaftseinrichtung der kreditgebenden deutschen Wirtschaft, bereits seit einiger Zeit ihre Geschäftspartner vertraglich zur Verwendung einer im Wortlaut vorgegebenen SCHUFA-Klausel verpflichtet. Dabei war auch eine spezielle „SCHUFA-Klausel für Telekommunikationskontoanträge“ vorgesehen. Das gewährleistete in der Vergangenheit eine aus meiner Sicht begrüßenswerte einheitliche Handhabung durch Telekommunikationsunternehmen bei der Einholung der Einwilligung zur Bonitätsprüfung bei der SCHUFA. Dabei soll es auch künftig bleiben. Die SCHUFA hat im Jahr 2000 eine neue überarbeitete „SCHUFA-Klausel für Telekommunikationsanträge“ vorgestellt (s. **Anlage 29**). In der Neufassung wurde der Wortlaut an Verfahrensänderungen bei der Bonitätsprüfung angepasst, der Hinweis auf die Übermittlung von Daten an Vertragspartner im europäischen Binnenmarkt neu aufgenommen und die Klausel insgesamt sprachlich überarbeitet und gestrafft. Die neue SCHUFA-Klausel ist datenschutzgerecht. Sie entspricht dem Wortlaut der allgemeinen SCHUFA-Klausel (s. **Anlage 30**), die auch mit den obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich im „Düsseldorfer Kreis“ abgestimmt worden ist (s. u. Nr. 31.1).

In Berichtszeitraum habe ich bei der Beratung und Kontrolle von Telekommunikationsunternehmen besonderen Augenmerk darauf gerichtet, dass die SCHUFA-Klausel in Antragsformularen für Telekommunikationsdienstleistungen stets in ihrem äußeren Erscheinungsbild hervorgehoben wird (§ 4 Abs. 2 Satz 3 BDSG), so dass die Aufmerksamkeit des Kunden gezielt auf die geforderte Einwilligung zur Datenübermittlung an die SCHUFA gelenkt wird. Außerdem habe ich empfohlen, die Erklärung innerhalb des Antrages an exponierter Stelle vorzusehen. Da der Text der SCHUFA-Klausel etwas länger ist, wird oft wegen der Übersichtlichkeit des Auftragsformulars oder aus Platzgründen darauf verzichtet,

den vollständigen Wortlaut in den Hauptteil des Antrages aufzunehmen. Hierfür habe ich Verständnis. Wenn die Erklärung im Hauptteil aber nur in verkürzter Form erscheint, muss sie einen deutlichen Hinweis auf den an anderer Stelle abgedruckten oder als Anlage beigefügten vollständigen Text enthalten.

10.11.2 TK-Unternehmen richtet eigene Bonitätsprüfung ein

Neuland betrat die Deutsche Telekom AG im Jahr 1999 mit der Einführung eines konzernweiten eigenen Bonitätsprüfungsverfahrens, zu dessen Zweck zuvor die Tochtergesellschaft SolvenTec GmbH gegründet worden war. Maßgeblich hierfür war, dass die Freischaltung eines Telefonanschlusses ohne Begrenzung der Tarifeinheiten, d. h. ohne Kreditlimit, erfolgt. Dies hatte in der Vergangenheit zu Verlusten bei der Deutschen Telekom AG geführt, wenn nämlich der Kunde, nachdem er telefoniert hatte, das von ihm geforderte Entgelt nicht zahlte. Das Unternehmen erwartet, mit der Geschäftsaufnahme der SolvenTec GmbH ein wesentliches Instrument zur Verhinderung vermeidbarer Forderungsausfälle geschaffen zu haben. Dabei soll das neue Verfahren eine für den jeweiligen Geschäftszweck geeignete Bonitätsprüfung gewährleisten. Das Konzept sieht vor, dass die SolvenTec GmbH ihre Prüfung auf alle im Konzern verfügbaren Informationen über den betreffenden Kunden stützt und zusätzliche externe Erkenntnisse verarbeiten kann. Hierzu werden mit Einwilligung des Kunden Auskünfte über personenbezogene Daten von den anderen Gesellschaften innerhalb des Telekom-Konzerns und/oder weiteren Wirtschaftsauskunfteien eingeholt.

Da das Bonitätsprüfungsverfahren in mehreren Schritten eingeführt werden sollte und mit Bonitätsprüfungen für die Deutsche Telekom AG im Zusammenhang mit dem Erbringen von Telekommunikationsdienstleistungen begonnen wurde, hatte sich die Deutsche Telekom AG frühzeitig an mich gewandt und um Beratung gebeten. Zu diesem Zweck wurden mir die einschlägigen Formulierungsvorschläge für die Verwendung in Auftragsformularen, den diesen beiliegenden Informationen zum Datenschutz und den Allgemeinen Geschäftsbedingungen zur Prüfung zugeleitet. Auf Wunsch wurden mir auch der Vertrag mit der SolvenTec GmbH zur Auftragsdatenverarbeitung nebst Dienstleistungsvereinbarung und sowohl das umfangreiche Fachkonzept als auch das Sicherheitskonzept überlassen, in dem die Aspekte der Datensicherheit und des Datenschutzes berücksichtigt waren. Meine Änderungsvorschläge wurden in einem Beratungsgespräch mit der Deutschen Telekom AG erörtert und ausnahmslos übernommen. In einem weiteren Beratungsgespräch hatte ich Gelegenheit, vor Ort die einzelnen Verfahrensabläufe des Bonitätsprüfungsverfahrens näher kennen zu lernen.

Fazit: Ein nachahmenswertes Beispiel für andere TK-Unternehmen und ein gutes Beispiel dafür, dass meine Tätigkeit im Rahmen von § 91 Abs. 4 TKG sich nicht allein auf eine Datenschutzkontrolle beschränken muss, sondern dass gerade auch die präventive Beratung in datenschutzrechtlichen Angelegenheiten der Telekommunikation zum Vorteil der Kunden und des Unternehmens wirkt.

10.12 Rechnung Online

Der von einem Telekommunikationsunternehmen angebotene Service „Rechnung Online“ ermöglicht dem Kunden, die Daten seiner Rechnung über das Internet mit einem aktuellen Web-Browser online anzusehen und auf seinen PC herunterzuladen. Anschließend kann er die Daten nach Belieben mit dem eigenen PC be- und verarbeiten. Dafür bietet „Rechnung Online“ bereits selbst eine ganze Reihe von Analysemöglichkeiten im direkten Zugriff. „Rechnung Online“ kann als Standardversion oder als Komfortversion beauftragt werden. Sie steht jeweils zu den Terminen zur Verfügung, die auch für die Papierrechnung gelten. Ein ständiger Zugriff auf den tagesaktuellen Rechnungsstand ist allerdings nicht möglich.

Bei der Standardversion basiert ein großer Teil der Funktionalitäten auf einer Verarbeitung der Verbindungsdaten. Dabei wird vorausgesetzt, dass der Kunde einen Einzelverbindungsnachweis beauftragt hat und die Speicherung seiner Verbindungsdaten bis zu 80 Tage nach Übermittlung der Rechnung zulässt. Damit ist zugleich die Einsichtnahme in den Einzelverbindungsnachweis online möglich. Die Rechnungsdaten werden nicht zusätzlich gespeichert, was ich begrüße.

Die Komfortversion von „Rechnung Online“ bietet Funktionalitäten, die insbesondere am betriebswirtschaftlichen Bedarf von Unternehmen mit umfangreichem Telekommunikationsaufkommen orientiert sind. Sie kann jedoch auch von Privatkunden beauftragt werden. Hierbei ist die Beauftragung eines Einzelverbindungsnachweises und die 80-Tage-Speicherung der Verbindungsdaten nicht zwingend, da ein Großteil der Funktionalitäten nicht auf einzelne Verbindungsdaten abstellt. Um einen schnellen Zugriff auf die Daten zu ermöglichen, werden die Rechnungs- und ggf. Verbindungsdaten im Gegensatz zur Standardversion zusätzlich auf einem Server gespeichert.

Nach meinen Feststellungen wird im Gesamtsystem von „Rechnung Online“ ein angemessener datenschutzbezogener Standard sowie ein hohes Niveau an Maßnahmen zur Datensicherheit realisiert. Das Telekommunikationsunternehmen habe ich um folgende Verbesserungen gebeten:

- Aus Gründen der Rechtssicherheit und zur Vermeidung von Arbeitsfehlern sollte das Auftragsverfahren so verbessert werden, dass mit der Beauftragung der Standardversion gleichzeitig auch bestätigt wird, dass der Einzelverbindungsnachweis erstellt wird und die Verbindungsdaten 80 Tage gespeichert werden.
- Mit „Rechnung Online“ kann das Kommunikationsverhalten einzelner Familienmitglieder oder Firmenmitarbeiter differenzierter analysiert werden als bei einem rein chronologisch aufgebauten Einzelverbindungsnachweis. Ich habe daher das Telekommunikationsunternehmen gebeten, in das Auftragsformular die Aufforderung an den Kunden aufzunehmen, Familienmitglieder bzw. Firmenangehörige auch hierüber zu informieren und diesen Sachverhalt bereits in der Produktinformation deutlich zu machen.
- Alle Datenverarbeitungsabläufe in „Rechnung Online“ sind darauf zu überprüfen, ob sie zu „Datenspuren“ der

Kunden führen. Diese dürfen nur insoweit gespeichert werden, wie es für einen sicheren Betrieb des Systems unabdingbar ist.

Der insgesamt positive Eindruck findet u. a. seine Bestätigung in einem sicheren Management von Nutzerkennung und Passwort. Wegen der Umsetzung meiner Forderungen stehe ich mit dem Telekommunikationsunternehmen weiterhin im Dialog.

10.13 Datenschutzrechtliche Anforderungen bei sogenannten Flatrate-Tarifen

Der Wettbewerb auf dem Telekommunikationsmarkt führt zu ständig neuen Dienstleistungsangeboten. Aus der Sicht der Kunden ist vor allem der Tarifbereich interessant, geht es dabei doch um das liebe Geld. Als besonders kundenfreundlich werden die neuerdings angebotenen Flatrate-Tarife angesehen. Sie ermöglichen es, für einen vereinbarten Pauschalbetrag beliebig viele Telefongespräche ohne Rücksicht auf die Nutzungsdauer zu führen. Das gesamte Gebührenaufkommen in festgelegten Zeiträumen oder an bestimmten Tagen (z. B. an Wochenenden, sonn- und feiertags) ist durch den Pauschalbetrag abgegolten. Ein Angebot, das auch für die steigende Zahl von Internet-Surfern von großem Interesse ist.

Solche neuen TK-Angebote müssen allerdings stets auch datenschutzrechtlich bewertet werden. Um es vorweg zu nehmen, die Flatrate-Tarife sind aus meiner Sicht unproblematisch und sogar zu begrüßen, führen sie doch zu einer Reduzierung der Erhebung, Speicherung und Verarbeitung personenbezogener Daten und tragen dem Prinzip der Datensparsamkeit Rechnung. Für Zwecke der Entgeltberechnung ist hier nämlich die Speicherung von Verbindungsdaten über das Verbindungsende hinaus nicht erforderlich. Etwas anderes gilt nur für eine Tarifvariante, bei der dem Kunden von seinem TK-Diensteanbieter eine bestimmte Anzahl von Freiminuten angeboten wird und ihm nur die Telefongebühren in Rechnung gestellt werden, die über das vereinbarte Kontingent hinausgehen. Wie bei normalen Tarifen greifen hier die Regelungen der TDSV in Bezug auf die Verarbeitung und Nutzung der entgeltrelevanten Verbindungsdaten ein. Bei der echten Flatrate ist die Rechtslage klar: Nach § 7 Abs. 3 TDSV sind die nicht für die Berechnung des Entgelts erforderlichen Verbindungsdaten nach Beendigung der Verbindung unverzüglich zu löschen. § 6 Abs. 2 TDSV schreibt konkret die Löschung spätestens am Tag nach Beendigung der Verbindung vor. Dies hat auch zur Folge, dass die im Rahmen der Flatrate aufgekommenen Verbindungen nicht in einem Einzelverbindungsnachweis aufgeführt werden können und dürfen.

10.14 Neuer Dienst: CallGuard – Call-Center müssen vor dummen Anrufen geschützt werden –

Anrufe bei Call-Centern kommerzieller Unternehmen oder auch Beratungsstellen, wie der Telefonseelsorge, sind in der Regel für den Anrufer kostenfrei. Dies hat in der Praxis dazu geführt, dass immer mehr Anrufer diese Nummern nur zum Spaß anwählen oder sogar die Mitarbeiter belästigen. Für die Anbieter der kostenfreien Service-Rufnummern und Hotlines ist dies ein unangenehmer Zustand, weil sie durch die große Anzahl von „Junk Calls“ in ihrer eigentlichen Arbeit empfindlich gestört werden und außerdem noch unnötige Kosten entstehen.

Ein TK-Unternehmen hatte im November 1999 ein neues Leistungsmerkmal – CallGuard – angeboten, mit dem diese Junk Calls abgewehrt werden können. CallGuard wird bei einem störenden Anruf durch den jeweiligen Mitarbeiter, der den Anruf erhält, aktiviert, indem er dieses Gespräch innerhalb einer bestimmten vorher festgelegten Zeitspanne beendet. Danach wird die Rufnummer des Anrufers in eine Sperrliste eingetragen. Die Sperrliste wird bei dem TK-Unternehmen gespeichert. Weder die Mitarbeiter der Call-Center, noch die Betreiber der Call-Center haben einen Einblick in die Liste. Bei einem erneuten Versuch, diese Service-Rufnummer anzurufen, wird der Anrufer nicht mehr durchgestellt, sondern landet automatisch auf einer Ansage. Dadurch wird eine Entlastung der Service-Rufnummern erreicht.

Das Angebot des TK-Unternehmens wird zunächst in zwei Varianten angeboten. Mit CallGuard 500 sind danach bis zu 500 Einträge in der Sperrliste möglich; mindestens 50 Rufnummern müssen eingetragen sein, bevor Rufnummern aus der Liste gelöscht werden können. Mit CallGuard 5 000 können 5 000 Rufnummern eingetragen werden, hier liegt der Mindesteintrag bei 501 Einträgen. Der Kunde kann eine entsprechende Anzahl von Einträgen individuell festlegen. Dies bedeutet, dass die Rufnummern so lange auf der Sperrliste gespeichert bleiben, bis die vorgegebene Zahl erreicht ist, und erst dann überschrieben werden sollen.

Dieses Angebot ist datenschutzrechtlich problematisch, weil dadurch nicht eindeutig ist, wie lange die Nummern gespeichert werden. Es ist nämlich nach Auskunft der Telefonseelsorge, die CallGuard bereits nutzt, nicht notwendig, dass zur Abwehr von Junk Calls Rufnummern über einen längeren Zeitraum gespeichert werden. Deshalb habe ich gefordert, dass das Leistungsmerkmal nur mit einer festgelegten, kürzeren Speicherfrist angeboten werden soll.

Datenschutzfreundlicher wäre es, nicht die Rufnummer an sich zu speichern, sondern nur einen darauf bezogenen sog. Hash-Wert. Dieser wird mit Hilfe einer Hash-Funktion ermittelt, die eine Nachricht beliebiger Länge auf den Hashwert verdichtet. Diese Möglichkeit wird derzeit noch geprüft.

10.15 Zusammenarbeit mit der Regulierungsbehörde für Telekommunikation und Post

Im Telekommunikationsbereich hat auch die RegTP kraft ihres gesetzlichen Auftrags nach § 91 TKG die Einhaltung der Vorschriften des Elften Teils des TKG sicherzustellen, die bestehenden Verpflichtungen durchzusetzen sowie datenschutzrechtliche Kontrollaufgaben im Zusammenhang

mit der Verarbeitung personenbezogener Daten bei der Erbringung von Telekommunikationsdiensten wahrzunehmen.

Diese doppelte Zuständigkeit, die ich bereits in meinem 17. TB (Nr.10.1.7) näher erläutert habe, macht eine enge Kooperation unerlässlich. Zwischen der RegTP und mir besteht Einvernehmen, dass alle grundlegenden datenschutzrechtlichen Fragen gemeinsam erörtert werden und beide Seiten bei ihrer Tätigkeit besonderen Augenmerk auf die gegenseitige Information richten. Aus diesem Grund wurde die bisherige enge und gute Zusammenarbeit intensiviert. Neben regelmäßigen Gesprächen in Form eines „Jour Fixe“, bei denen zwecks Koordinierung der beiderseitigen Aufgabenerfüllung wichtige grundsätzliche datenschutzrechtliche Fragen erörtert und geklärt wurden, fanden in Einzelfällen auch gegenseitige Konsultationen statt. Dies gilt insbesondere bei der Bearbeitung von Beschwerden von Bürgern, die sich wegen einer Datenschutzverletzung sowohl an die RegTP als auch an mich gewandt hatten. Diese vertrauensvolle Zusammenarbeit umfasste auch den Erfahrungsaustausch über das Ergebnis durchgeführter Kontrollen. Beispiele für gemeinsame Erörterungen sind:

- Novellierung der Telekommunikations-Datenschutzverordnung (TDSV) (s. o. Nr. 10.1.2);
- Datenschutzgerechte Ausgestaltung von Auftragsformularen und Allgemeinen Geschäftsbedingungen bei Telekommunikationsunternehmen;
- Überarbeitung des Katalogs von Sicherheitsanforderungen (§ 87 TKG);
- Automatisiertes Auskunftsverfahren nach § 90 TKG (s. o. Nr. 10.3);
- Erarbeitung von Richtlinien, den so genannten Guidelines, für Telekommunikationsunternehmen bezüglich der Informationspflicht gegenüber ihren Kunden nach der neuen TDSV (s. o. Nr. 10.9.1).

Ich gehe davon aus, dass im Interesse der Telekommunikationskunden die Zusammenarbeit mit der RegTP auch weiterhin so effektiv bleibt.

10.16 Erfahrungsbericht: TK-Anlagen in Bundesministerien

Um einen Überblick über die Verarbeitung von Verbindungsdaten in Telefonanlagen bei den obersten Bundesbehörden zu erhalten, hatte ich gegen Ende des Berichtszeitraums an alle Bundesministerien einen Fragebogen versandt. Zudem hatte ich um Zusendung der entsprechenden Dienstvereinbarungen gebeten. Bei der Auswertung der Fragebögen fiel auf, dass ein beträchtlicher Teil der Ministerien die gültigen Dienstanschlussvorschriften (DAV) vom 18. Dezember 95 nur unvollständig umsetzt. So soll etwa Uhrzeit und Dauer von Gesprächen entsprechend der DAV nicht erfasst werden, damit eine Verhaltens- und Leistungskontrolle der Mitarbeiter nicht möglich ist. Gleichwohl erfassen sieben von 15 Ministerien die Uhrzeit. Ich hatte bereits vielfach in meinen Tätigkeitsberichten darauf hingewiesen, dass die Erfassung der Uhrzeit nicht erforderlich und damit unzulässig ist (siehe z. B. 16. TB Nr. 7.8 und 15. TB Nr. 9.8.1).

Die Speicherdauer der Verbindungsdaten – in der DAV sind bis zu 3 Monaten vorgesehen – beträgt bei fünf Ministerien bis zu sechs Monaten. In einzelnen Fällen sind auch Widersprüche zwischen der jeweiligen Dienstvereinbarung und den Angaben im Fragebogen aufgetaucht. So wird beispielsweise bei einem Ministerium die Uhrzeit erfasst, obwohl dies in der Dienstvereinbarung nicht vorgesehen ist. In zwei Ministerien wird die Dienstvereinbarung erst erarbeitet. In einem anderen wurde nur angegeben, dass es keine gibt.

In drei Fällen wird eine Aufzeichnung von Gesprächen in der Dienstvereinbarung erwähnt. In einem Fall erscheinen die Regelungen angemessen, in zwei weiteren Fällen habe ich bis Redaktionsschluss noch nicht klären können, ob die Gesprächsaufzeichnung dort gerechtfertigt ist.

Andererseits sind mir auch positive Dinge aufgefallen. So wird nur in wenigen Fällen eine Fernwartung der TK-Anlage durchgeführt, und dies dann auch nur mit Wissen der Ministerien. Auf die Sicherheitsrisiken bei Fernwartung, z. B. durch Hacker, hatte ich bereits in meinem 12. TB unter Nr. 24.3 d) hingewiesen. Hervorheben möchte ich auch, dass datenschutzgerechte Sonderregelungen für die Erhebung oder Kontrolle der Verbindungsdaten bei besonders zu schützenden Nebenstellen, z. B. vom Personalrat, in allen Ministerien getroffen wurden.

Ich möchte den Datenschutzbeauftragten und den Personalvertretungen der Ministerien und der anderen Bundesbehörden dringend empfehlen, die Dienstvereinbarungen anhand der Vorgaben der DAV zu prüfen und sich die technische Umsetzung bestätigen zu lassen. Unabhängig davon werde ich die festgestellten Mängel und Probleme den betroffenen Ministerien gegenüber ansprechen und datenschutzgerechte Lösungen einfordern.

10.17 Kontrolle bei Corporate Networks

Die Vorschriften zum Datenschutz im TKG richten sich an Personen oder Unternehmen, die geschäftsmäßig Telekommunikationsdienste anbieten. Dementsprechend sind die gesetzlichen Vorschriften unabhängig von der Frage anwendbar, ob eine Gewinnerzielungsabsicht besteht oder nicht. Unerheblich ist es auch, ob Telekommunikationsdienste für die Öffentlichkeit angeboten werden, oder nur für „geschlossene Benutzergruppen“, zu denen die sog. Corporate Networks gehören. Gleichwohl differenziert die neue Telekommunikations-Datenschutzverordnung in ihren Regelungen dort wo es sachgerecht und angemessen ist zwischen geschlossenen Benutzergruppen und den Telekommunikationsunternehmen, die ihre Leistung gegenüber jedermann anbieten (s. o. Nr. 10.1.2).

Ein Schwerpunkt meiner Kontrolltätigkeit galt nach der Liberalisierung des Telekommunikationsbereiches zunächst den Diensteanbietern für die Öffentlichkeit. Im Berichtszeitraum habe ich jetzt aber auch die Telekommunikationsnetze einer Bundesbehörde und zweier Un-

ternehmen kontrolliert. In allen Fällen wurden keine gravierenden Mängel festgestellt. Die von mir festgestellten kleineren Fehler sind inzwischen behoben. Es hat sich u. a. gezeigt, dass gerade Unternehmen ein großes Eigeninteresse an der Beachtung der einschlägigen Vorschriften haben, weil sich diese auch zum Vorteil der Unternehmenssicherheit auswirken.

11 Bundeskriminalamt

11.1 Durchführung des Bundeskriminalamtgesetzes

Im Berichtszeitraum gab es Probleme mit den Errichtungsanordnungen nach § 34 BKAG und nach langer Zeit auch wieder mit neuen sog. personenbezogenen Hinweisen, die in INPOL-Dateien gespeichert werden sollen.

Zu Errichtungsanordnungen für Dateien beim BKA:

Mit der Novellierung des BKAG im Jahre 1997 mussten aufgrund der veränderten Gesetzeslage die bestehenden Errichtungsanordnungen für automatisiert betriebene Dateien beim BKA überarbeitet werden. Da diese Dateien in vielen Bereichen typengleich sind (z. B. Verbunddateien, Zentraldateien), wurden aus arbeitsökonomischen Gründen gemeinsam mit dem BMI und dem BKA Mustererrichtungsanordnungen erarbeitet. Unabhängig von den Vorgaben nach § 34 BKAG bilden sie ein Gerüst mit den entsprechenden Angaben, die auf alle Dateien eines bestimmten Typs zutreffen. Die Besonderheiten einzelner Dateien sind abweichend im Einzelfall zu regeln und in diese Mustererrichtungsanordnung einzufügen. Auf diese Weise wurde zwischen den Beteiligten eine Verfahrensregelung für ein pragmatisches und flexibles Vorgehen beim Erlass von Errichtungsanordnungen nach § 34 BKAG vereinbart.

Bei den Anhörungsverfahren zu den Errichtungsanordnungen gibt es unterschiedliche Ansichten darüber, inwieweit bei der zu benennenden Rechtsgrundlage für die jeweilige Datei die nach § 7 Abs. 6 BKAG zu erlassende Rechtsverordnung eine Rolle spielt (s. 17. TB Nr. 11.1). Ich bin der Auffassung, dass das BMI aufgrund des neuen BKAG verpflichtet ist, im Wege einer Rechtsverordnung nähere Einzelheiten zur Datenspeicherung festzulegen, da § 7 Abs. 6 BKAG eindeutig ist: *„Das Bundesministerium des Innern bestimmt mit Zustimmung des Bundesrates durch Rechtsverordnung das Nähere über die Art der Daten, die nach den §§ 8 und 9 gespeichert werden dürfen."* Das BMI ist hingegen der Auffassung, § 7 Abs. 6 BKAG komme lediglich deklaratorische Bedeutung zu. Es sieht keine Veranlassung, eine Rechtsverordnung zu erlassen. Jedoch ergibt sich aus den Materialien zum Gesetzgebungsverfahren kein Anhaltspunkt für die vom BMI vertretene Rechtsmeinung, die für mich auch deswegen nicht nachvollziehbar ist, weil diese vom Gesetzgeber im Hinblick auf mehr Flexibilität bewusst aufgenommene Verordnungsermächtigung sonst leer laufen würde.

Zu neuen personengebundenen Hinweisen:

Bereits in meinem 8. TB für das Jahre 1985 (Nr. 12.3) hatte ich unter der Überschrift *„Personengebundene Hinweise und Gefahr der sozialen Abstempelung"* darüber berichtet, dass sog. personengebundene Hinweise, u. a. „bewaffnet", „gewalttätig", „geisteskrank", „Ansteckungsgefahr" oder „Freitodgefahr", in INPOL-Dateien gespeichert werden. Die Bedenken einer sozialen Abstempelung, so habe ich immer argumentiert, müssen jedoch dann zurückstehen, wenn es um die Abwehr von Gefahren für Polizeibeamte wie auch unter Umständen für den Betroffenen selbst geht. Insoweit bietet sich an, solche Hinweise nicht in allen INPOL-Dateien, sondern nur in Fahndungsdateien aufzunehmen. Die Speicherung solcher Daten in anderen Dateien, die nicht ein unmittelbares polizeiliches Vorgehen gegenüber den Betroffenen unterstützen sollen, ist für mich problematisch. Typisches Beispiel für eine solche Datei ist der KAN.

Das Problem schien gelöst zu sein, weil lange Zeit keine neuen Hinweise dazukamen. Im Herbst 2000 teilte das BMI mir jedoch mit, dass beschlossen worden sei, den Hinweis „Straftäter einer verbotenen militanten Organisation/Vereinigung/Partei/Gruppe" (VEMO) in den Dateien „Kriminalaktennachweis" und „Arbeitsdatei PIOS innere Sicherheit" (APIS) und den Hinweis „rechtsmotiviert/Gewalttäter Rechts" (REMO) in den Dateien „Personenfahndung", „Kriminalaktennachweis" und „Erkennungsdienst" zu speichern.

Als Aussonderungsprüffrist ist keine verkürzte Frist, sondern die des dazugehörigen Personendatensatzes – in der Regel 10 Jahre – vorgesehen. Ich habe nicht nur Bedenken, ob diese Merkmale überhaupt gespeichert werden dürfen, sondern auch, ob die Frist angemessen ist. Gerade bei diesen Merkmalen ist nicht auszuschließen, dass sie schon nach kurzer Zeit nicht mehr aktuell sind. Zur rechtlichen Bewertung habe ich dem BMI mitgeteilt, dass keines dieser personenbezogenen Merkmale geeignet ist zur Eigensicherung der Polizeibeamten gem. der Regelung des § 7 Abs. 3 BKAG. Hierfür stehen bereits andere personengebundene Hinweise zur Verfügung (beispielsweise „gewalttätig", „bewaffnet"), die es dem Polizeibeamten erlauben, sich entsprechend auf eine Gefahrensituation einzustellen. Es besteht Übereinstimmung mit dem BMI, dass eine Speicherung auf der Basis des § 7 Abs. 3 BKAG nicht zulässig ist.

Somit käme allenfalls noch § 8 Abs. 2 BKAG als tragfähige Norm für die Speicherung dieser Hinweise in Betracht. Danach können weitere personenbezogene Daten von Beschuldigten und von Personen, die einer Straftat verdächtig sind, gespeichert, verändert und genutzt werden, soweit dies erforderlich ist, weil wegen der Art und Ausführung der Tat, der Persönlichkeit des Betroffenen oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass Strafverfahren gegen den Beschuldigten oder Tatverdächtigen zu führen sind. Soll eine Speicherung hierauf gestützt werden, bedarf es einer entsprechenden,

nachvollziehbaren Prognoseentscheidung. Diese dürfte allerdings nur äußerst schwer zu treffen sein. Ich habe deshalb gegenüber dem BMI angeregt, auf die Erfassung dieser beiden Hinweise zu verzichten. Das BMI teilt jedoch meine Rechtsauffassung nicht. Ziel sei es vielmehr, mit der Einführung des Hinweises „REMO“ den Polizeivollzugsbeamten in Bund und Ländern eine entsprechende personenbezogene Information bei polizeilichen Kontrollen vor Ort zukommen zu lassen, damit diese in die Lage versetzt werden, geeignete polizeipräventive oder -repressive Maßnahmen zu ergreifen.

Auch hinsichtlich der vom BMI behaupteten KAN-Relevanz dieser Daten kann ich dessen Auffassung nicht zustimmen. Ich vermag nicht zu erkennen, dass all diesen Delikten im Bereich der Prävention oder Repression von Straftaten länderübergreifende, internationale oder erhebliche Bedeutung beizumessen ist. Die hiermit verbundene grundsätzliche Speicherung für die Dauer von zehn Jahren erscheint aus meiner Sicht weder sachgemäß noch entspricht sie dem Prinzip der Verhältnismäßigkeit.

11.2 INPOL-neu

Nach etwa 10 Jahren konzeptioneller Arbeit und ersten Tests, über die ich mehrfach berichtet habe (zuletzt 17. TB Nr. 11.9), wird INPOL-neu im Jahr 2001 mit einigen Anwendungen in den Echtbetrieb gehen. Bis dahin war für den Datenschutz ein langer Weg zurückzulegen. Gemeinsam mit den Landesbeauftragten für den Datenschutz war über schwierige Probleme zu beraten. So wurden Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur

- **Auftragsdatenverarbeitung** des Bundeskriminalamtes für Polizeien der Länder

  und

- Datenspeicherung im **Kriminalaktennachweis** (KAN)

gefasst (s. u. Nrn. 11.2.1 und 11.2.2).

11.2.1 Auftragsdatenverarbeitung des BKA

Meine Besorgnis darüber, im Zusammenhang mit INPOL-neu Landesdatenbestände im Wege der Auftragsdatenverarbeitung beim BKA für die Länder zu verwalten, begründe ich vor allem damit, dass die rechtliche Grundlage, auf die diese gestützt wird (§ 2 Abs. 5 BKAG), nicht ausreichend ist. § 2 Abs. 5 wurde auf Initiative des Bundesrates vor dem Hintergrund in das neue BKAG aufgenommen, dass für die bisher in Einzelfällen geübte Praxis auch weiterhin Bedarf bestehe, wenn z. B. für ein Verfahren in einem oder mehreren Ländern nur die Datenverarbeitungsanlage und Datenverarbeitungsanwendungen des BKA eine sachgerechte Verarbeitung der anfallenden Daten ermöglichen könnten (Bundestagsdrucksache 13/1550). Bei INPOL-neu ist der Sachverhalt jedoch ein anderer. Mehrere Länder brachten vor, dass sie aufgrund des entstandenen Zeitdruckes keine eigene Datenverarbeitung mehr für den Datenbestand aufbauen könnten, der bisher auf Landesrechnern geführt wird. Teilweise wurden für die Inanspruchnahme der Auftragsdatenverarbeitung Kostengesichtspunkte oder allgemein strategische Gründe genannt. Nachdem wegen der rechtlichen Ausgangssituation zunächst lange gezögert worden war – auch das BMI stand der Auftragsdatenverarbeitung ablehnend gegenüber –, fasste der Arbeitskreis II „Innere Sicherheit“ der Ständigen Konferenz der Innenminister und Innensenatoren (IMK) der Länder am 5./6. April 2000 den Beschluss zur vorübergehenden Auftragsdatenverarbeitung von Landesdaten beim BKA. Hierfür wurde ein Zeitrahmen von 4 Jahren geplant. Die IMK hat diesen Beschluss am 5. Mai 2000 bestätigt. Die Datenschutzbeauftragten des Bundes und der Länder stellten ihre grundsätzlichen Bedenken zurück und waren bereit, eine übergangsweise Datenverarbeitung unter bestimmten Kautelen zu tolerieren, um einen verzögerten Betrieb von INPOL-neu und damit verbundene erhebliche Kosten zu vermeiden.

Die Polizei war jedoch an einer dauerhaften Auftragsdatenverarbeitung interessiert und initiierte eine erneute Beschlussfassung des AK II und der IMK mit dem Ziel einer zeitlich unbefristeten Auftragsverarbeitung. Dagegen hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder den Beschluss vom 10. Oktober 2000 (s. **Anlage 23**) gefasst. Der AK II hat sich demgegenüber aber mehrheitlich für eine dauerhafte Auftragsdatenverarbeitung ausgesprochen. Die IMK hat diesen Beschluss bestätigt.

Damit ist es leider bei der divergierenden Auslegung des BKAG geblieben. Ich habe darum dem BMI empfohlen, das BKAG entsprechend zu ändern, wenn es denn politisch wirklich als notwenig angesehen wird, das BKA als Auftragnehmer für die Länder tätig werden zu lassen, und zwar über die bisherige Möglichkeit im begründeten Einzelfall hinausgehend. Legte man hier § 11 BDSG zugrunde, hieße das, dass die Länder dem BKA einen präzisen Auftrag erteilten, in dem die Datenverarbeitung und -nutzung sowie die technischen und organisatorischen Maßnahmen festgelegt sind, die eine sichere Verarbeitung garantieren. Zu meinem Bedauern hat das BMI nicht vor, das BKAG zu präzisieren, was zwangsläufig dazu führen wird, dass die Landesbeauftragten und auch ich bei Beratungen und Kontrollen betreffend die im Rahmen von INPOL-neu vorgesehene Auftragsdatenverarbeitung in eine äußerst schwierige Lage gebracht werden.

11.2.2 Datenspeicherung im Kriminalaktennachweis

Ein weiteres Problem bei INPOL-neu betrifft die Frage, in welchem Umfang personenbezogene Daten im KAN gespeichert werden dürfen. Konkret geht es darum, ob die Polizeibehörden jede Information über eine Person im KAN speichern dürfen oder ob in der Regelung des § 2 Abs. 1 BKAG tatbestandliche Beschränkungen liegen, die dies nur dann zulassen, wenn jede Erkenntnis für sich allein genommen die gesetzlichen Voraussetzungen erfüllt. Letzteres ist die Auffassung der Datenschutzbeauftragten des Bundes und der Länder (s. **Anlage 19**). Dagegen argumentieren die Vertreter der Polizeien und das BMI mit der polizeifachlichen Notwendigkeit der Abbildung der kriminellen Historie einer Person und fordern demzufolge, dass auch solche personenbezogene Daten

zu einem bereits im KAN gespeicherten Datensatz hinzugespeichert werden dürfen, die nicht die Kriterien des § 2 Abs. 1 BKAG – Speicherung nur von Daten über Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung – erfüllen.

Der KAN ist nach der derzeit geltenden Errichtungsanordnung eine Datei, die dem Nachweis von Kriminalakten dient, die beim Bund oder bei den Ländern in Fällen schwerer oder überregional bedeutsamer Straftaten über Beschuldigte oder sonst tatverdächtige Personen angelegt wurden. Nach einem Arbeitsentwurf für die neue Errichtungsanordnung des KAN im Zusammenhang mit INPOL-neu soll die Zweckbeschreibung künftig folgendermaßen aussehen:

„Der KAN dient

- *dem Nachweis von Kriminalakten, die beim Bund und bei den Ländern in Fällen schwerer oder überregional bedeutsamer Straftaten über Beschuldigte oder sonst tatverdächtige Personen angelegt sind,*
- *der Abbildung des kriminellen Werdegangs der jeweiligen Person, in dem auch alle bei anderen Polizeidienststellen über den Beschuldigten oder Tatverdächtigen geführte Kriminalakten aufgenommen werden, die für sich genommen nicht die KAN-Zugangskriterien erfüllen, wenn mindestens eine Straftat die Zugangskriterien zum KAN erfüllt.*

Der KAN kann Daten enthalten,

- *die als solche selbst nicht ohne Weiteres die KAN-Zugangskriterien erfüllen, jedoch aufgrund einer Bewertung (Prognose) ergeben, dass diese zur Verhütung von Straftaten von länderübergreifender, internationaler oder erheblicher Bedeutung beitragen können.*

Schwere Straftaten sind,

- *Verbrechen und*
- *die in § 100a StPO aufgeführten Vergehen.*

Überregional bedeutsame Straftaten liegen vor, wenn der Verdacht besteht, auf

- *gewohnheits-, gewerbs- oder bandenmäßige Begehung,*
- *Triebtäterschaft,*
- *planmäßige überörtliche Begehung,*
- *Handeln zur Verfolgung extremistischer Ziele,*
- *Begehung unter Mitführung von Schusswaffen,*
- *internationale Betätigung,*
- *erneute Straffälligkeit des Beschuldigten oder Tatverdächtigen außerhalb ihres Wohn- oder Aufenthaltbereichs,*
- *Begehung fremdenfeindlicher Straftaten.“*

Der neue KAN wird also eine Datei sein, die von der Zweckbeschreibung und vom Datenvolumen her bereits wesentliche Weiterungen gegenüber dem jetzigen KAN enthält, und die bezogen auf die durch Gesetz zugewiesenen Aufgaben und Befugnissen der Zentralstelle, das BKA, äußerst problematisch sind. Die mir zugegangenen Arbeitsentwurfsfassungen der Errichtungsanordnungen werden gemeinsam mit der Arbeitsgruppe INPOL-neu der Datenschutzbeauftragten des Bundes und der Länder erörtert, um im Vorfeld des Anhörungsverfahrens nach § 34 BKAG möglichst weitgehenden Konsens zu erzielen. Diese Verfahrensweise bietet sich aus arbeitsökonomischer Sicht an und ist geeignet, das Anhörungsverfahren nach § 34 BKAG zu verschlanken.

11.2.3 Migration des Datenbestandes

Bevor INPOL-neu in den Echtbetrieb übergehen kann, sind noch wichtige Fragen der Migration, also des Übergangs der Daten von INPOL-aktuell zu INPOL-neu, zu lösen. Aus meiner Sicht ist dabei wichtig, dass jedenfalls nur solche Daten in INPOL-neu aufgenommen werden dürfen, die den – seit 1997 – veränderten rechtlichen Bedingungen genügen. Gegenüber der Projektgruppe INPOL-neu beim BKA weise ich bereits seit längerem im Rahmen der Erstellung der entsprechenden Konzepte darauf hin, dass nach den gesetzlichen Bestimmungen (§§ 8, 9, 32 BKAG) eine Überprüfung des gesamten Datenbestandes zu erfolgen hat. Dies ist entsprechend der datenschutzrechtlichen Verantwortung nach § 12 Abs. 2 BKAG von dem jeweiligen Datenbesitzer durchzuführen. Nachdem zu meinen bisherigen mündlichen wie auch schriftlichen Hinweisen gegenüber dem BKA nicht befriedigend Stellung genommen und mir sogar mitgeteilt wurde, dass „datenschutzrechtliche Aspekte dabei bisher noch keine wesentliche Rolle gespielt“ hätten, habe ich das BMI auf das Problem hingewiesen und deutlich gemacht, dass eine ausschließlich unter datenverarbeitungstechnischen Möglichkeiten stattfindende Selektion nicht relevanter Datensätze nicht ausreicht. Es ist anhand der Aktenunterlagen bezogen auf jeden Datensatzbesitzer im Einzelfall zu prüfen, inwieweit die Speicherungsvoraussetzungen im konkreten Fall noch erfüllt sind und ob die für jeden Datensatz festgesetzten Aussonderungsprüffristen angemessen sind.

Ich erwarte, dass diese Forderung, die letztlich auch im ureigenen polizeilichen Interesse liegt, von allen Beteiligten aufgegriffen wird und in Kürze mit den notwendigen Arbeiten zur Bestandsbereinigung beim Bund und in den Ländern begonnen wird.

11.2.4 DNA-Merker als neues Datum in INPOL-neu

Die Vertreter der Polizeien des Bundes und der Länder planen, einen sog. **DNA-Merker** in einige Dateien von INPOL-neu aufzunehmen. Dieser DNA-Merker gibt dem Nutzer einen Hinweis darauf, ob in einer speziellen Datei (DNA-Analyse-Datei – vgl. Nr. 11.5 –) Informationen über DNA-Material vorliegt, das in der Vergangenheit einer Person entnommen worden ist. Diese zusätzliche Information, die nunmehr in INPOL-neu bereitgestellt werden soll, wird dem Polizeibeamten bei jeder Abfrage

einer Personalie zur Verfügung stehen. Aus datenschutzrechtlicher Sicht wurden hiergegen bereits während der Konzeptionsphase von INPOL-neu Bedenken geäußert, weil durch die Erfassung dieses Merkmals eine stigmatisierende Wirkung im Kontakt zwischen Polizei und Bürger erzeugt werden könnte, die unter Umständen dazu führt, dass der Bürger weitergehenden Kontrollen unterzogen wird. Rechtlicher Ansatzpunkt für derartige Überlegungen sind die engen Zweckbestimmungsregelungen im DNA-Identitätsfeststellungsgesetz und in der Errichtungsanordnung für die DNA-Analyse-Datei beim BKA. Zunächst zeichnete sich in den Beratungen eine Regelung ab, wonach die Information nur über eine zweite Abfrage zur Verfügung gestellt würde. Diese Abfrage sollte durch flankierende Maßnahmen (Protokollaufzeichnung o. ä.) für Zwecke einer datenschutzrechtlichen Kontrolle abgesichert werden. Das BKA hat mir dann später auf Nachfrage mitgeteilt, dass die Realisierung dieses Vorschlages nur mit erheblichem Aufwand möglich sei und man deswegen diesem Vorschlag nicht folgen wolle. Hierbei spiele auch eine Rolle, dass bereits im jetzigen KAN darauf hingewiesen wird, wenn es zu einer Person ein DNA-Muster gibt. Auf den KAN könne im übrigen von jemanden, der berechtigt auf INPOL zugreifen darf, nicht direkt, sondern nur im Zusammenhang mit bestimmten Abfragen zugegriffen werden.

Diese Begründung ist für mich allerdings unbefriedigend, sie lässt nicht zu, dass nachgeprüft werden kann, ob der Zugriff, die Anfrage nach einem DNA-Muster erforderlich war. Darüber hinaus werden die vorstehend genannten engen Zweckbestimmungsregelungen in kleinen Schritten aufgeweicht. Auch hier zeichnet sich kein für mich gangbarer Kompromiss ab.

11.3 Ohne polizeiliche Erkenntnisse Daten im KAN gespeichert!

Die herausragende Bedeutung des § 2 Abs. 1 BKAG habe ich bereits oben (Nrn. 11.1, 11.2) ausführlich dargestellt. Welche Auswirkungen sich jedoch für Betroffene aus einer unzutreffenden Anwendung dieser Norm ergeben, zeigt der Fall eines in Burma geborenen Petenten, der mittlerweile die deutsche Staatsangehörigkeit angenommen hat und seit vielen Jahren in Deutschland wohnt. Er war bei der Einreise in die Vereinigten Staaten von der dortigen Einwanderungsbehörde verhört worden, was möglicherweise mit einem Eintrag in der „Black-List“ des US-Immigration-Office zusammenhing. Meine Kontrolle beim BKA ergab, dass Daten des Petenten im KAN für die Dauer von 10 Jahren gespeichert waren, was auf einer Anfrage der amerikanischen Drogenbekämpfungsbehörde (DEA) beruhte, die den Petenten im Verdacht hatte, mit der „Mong Tay Army“ und deren Vorgängerorganisation – einer kriminellen Organisation, die sich nahezu ausschließlich aus dem illegalen Handel mit Rauschgift finanzieren soll – in Verbindung gestanden zu haben. Ob der Petent in den organisierten Drogenhandel involviert war bzw. ist, konnte bisher nicht geklärt werden. Aus einem Vermerk eines Verbindungsbeamten des BKA in Bangkok war zu entnehmen, dass sich die amerikanische Drogenbekämpfungsbehörde seinerzeit bemüht hatte, die Einreise des Petenten in die Vereinigten Staaten zu verhindern. Es war wohl geplant, den Petenten in die „Black-List“ aufnehmen zu lassen. Dies ist offenbar geschehen, da der Petent nach nunmehr fünf Jahren Schwierigkeiten bei der Einreise in die Vereinigten Staaten bekommen hat. Das BKA hatte 1994 über das Landeskriminalamt Schleswig-Holstein eine Abklärung zur Person des Petenten vornehmen lassen. Die Antwort des Landeskriminalamtes Schleswig-Holstein, die die vollständigen Personalien und den Hinweis enthielt, dass der Betroffene polizeilich nicht bekannt sei, wurde dem Verbindungsbeamten des BKA nach Bangkok übermittelt. Dieser Vorgang, der keine polizeilich relevanten Erkenntnisse enthielt, ist vom BKA im KAN für die Dauer von 10 Jahren gespeichert worden.

Nachdem der Sachverhalt aufgeklärt war, habe ich das BKA gebeten, die Zulässigkeit dieser Speicherung zu überprüfen, da ich die Speicherkriterien des § 8 BKAG mangels kriminalistischem Hintergrund für nicht erfüllt ansehe. Nachdem das BKA zu der Auffassung gelangt war, dass sich seit Eingang der Informationen aus dem Jahre 1994 keine Anhaltspunkte ergeben hätten, die den damaligen Verdacht erhärteten, und nachdem es auch keine neuen Erkenntnisse über den Petenten gab, wurden dessen Daten im KAN gelöscht und die zugrundeliegenden Unterlagen vernichtet.

Ich werde diesen Fall bei der Diskussion über die neugefasste Errichtungsanordnung für den KAN zum Anlass nehmen, eingehend mit dem BMI und dem BKA die Frage zu erörtern, inwieweit solche Sachverhalte die Zugangsvoraussetzungen für eine KAN-Speicherung überhaupt erfüllen können. Nach formaler Betrachtungsweise ließe sich möglicherweise das Merkmal „internationale Bedeutung“ im Sinne von § 2 Abs. 1 BKAG bejahen, jedoch lässt diese Betrachtungsweise außer acht, dass es sich in derartigen Fällen ausschließlich um eine Erkenntnisanfrage einer ausländischen Stelle handelte, der offenbar weder ein konkreter Verdacht noch ein Ermittlungsverfahren zugrunde lagen. In derartigen Fällen darf eine Speicherung im KAN auf Grund bloßer Erkenntnisanfragen ausländischer Polizeibehörden generell nicht erfolgen. Die KAN-Kriterien sind in der Errichtungsanordnung bzw. in einem Anhang zur Errichtungsanordnung präzise zu umschreiben. Ich werde hierauf mein besonderes Augenmerk richten.

11.4 VICLAS-Datei

Das Kürzel „VICLAS“ steht für „Violent Crime Linkage Analysis System“ und bedeutet „Analyse-System zur Serienzusammenführung von Gewaltverbrechen“. Das ursprünglich von der kanadischen Polizei entwickelte Datenbanksystem dient dazu, Angaben zu bestimmten Serienstraftaten im Bereich der schweren Gewaltkriminalität zusammenzuführen, um sie effektiv analysieren zu können. Das tatrelevante Verhalten des Straftäters wird anhand des Einzelfalls analysiert, strukturiert abgebildet

und mit anderen in VICLAS gespeicherten Fällen verglichen. VICLAS verfolgt das Ziel, Serienzusammenhänge zwischen besonders schweren Straftaten besser als bisher und selbst bei divergierender Begehungsweise erkennen zu können und ungeklärte Straftaten aufzuklären, falls der Täter bei mindestens einer Tat der erkannten Serie bekannt ist. Die Philosophie von VICLAS ist aus der Erkenntnis geboren, dass jeder Gewalttäter eine „Handschrift“ hat und sie am Tatort oder am Opfer hinterlässt. Wenn Verhaltens- und Vorgehensmuster des be- oder unbekannten Täters erfasst werden, wird es möglich, diese „Handschrift“ zu identifizieren, und man erkennt weitere tat- oder täterbezogene Zusammenhänge. Die Daten für VICLAS werden mit einem teilstandardisierten Fragebogen von speziell ausgebildeten Polizeibeamten erhoben.

Seit dem 1. Juni 2000 wird eine VICLAS-Datei als Verbunddatei des polizeilichen Informationssystems des Bundes und der Länder beim BKA geführt. In ihr werden Vermisstenfälle, bei denen die Gesamtumstände auf ein Verbrechen hindeuten, Tötungsdelikte sowie Straftaten gegen die sexuelle Selbstbestimmung erfasst und analysiert. Das BKA geht jährlich von 10 000 bis 14 000 relevanten Straftaten aus, was ca. 0,1 % bis 0,2 % der gesamten in der polizeilichen Kriminalstatistik aufgezählten Straftaten ausmacht .

Der Einführung neuer Ermittlungsansätze und -methoden, wie der VICLAS-Datenbank, stehe ich stets aufgeschlossen gegenüber, wenn sie der Verhinderung und Aufklärung schwerer Gewaltdelikte dienen. Bei VICLAS kommt hinzu, dass im Ausland damit bereits positive Erfahrungen gesammelt werden konnten. Im Rahmen des Anhörungsverfahrens vor Erlass der Errichtungsanordnung für die Datei habe ich aber im Interesse der Opfer eine Änderung gefordert.

Nach der Konzeption von VICLAS wird neben den am Tatort festgestellten Sachbeweisen das Opfer als „Spiegel des Täterverhaltens“ stärker in das Blickfeld genommen, indem Einzelheiten des Verhaltens des Täters gegenüber dem Opfer in die Datenbankauswertung mit einfließen. Dies hat zur Folge, dass u. a. eine Fülle von Daten aus den intimsten Bereichen von Opfern VICLAS-relevanter Straftaten, z. B. Angaben zum Lebensunterhalt und -stil, sowie zum tatbezogenen Täter-Opfer-Verhalten Eingang in die Datei finden. Das Erfordernis der Speicherung derartig detaillierter und sensibler Datenfelder ist im Hinblick auf die genannte Zielrichtung von VICLAS nachvollziehbar. Für problematisch halte ich hingegen die Aufnahme der Personalien dieser Opfer in die Datei.

Um meinen Bedenken Rechnung zu tragen, sieht das Dateistatut nunmehr die Aufnahme von Personalien der Opfer nur vor, sofern diese hierin ausdrücklich und schriftlich eingewilligt haben. Der Text der von den Opfern bzw. ihren gesetzlichen Vertretern abzugebenen Einwilligungsklärung ist mit mir abgestimmt worden. Er enthält neben Informationen zum Zweck der Datenbank VICLAS sowie zum Erfordernis der Einwilligung als Voraussetzung für eine Speicherung vor allem auch den Hinweis auf die Möglichkeit des Widerrufs dieser Einwilligung, welcher die Löschung der Personalien in der Datei zur Folge hätte. Erteilt ein Opfer seine Einwilligung nicht, wird auf die Speicherung aller Daten verzichtet, die zur Identifikation des Opfers führen könnten.

Mit diesen Regelungen in der Errichtungsanordnung trage ich den Betrieb der VICLAS-Datei beim BKA vorbehaltlich einer späteren datenschutzrechtlichen Kontrolle mit.

11.5 Geldwäsche-Datei

In meinem 17. TB (Nr. 11.7) hatte ich über die Bestrebungen der Polizeien von Bund und Ländern berichtet, den gesetzlichen Regelungen zur Geldwäschebekämpfung dadurch mehr Wirksamkeit zu verschaffen, dass beim BKA eine zentrale Datei zur bundesweiten Zusammenführung von Geldwäscheverdachtsanzeigen eingerichtet werden sollte. Mit dieser Maßnahme sollten die Erfolgsquoten von Verdachtsanzeigen wesentlich gesteigert und die Auskunftsfähigkeit gegenüber dem Ausland erheblich verbessert werden.

Seit dem 29. Juni 2000 wird die Geldwäsche-Datei als sog. Verbunddatei, die sowohl vom BKA als auch von den Landespolizeibehörden genutzt werden kann, beim BKA betrieben.

Anlässlich der Beratungen der Errichtungsanordnung zu dieser Datei war es vor allem mein Anliegen, die „Treffsicherheit“ der Verdachtsanzeigen bei gleichzeitiger deutlicher Reduzierung ihrer Zahl zu erhöhen, um eine bundesweite Speicherung von „Verdachtsdaten“ Unschuldiger in der Geldwäsche-Datei möglichst zu vermeiden. Problematisch war deshalb vor allem, ob in der Datei auch Angaben zu Personen gespeichert werden sollten, gegen die wegen Verdachtsanzeigen zunächst keine konkreten strafrechtlichen Ermittlungen eingeleitet werden.

Die Ermittlungstätigkeit bei Geldwäschedelikten wird im Wege der Verdachtsanzeige zumeist seitens privatwirtschaftlicher Unternehmen initiiert. Dies macht es aus Sicht der Strafverfolgungsbehörden erforderlich, neben den aufgrund eines Anfangsverdachtes formal den Beschuldigtenstatus erhaltenden Personen auch jene zu erfassen, bei denen zwar im konkreten Einzelfall die Beweislage nicht ausreicht, bei denen aber immer noch genügend Anhaltspunkte vorliegen, um den Verdacht einer Straftat zu bejahen. Zudem kann nach Auffassung der Strafverfolgungsbehörden die Datei ihre Funktion als Verdachtsgewinnungs- und -erhärtungsinstrument nur erfüllen, wenn auch die Daten der Personengruppe der insoweit „Verdächtigen“ darin aufgenommen werden.

§ 8 Abs. 2 BKAG erlaubt zwar neben der Speicherung personenbezogener Daten Beschuldigter auch solche von Verdächtigen in Dateien des BKA. Letztere setzt jedoch voraus, dass aufgrund von Erkenntnissen über die Tat, die Persönlichkeit des Betroffenen oder andere Umstände Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen den Verdächtigen zu führen sein werden.

Geldwäscheverdachtsanzeigen, die durch gesetzliche Mitteilungspflichten eines nach den Vorschriften des

Geldwäschegesetzes anzeigepflichtigen Institutes ausgelöst werden und denen häufig nur die bloße Annahme eines geldwäscherelevanten Vorgangs zugrunde liegt, sind mit Strafanzeigen aufgrund der Beobachtung einer Straftat oder aus eigener Rechtsbetroffenheit meiner Ansicht nach aber nicht vergleichbar. Ihr fehlt regelmäßig die Qualität, um die nach § 8 Abs. 2 BKAG geforderte Negativprognose begründen zu können. Damit besteht aus meiner Sicht die Gefahr, dass die Daten vieler unbescholtener Personen in der Datei gespeichert werden.

Eine Verbesserung konnte im Laufe der Beratungen der Errichtungsanordnung insofern erreicht werden, als eine „Indikatorenliste“, die abstrakt Anhaltspunkte für eine Geldwäschehandlung aufführt, erarbeitet und in die Dateianordnung mit einbezogen wurde. Sie enthält aus meiner Sicht akzeptable Kriterien, um beurteilen zu können, wann aufgrund einer Verdachtsanzeige die Verdachtsschwelle i. S. des § 8 Abs. 2 BKAG erreicht ist. Unter der Voraussetzung, dass diese Indikatorenliste vor Einspeicherung personenbezogener Daten durch die Polizeibehörden konkret geprüft wird und nur bei Vorliegen entsprechender Indikatoren auch eine Speicherung erfolgt, habe ich der Aufnahme „Verdächtiger“ in die Geldwäsche-Datei zugestimmt.

Als weiteres datenschutzrechtliches Korrektiv hatte ich für diese Personengruppe kurze Aussonderungsprüffristen gefordert. Zwar ist diese Frist, die nach dem BKAG bis zu zehn Jahre betragen kann, auf vier Jahre festgelegt worden. Gleichwohl hatte ich für eine kürzere Prüffrist votiert, zumal es sich hierbei nicht um eine Höchstspeicherfrist, sondern um einen Termin handelt, zu dem lediglich die weitere Erforderlichkeit der Speicherung geprüft werden muss. Die regelmäßige Datenpflege in kürzeren Abständen hätte aus meiner Sicht dazu geführt, dass der Datenbestand in der Geldwäsche-Datei auf einem noch aktuelleren Stand gehalten werden kann, in dem unbegründete Verdachtsanzeigen und damit die Speicherung strafrechtlich Unbescholtener frühzeitiger hätten ausgesondert werden können.

Ein sorgfältiger Umgang mit den in der Geldwäsche-Datei gespeicherten personenbezogenen Daten ist auch insofern geboten, als der Ministerrat am 17. November 2000 einen Beschluss über die Vereinbarungen für eine Zusammenarbeit zwischen den zentralen Meldestellen der EU-Mitgliedstaaten im Bereich der Geldwäschebekämpfung gefasst hat. Dieser sieht einen Austausch aller verfügbaren Informationen zwischen den zentralen Meldestellen – in Deutschland ist dies das BKA – vor, die für die Analyse von Informationen oder für Ermittlungen im Zusammenhang mit Geldwäsche und den dabei beteiligten Personen von Belang sein können. Einbezogen sind dabei grundsätzlich auch die in der Geldwäsche-Datei gespeicherten personenbezogenen Daten zu Verdächtigen.

In den kommenden Jahren muss daher bewertet werden, inwieweit die Erwartungen der Strafverfolgungsbehörden mit der Einrichtung der Geldwäsche-Datei erfüllt werden. Insbesondere die Verwendung von Daten derjenigen Personen, gegen den sich ein strafrechtlicher Anfangsverdacht aufgrund einer Verdachtsanzeige nicht begründen lässt, bedarf der datenschutzrechtlichen Beobachtung.

11.6 DNA-Analyse-Datei

Bereits in meinem 17. TB (Nr. 6.3) habe ich über die Einrichtung einer DNA-Analyse-Datei als Verbundanwendung beim BKA berichtet, die dort im April 1998 in Betrieb gegangen war. Die nach § 34 BKAG hierzu erforderliche Errichtungsanordnung wurde allerdings erst am 27. Oktober1999 endgültig in Kraft gesetzt, weil insbesondere die Frage der Zulässigkeit molekular-genetischer Untersuchungen – ausschließlich aufgrund richterlicher Anordnung oder auch mit Einwilligung eines Betroffenen – entschieden werden musste (s. auch o. Nr. 6.3). Das BMI hat sich – entgegen der Entschließung der 58. Datenschutzkonferenz vom 13. Oktober 1999 zum Einsatz der DNA-Analyse zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen (s. **Anlage 25**) – dafür entschieden, die Entnahme von genetischem Material auch aufgrund der Einwilligung des Betroffenen zuzulassen und hat dies in der Errichtungsanordnung zur DNA-Datei ausdrücklich als „Kann-Bestimmung“ festgelegt. Das BMI folgte damit einer Entschließung des AK II der IMK, der die Einwilligung eines Betroffenen als Zulässigkeitsvoraussetzung für ausreichend angesehen hatte. Damit bleibt diese juristische Streitfrage einer obergerichtlichen Entscheidung vorbehalten, nachdem die bisher ergangene Rechtsprechung der Instanzgerichte nicht einheitlich entschieden hat.

Im übrigen hat die Verbunddatei bereits einen respektablen Umfang erreicht. Ende 2000 waren dort nach Angaben des BKA rd. 72 300 Personendatensätze und rd. 8 800 Spurendatensätze registriert. Die Anzahl der verifizierten Trefferfälle betraf weit überwiegend Eigentumsdelikte.

11.7 Automatisiertes Fingerabdruck-Identifizierungssystem – AFIS –

Fast acht Jahre nach der Aufnahme des Probebetriebs wurden im Jahre 2000 für das automatisierte Fingerabdruck-Identifizierungssystem **AFIS** die nach § 34 BKA-Gesetz erforderlichen Errichtungsanordnungen vom BMI erlassen. Vorausgegangen waren jahrelange Auseinandersetzungen mit den Ländern und mit mir über den Inhalt dieser Anordnungen (vgl. unter anderem 17. TB Nr. 11.8). Bereits 1997 hatte sich das BMI bereit erklärt, gesonderte Errichtungsanordnungen für die Anwendungen AFIS-P (Polizei, Ausländer) und AFIS-A (Asyl) zu erlassen. In AFIS-P werden die Daten insbesondere von Beschuldigten und Verdächtigen gespeichert, die erkennungsdienstlich behandelt wurden, sowie von Personen gemäß § 41 AuslG, das sind Ausländer, deren Identität nicht zweifelsfrei feststeht. In der Datei AFIS-A werden die Daten von Personen erfasst, die gemäß § 16 AsylVfG erkennungsdienstlich behandelt wurden, das sind alle Asylbewerber, es sei denn sie besitzen eine unbefristete Aufenthaltsgenehmigung oder haben das 14. Lebensjahr noch nicht vollendet. Die beiden Datenbestände sind logisch vonei-

nander getrennt, außerdem werden die Fingerabdruckblätter von Ausländern und Asylbewerbern gemäß § 78 Abs. 2 AuslG bzw. § 16 AsylVfG gesondert von anderen Unterlagen aufbewahrt. Zudem werden die Daten von nach § 41 AuslG behandelten Personen in der Datei AFIS-P mit einem Merker versehen, um auch so den Anforderungen des § 78 AuslG zu genügen. Dort ist zwar nur von der getrennten Aufbewahrung der nach § 41 AuslG gewonnenen Unterlagen die Rede. Daraus resultiert jedoch auch eine zumindest logische Trennung dieser Daten in der Datei AFIS-P von denjenigen der erkennungsdienstlichbehandelten Beschuldigten und Verdächtigen. Diese zweigleisige Verfahrensweise entspricht einer alten Forderung von mir.

11.8 BKA recherchiert im Internet

Auf Beschluss der Ständigen Konferenz der Innenminister und -senatoren des Bundes und der Länder vom 20. November 1998 ist das BKA als zentrale Stelle für das gesamte Bundesgebiet mit der Durchführung anlassunabhängiger Recherchen im Internet sowie den Online-Diensten und der Weiterleitung der daraus gewonnenen Erkenntnisse an die zuständigen Strafverfolgungsbehörden beauftragt worden. Gegen die praktische Durchführung anlassunabhängiger Recherchen im Internet durch das BKA habe ich keine grundlegenden datenschutzrechtlichen Bedenken.

§ 2 Abs. 1 i. V. m. § 7 Abs. 2 BKAG, die die Befugnisse des BKA als Zentralstelle für die Polizei des Bundes und der Länder bei der Datenerhebung festlegen und insofern als Grundlage für die anlassunabhängige Internet-Recherche heranzuziehen sind, erlauben eine offene Datenerhebung u. a. auch bei nicht-öffentlichen Stellen. Für eine verdeckte, die polizeiliche Identität bewusst verheimlichende oder verschleiernde Recherche im Internet im Rahmen der Zentralstellenaufgabe des BKA fehlt es jedoch an einer entsprechenden gesetzlichen Ermächtigung im BKAG. Zudem kann sich das BKA in diesem Stadium der Beobachtung noch nicht auf die Regelungen der StPO stützen.

Nach meinen Feststellungen bewegt sich das BKA bei Internet-Recherchen innerhalb dieses Rechtsrahmens.

Es „surft“ nur in frei zugänglichen, gleichwohl einschlägigen Bereichen und folgt dort Anpreisungen und Einladungen. Die Recherche-Ergebnisse werden an die zuständigen Strafverfolgungsbehörden weitergeleitet. Auf diese Weise wurden, wie mir das BKA mitteilte, im Zeitraum vom 1. Januar bis 10. Oktober 2000 von der „Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD)“ des BKA insgesamt 1115 Verdachtsmeldungen bearbeitet. In 1 015 Fällen wurden aufgrund eines Anfangsverdachts Anzeigen erstellt und an die zuständigen Dienststellen im In- und Ausland weitergeleitet. Diese gliedern sich im Einzelnen wie folgt auf:

- 881 Fälle von Kinderpornographie
- 6 Staatsschutzdelikte
- 14 Delikte nach dem Betäubungsmittelgesetz
- 31 Delikte nach dem Arzneimittelgesetz
- 10 Delikte nach dem Urheberschutzrecht
- 43 Fälle von Tierpornographie
- 12 Fälle sexuellen Missbrauchs von Kindern
- 18 sonstige Delikte

Rund 83 % aller Verdachtsanzeigen waren Auslandsfälle, rund 17 % Inlandsfälle.

Neben der Kinderpornographie bildet in der letzten Zeit auch die Bekämpfung von strafbaren rechtsextremistischen und fremdenfeindlichen Inhalten im Internet einen Schwerpunkt der Internetrecherche des BKA.

Auch wenn die in der Praxis durchgeführte anlassunabhängige Internet-Recherche keinen grundlegenden datenschutzrechtlichen Bedenken begegnet, ist es rechtlich nicht zulässig, wenn sich das BKA im Zusammenhang mit solchen Recherchen auf § 89 Abs. 6 TKG beruft, um bei einem Zugangsprovider die Identität eines Nutzers zu ermitteln, dem zu einem bestimmten Zeitpunkt eine bestimmte IP-Adresse zugeteilt wurde. Der Bezugnahme auf das TKG liegt die irrige Auffassung zugrunde, dass der Zugangsprovider hier einen Telekommunikationsdienst anbietet. Die Notwendigkeit des Einschaltens des Providers wird vom BKA mit dem Erfordernis begründet, einen raschen Zugriff der Strafverfolgungsbehörden und damit die Beweissicherung zu gewährleisten. Dies könne nur dadurch sichergestellt werden, dass die Verdachtsmeldung des BKA an die örtlich zuständige Staatsanwaltschaft am Wohn- bzw. Geschäftssitz des Nutzers, auf dessen PC sich das vermutlich strafrechtlich-relevante Material befindet, weitergeleitet wird. Der Nutzer lasse sich dabei nur mit Hilfe der beim Provider vorhandenen Daten ermitteln.

Ein Zugangsprovider ist Teledienstеanbieter i. S. von § 2 Abs. 2 Nr. 3 TDG. Somit ist das Teledienstedatenschutzgesetz (TDDSG) einschlägig, das in § 2 Nr. 1 auch den Zugangsprovider als *„Diensteanbieter im Sinne dieses Gesetzes“* einschließt. Es sieht eine Auskunftsverpflichtung des Providers gegenüber Dritten nicht vor und begründet daher auch kein entsprechendes Ersuchen des BKA. Die Befugnisse der Strafverfolgungsbehörden hingegen bleiben gem. § 6 Abs. 3 Satz 2 TDDSG unberührt. In den Fällen, in denen mit den Rechercheergebnissen ein strafprozessualer Anfangsverdacht noch nicht begründet werden kann, ist es aus meiner Sicht aber akzeptabel, den Provider mit dem Hinweis auf ein bevorstehendes, durch eine zuständige Strafverfolgungsbehörde zu führendes Ermittlungsverfahren im Einzelfall um die Speicherung der entsprechenden Daten zu bitten.

Bei der Bekämpfung der Internetkriminalität bemüht sich das BKA um eine dauerhafte Zusammenarbeit mit den Providern. Ich unterstütze dies, zumal es im

beiderseitigen Interesse von Internet-Nutzern und Internet-Betreibern liegt, das Vertrauen in dieses Medium zu erhalten und keinen rechtsfreien Raum entstehen zu lassen. Zugleich begrüße ich, dass meine Dienststelle an den bisherigen Beratungen mit den Providern beteiligt wurde. Die Bemühungen führen aber nur dann zum Erfolg, wenn sich die Polizei auch der datenschutzrechtlichen Vorgaben, die von den Internetbetreibern zu beachten sind, bewusst ist. Herausgabeverlangen, gestützt auf nicht einschlägige Rechtsvorschriften, führen zur Verunsicherung der Provider über den Umfang ihrer Auskunftsverpflichtungen gegenüber den Polizei- und Sicherheitsbehörden einerseits und der von ihnen zu beachtenden Löschungsverpflichtungen bezogen auf Nutzerdaten andererseits.

Ich werde die Aktivitäten der Sicherheitsbehörden im Internet auch weiterhin aufmerksam beobachten, damit die Datenschutzrechte der Internet-Nutzer gewahrt bleiben.

11.9 Rechtstatsachen – leider wenig Neues

Bereits mehrfach (zuletzt 17. TB Nr. 11.2) habe ich die Notwendigkeit einer wirksamen Erfolgskontrolle bei strafprozessualen wie auch bei präventiv-polizeilichen Eingriffsbefugnissen betont, wie z. B. bei der Telefonüberwachung (s. o. Nr. 6.4.2). Die Bundesregierung hat in ihrer schriftlichen Stellungnahme zu meinem 17. TB ebenfalls erklärt, dass die systematische Evaluation gesetzlicher Eingriffsinstrumente unter Einbeziehung der Wissenschaft und des BfD einen Schwerpunkt der Arbeiten im Bereich der Inneren Sicherheit in dieser Legislaturperiode bilde.

Leider sieht die Realität anders aus. Der Gesprächskreis „Rechtstatsachen“ beim BKA, in dem ich vertreten bin, trat letztmals im März 1999 auf Einladung des BKA zu einem Meinungsaustausch über den Fortgang der verschiedenen Initiativen auf dem Gebiet der Rechtstatsachenforschung zusammen. Bis Redaktionsschluss hat keine weitere Sitzung des Arbeitskreises stattgefunden. Das BMI hat mir lediglich ergänzend über einige von ihm initiierte kleinere Auswertungsprojekte berichtet, die teils abgeschlossen, teilweise aber auch nicht in Angriff genommen wurden.

Auch die Hoffnungen, die ich in die Tätigkeit der beim BKA geführten Rechtstatsachensammelstelle gesetzt hatte, haben sich nicht alle erfüllt. Das Themenraster, aufgrund dessen das BKA, das ZKA, der BGS und die Landeskriminalämter Fallbeispiele aus der polizeilichen Praxis in die von der Rechtstatsachensammelstelle betriebene Bund-/Länder-Fallsammlung anliefern, stammt aus dem Jahr 1995. Ich habe Zweifel, dass die Rechtstatsachensammelstelle ohne Anpassung des Themenrasters an die neuen Entwicklungen auch im präventiv-polizeilichen Bereich ihre Aufgabe, dem Gesetzgeber durch das Sammeln empirischer Daten eine Basis zur Evaluierung der vorhandenen rechtlichen Instrumentarien zu verschaffen, sachgerecht erfüllen kann. Zudem verläuft die Datenanlieferung durch die Länder weiterhin nicht optimal, ohne dass bisher Bestrebungen erkennbar sind, die zugrundeliegenden Meldeverfahren zu verbessern. Insbesondere wird die Aufgabe der Rechtstatsachenstelle dadurch eingeschränkt, dass sich ihr Auftrag auf das Sammeln von Rechtstatsachen beschränkt, also keinerlei Auswertungen zulässt.

Große Erwartungen setze ich auf das vom BMJ gestartete Forschungsvorhaben „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO“. Dem Projekt kommt deshalb große Bedeutung zu, weil die Anzahl der Maßnahmen zur Telefonüberwachung seit Jahren steil ansteigt (s. o. Nr. 6.4.2), was der Forschung angesichts der großen Zahl von Fällen eine repräsentative Auswertung ermöglicht und Zufallsergebnisse ausschließt. Da eine Telefonüberwachung einen besonders tiefen Eingriff in das Fernmeldegeheimnis bedeutet, der an sich nur als „ultima ratio“ gedacht war, wird eine Ursache-Wirkung-Analyse auch zu Erkenntnissen für die politischen Entscheidungsträger beitragen. Die Durchführung des Vorhabens hat sich infolge datenschutzrechtlicher Probleme bei der Datenanlieferung durch die Länder etwas verzögert, doch hoffe ich, dass diese Schwierigkeiten mit der im StVÄG 1999 (s. o. Nr. 6.2) enthaltenen Forschungsklausel nunmehr behoben sind. Mit Ergebnissen ist im Herbst 2001 zu rechnen.

Wegen der Bedeutung, die ich einer effizienten Gesetzesevaluation bei Eingriffsmaßnahmen im Hinblick auf den Persönlichkeitsschutz beimesse, habe ich im Januar 2001 die hauptsächlich beteiligten Ressorts BMI und BMJ sowie das BKA zu einer Besprechung geladen, um eine Bestandsaufnahme der Bemühungen auf Seiten des Bundes vorzunehmen. Bei der Gelegenheit habe ich nochmals an die Teilnehmer appelliert, in ihren Anstrengungen für mehr Evaluation von Rechtstatsachen nicht nachzulassen und insbesondere die angefangenen Projekte zügig zum Abschluss zu bringen, damit eine ausreichende Datenbasis für Maßnahmen des Gesetzgebers vorhanden ist.

11.10 Schengener Durchführungsübereinkommen

11.10.1 Gemeinsame Kontrollinstanz

Die Zusammenarbeit der Vertragsparteien von Schengen verlief bis zum Inkrafttreten des Amsterdamer Vertrages Mitte 1999 außerhalb des Rahmens der Europäischen Union. Aufgrund des Protokolls zur Einbeziehung des Schengen-Besitzstands in den Rahmen der EU, das dem Vertrag von Amsterdam beigefügt ist, gehören wichtige Beschlüsse und Erklärungen des früheren Exekutivausschusses von Schengen zum gemeinschaftlichen Besitzstand, auch solche mit Bezug zur Gemeinsamen Kontrollinstanz (GKI). Die GKI ihrerseits hatte darauf gedrängt, dass auch ihre eigenen Beschlüsse in den Schengen-Besitzstand aufgenommen werden. Dem ist der Rat leider nicht gefolgt und hat am 20. Mai 1999 einen „Beschluss über eine Gemeinsame Kontrollinstanz auf der Grundlage von Art. 115 des Schengener Übereinkommens vom 14. Juni 1985, betreffend den schrittweisen Abbau der Kontrollen an gemeinsamen Grenzen, unterzeichnet am 19. Juni 1990“, gefasst.

Damit ist zwar der unabhängige Status der GKI im Rahmen der dritten Säule der Union gesichert, gleichwohl betont die Kontrollinstanz, dass auch ihre Stellungnahmen und Empfehlungen von jedem Schengen-Staat, auch den neu hinzutretenden, zu berücksichtigen sind. Die logistische Unterstützung der GKI durch das Generalsekretariat des EU-Rates verläuft bisher zufriedenstellend; ihre eigenständige Funktion erscheint gesichert.

Des weiteren hat die GKI im Jahre 1999 ihren dritten und im Herbst 2000 ihren vierten Tätigkeitsbericht vorgestellt, in denen über die Aktivitäten des Kontrollorgans bis einschließlich Februar 2000 berichtet wird. Unter anderem hat eine Arbeitsgruppe der GKI im Frühjahr 1999 unter Beteiligung meiner Dienststelle einen weiteren Kontrollbesuch beim C.SIS in Straßburg durchgeführt. Dabei wurde festgestellt, dass die Empfehlungen der GKI aufgrund ihres Kontrollbesuchs vom Herbst 1996 (vgl. 16. TB Nr. 11.6.2) nur teilweise umgesetzt waren. Die zuständigen Schengen-Gremien sind der Auffassung, dass sich einige Vorschläge der GKI mit der aktuellen Schengen-Konfiguration des SIS nicht verwirklichen lassen und verweisen auf eine neue Generation des SIS, die in einigen Jahren das geltende System, das bereits mehrfach modifiziert wurde, als SIS II ablösen soll. Die datenschutzrechtliche Begleitung dieses Projekts wird voraussichtlich eines der Schwerpunktthemen der GKI in den kommenden Jahren sein.

Das SIS, an das derzeit zehn Mitgliedstaaten angeschlossen sind, soll im Jahr 2001 aufgrund von Ratsbeschlüssen erneut erweitert werden. Die technischen Voraussetzungen wurden mit der Inbetriebnahme des SIS I+ geschaffen. Diesmal geht es um die nordischen Länder Dänemark, Finnland, Schweden, Norwegen und Island. Dabei werden die beiden letzteren Staaten, da sie nicht der EU angehören, lediglich als assoziierte Mitglieder am System teilnehmen. Neben den technischen und organisatorischen Voraussetzungen setzt ein Anschluss an das SIS voraus, dass in den Beitrittsstaaten ein angemessener Datenschutzstandard gemäß Art. 117 SDÜ gewährleistet ist. Zu diesem Zweck ist die GKI von der Art. 36-Gruppe beteiligt worden. Das Kontrollgremium hat nach Anhörung von Datenschutzexperten der Beitrittsstaaten keine grundlegenden datenschutzrechtlichen Bedenken mehr gegen den Beitritt der nordischen Länder, nachdem festgestellt werden konnte, dass alle Beitrittskandidaten über eine unabhängige Datenschutzkontrolle verfügen und über den Schengen-Besitzstand (s. o.) auch den der GKI anerkennen.

Gegen Ende des Berichtszeitraums sind in den Ratsgremien Initiativen gestartet worden, um das SIS gemäß den Anforderungen der Benutzer fortzuentwickeln. Ich habe mich von Anfang an gegen überzogene Lösungsvorschläge ausgesprochen, die den Persönlichkeitsschutz von Betroffenen übermäßig einschränken. Ich werde auch in der GKI darauf drängen, dass solchen Vorschlägen energisch entgegengetreten wird. Dies bedeutet nicht, dass sich der Datenschutz gegen jegliche Verbesserungsvorschläge zum SIS wendet. Aber auch hier muss ein ausgewogenes Verhältnis zwischen den Forderungen der Sicherheitsbehörden und den schutzwürdigen Interessen der betroffenen Bürger gefunden werden.

11.10.2 Bilaterale Zusammenarbeit mit anderen nationalen Kontrollinstanzen außerhalb des Rahmens der GKI

Im Berichtszeitraum hat sich eine intensive bilaterale Zusammenarbeit mit den Datenschutzkontrollinstanzen einiger anderer Schengen-Staaten gemäß Art. 114 Abs. 2 SDÜ entwickelt. Dies beruht darauf, dass ein Betroffener seine Rechte, insbesondere das Recht auf Auskunft, nach seiner Wahl in jedem Vertragsstaat ausüben kann. Wenn deutsche Stellen Ausschreibungen im SIS veranlasst haben, werde ich von ausländischen Partnerbehörden um Klärung möglicher Speicherungen beim deutschen SIRENE-Büro (BKA) ersucht. Nach einer vorläufigen Antwort des BKA, die Aufschluss über eine Ausschreibung im SIS gibt, beteilige ich den jeweils zuständigen Landesbeauftragten für den Datenschutz zwecks datenschutzrechtlicher Kontrolle derjenigen Stelle (Ausländerbehörde), die für die Ausschreibung verantwortlich ist. Nach Eingang des Ergebnisses der Kontrolle informiere ich die ersuchende ausländische Datenschutzkontrollinstanz über das Ergebnis der Kontrolle, damit sie den Betroffenen unterrichten kann.

11.10.3 Probleme bei der Anwendung des Schengener Durchführungsübereinkommens

Bei den vorgenannten Kontrollen haben sich für mich interessante Erkenntnisse ergeben:

- Deutsche Stellen, zumeist Ausländerbehörden, haben Ende 2000 mehr als 300 000 Ausschreibungen zur Einreiseverweigerung für Drittausländer nach Art. 96 SDÜ vorgehalten. Ein nicht unerheblicher Anteil dieser Ausschreibungen erfolgte zu Unrecht, weil er nicht den Kriterien des Art. 96 Abs. 3 SDÜ entsprach. Die Ausschreibungen wären daher zu löschen. Dies gilt für diejenigen Fälle, in denen ein Asylbewerber nach rechtskräftiger Ablehnung seines Asylbegehrens untergetaucht ist, denn es handelt sich dann um Ausschreibungen, die lediglich der Aufenthaltsermittlung dienen. Die Erfassung in nationalen Verfahren, z. B. INPOL oder AZR, bleibt jedoch hiervon unberührt. Eine Erfassung nach Art. 96 Abs. 3 SDÜ ist dann nur zulässig, wenn ein Drittausländer im Sinne von § 8 Abs. 2 Satz 1 AuslG ausgewiesen, zurückgewiesen oder abgeschoben wurde. Das BMI teilt diese Auffassung. Das Bundesverwaltungsamt hat Anfang des Jahres 2000 den Ausschreibungsbestand nach Art. 96 SDÜ ausgewertet und zahlreiche unzulässige Ausschreibungen festgestellt. Das BMI hat daraufhin die Länder aufgefordert, die festgestellte Praxis abzustellen.
- Die grundsätzlich drei Jahre betragende Ausschreibungsfrist nach Art. 112 SDÜ wird vielfach überschritten. Ich habe zwar in Anbetracht des Massenverfahrens vor Jahren gegen eine pauschale Verlängerung der

Speicherfrist um weitere drei Jahre keine grundlegenden Einwendungen erhoben. Eine darüber hinaus gehende weitere Verlängerung erscheint mir jedoch nur hinnehmbar, wenn sie im Einzelfall von der ausschreibenden Stelle aus Gründen der öffentlichen Sicherheit und Ordnung oder der nationalen Sicherheit als unbedingt erforderlich angesehen wird. Keinesfalls genügt die bloße Bezugnahme auf die längeren Speicherungsfristen für inländische Fahndungen. Ich habe dies auch gegenüber dem BMI klargestellt. Die Gespräche hierüber mit dem BMI waren bei Redaktionsschluss noch nicht abgeschlossen.

- Bei Ausschreibungen nach Art. 96 SDÜ tritt das Problem der missbräuchlichen Verwendung der Identität auf, wobei sich nicht sofort feststellen lässt, ob die Polizei bei einer Personenkontrolle an der Grenze den gesuchten Straftäter, der die Personalien einer unbescholtenen Person benutzt, oder die unschuldige Person selbst vor sich hat. Dies kann für die unbescholtene Person sehr unangenehme Konsequenzen bis zur Klärung der Identität aufwerfen. Da dieses Problem mit dem aktuellen SIS datenverarbeitungstechnisch nicht zufriedenstellend lösbar ist, bedienen sich hiesige Polizeidienststellen einer vorläufigen Lösung, indem sie dem Betroffenen nach einer erkennungsdienstlichen Behandlung eine sogenannte Identitätsbescheinigung ausstellen, mit der er seine wahre Identität im Falle von polizeilichen Kontrollen nachweisen kann. Dies ist naturgemäß nur eine Behelfslösung, da sie im Einzelfall mit dem Verhältnismäßigkeitsprinzip kollidieren kann. Auch ist es zuweilen schwer vermittelbar, dass z. B. ein ausländischer Betroffener sich eine solche Identitätsbescheinigung ausstellen lassen soll, wenn ein von deutschen Stellen gesuchter Straftäter sich seiner Personalien bedient. Andererseits kann man bei gesuchten Schwerkriminellen kaum auf die weitere Speicherung von Alias-Personalien verzichten. Die GKI drängt darauf, dass bei der Neukonzeption des SIS eine datenschutzkonforme Lösung gefunden wird, die den unbescholtenen Betroffenen so wenig wie möglich in seinen Freiheitsrechten beeinträchtigt. Dies könnte beispielsweise durch ergänzende Angaben in dem Fahndungssystem geschehen.

- Auf einen besonders gravierenden Fall der missbräuchlichen Verwendung von Alias-Personalien hat mich ein italienischer Staatsbürger hingewiesen. Der Petent teilte mir mit, dass er im August 2000 nach einem Flug von Athen über Zürich nach Brüssel von der belgischen Grenzpolizei festgehalten wurde, weil seine Personalien von deutschen Stellen im SIS gespeichert waren. Nachdem er seine Identität als italienischer Staatsbürger nachweisen konnte, wurde er von der Grenzpolizei wieder entlassen. Meine daraufhin durchgeführte Kontrolle ergab, dass sich eine dritte Person missbräuchlich der Personalien des Petenten bedient und hierbei seinen gestohlenen Pass benutzt hatte. Daraufhin wurden die Personalien des Petenten als Alias-Datensatz zu dieser dritten Person im SIS gespeichert. Diese Person, die sich im März 2000 in Deutschland mit dem gestohlenen Pass des Petenten ausgewiesen hatte, wurde im Juni 2000 abgeschoben. Da der missbräuchlich benutzte Pass sichergestellt wurde und somit eine erneute missbräuchliche Benutzung auszuschließen ist, wurde der Alias-Datensatz des Petenten inzwischen gelöscht.

Damit ist die Angelegenheit für den Petenten im Ergebnis zwar zufriedenstellend beendet, da die durch die SIS-Speicherung eingetretenen Reisebeschränkungen nicht mehr bestehen. Gleichwohl war die nach Art. 96 SDÜ erfolgte Speicherung der Personalien des Petenten – auch als Alias-Datensatz – rechtswidrig. Nach dieser Vorschrift dürfen in das SIS nur Daten von Drittausländern eingestellt werden. Da der Petent jedoch die italienische Staatsbürgerschaft besitzt, war die Speicherung seiner Personalien nach Art. 96 SDÜ von Anfang an unzulässig. Spätestens bei Sicherstellung des gestohlenen Passes hätte die Unzulässigkeit der Speicherung bemerkt werden und die sofortige Löschung des Datensatzes erfolgen müssen.

Damit derartige Fälle für die Zukunft ausgeschlossen werden, habe ich das BMI gebeten, sicherzustellen, dass künftig Speicherungen nach Art. 96 SDÜ von Personalien von Staatsbürgern aus dem Hoheitsgebiet der Schengen-Vertragsstaaten, deren Daten missbräuchlich benutzt werden, unterbleiben. Auch diesbezüglich sind die Gespräche mit dem BMI noch nicht abgeschlossen.

11.11 EUROPOL – Gemeinsame Kontrollinstanz

Das Europäische Polizeiamt EUROPOL hat zum 1. Juli 1999 seinen Wirkbetrieb aufgenommen, nachdem im Anschluss an die Ratifizierung des EUROPOL-Übereinkommens auch die sonstigen Rechtsakte, darunter die Geschäftsordnung für die **Gemeinsame Kontrollinstanz** (GKI), vom Rat gebilligt worden waren. Unabhängig davon hat sich die GKI, in der ich gemeinsam mit dem LfD Sachsen-Anhalt vertreten bin, als das für den Datenschutz bei EUROPOL zuständige unabhängige Kontrollorgan bereits im Oktober 1998, also kurz nach Inkrafttreten der Konvention zum 1. Oktober 1998 konstituiert. Sie wurde unmittelbar danach mit den schwierigen Beratungen beim Rat über ihre eigene Geschäftsordnung konfrontiert. Dies ging so weit, dass die GKI, nachdem sie die Geschäftsordnung bereits gebilligt hatte, erneut darüber zu befinden hatte, weil die von ihr zunächst gebilligte Fassung im Rat keine Mehrheit fand. Besonders umstritten waren dabei die Regelungen über das Verfahren vor dem **Beschwerdeausschuss** (vgl. 17. TB Nr. 11.3). Ich habe dem Kompromiss letztlich zugestimmt, zumal es sich nicht um rein datenschutzrechtliche Fragen handelte. Entscheidend bleibt, dass Beschwerden gegen Entscheidungen von EUROPOL durch eine unabhängige Instanz überprüft werden. Die Unabhängigkeit der GKI ist durch die Regelungen in der Konvention und in der Geschäftsordnung gewährleistet. Die Kontrollinstanz verfügt zudem über einen eigenen Haushalt im Rahmen des EUROPOL-Budgets.

Da der Wirkbetrieb von EUROPOL sich so lange verzögert hatte, beschloss die GKI, proaktiv tätig zu werden.

Eine kleine Arbeitsgruppe unter Beteiligung der deutschen Delegation arbeitete einen Aktionsplan aus, der verschiedene Tätigkeitsschwerpunkte enthält, z. B. zu den Kontrollbesuchen, zur Anhörung bei Errichtungsanordnungen oder auch zur Öffentlichkeitsarbeit. Zu diesem Zweck wurden weitere Arbeitsgruppen aus je 4 bis 5 Mitgliedern gebildet, die die einzelnen Projekte, wie z. B. ein Prüfungsraster für datenschutzrechtliche Kontrollen, vorantreiben sollten. Die Vorschläge der Arbeitsgruppen wurden anschließend im Plenum der GKI erörtert und trugen so zur Straffung der Arbeit bei. Eine der Arbeitsgruppen war ein sog. Prüfungsteam, das im November 2000 eine erste datenschutzrechtliche Kontrolle bei EUROPOL durchführte. Diese bezog sich in erster Linie auf Fragen der Datensicherheit. Außerdem wurden einige Analyseprojekte nach Artikel 10 der Konvention kontrolliert. Eine Bewertung lässt sich erst nach Fertigstellung des Kontrollberichts ziehen, der bei Redaktionsschluss noch nicht vorlag. Das sog. Prüfungsteam sollte sich mit den verarbeitungstechnischen und datenschutzrechtlichen Vorkehrungen bei EUROPOL vertraut machen, was die weitere Tätigkeit der GKI erleichtern dürfte. Für das Jahr 2001 ist eine umfangreichere Kontrolle bei EUROPOL vorgesehen. Ihre Durchführung hängt aber von den weiteren Aktivitäten von EUROPOL beim Aufbau seiner Informationsverarbeitung ab. Hierbei gibt es noch Verzögerungen aufgrund technischer Schwierigkeiten.

Nach Artikel 12 der EUROPOL-Konvention ist die GKI beim Erlass von Errichtungsordnungen zu Analysedateien anzuhören. Bereits kurz nach seiner Tätigkeitsaufnahme hat EUROPOL der GKI mehrere Entwürfe solcher Errichtungsanordnungen zugeleitet. Im Rahmen der Anhörung hat sich die GKI u. a. für eine restriktive Speicherung von Daten über sonstige Personen (Zeugen, Informanten, Opfer usw.) ausgesprochen. Insbesondere sollten sog. sensitive Daten, z. B. über rassische Herkunft, Religion usw. vor allem zu Opfern nach Möglichkeit nicht gespeichert werden. Im einzelnen wird die GKI ihre Aktivitäten in einem eigenen Tätigkeitsbericht darstellen.

Nationale Stelle i. S. von Artikel 4 der Konvention ist das BKA. Es ist damit laut Vertragsgesetz für den Informationsaustausch mit EUROPOL verantwortlich. Ich habe das BKA aufgesucht, noch bevor erstmals Daten für Analysezwecke an EUROPOL übermittelt wurden. Das BKA plant eine dezentrale Übermittlung von Daten durch seine Fachdienststellen an EUROPOL. Ich habe dagegen vorgeschlagen, die Daten zentral über eine zu bestimmende Organisationseinheit zu übermitteln, damit einfacher festgestellt werden kann, wer welche Daten an EUROPOL übermittelt hat. Dies halte ich auch wegen des Rechts der Betroffenen auf Auskunft für wichtig sowie im Hinblick auf meine Kontrolltätigkeit. Das BKA möchte allerdings von einer speziellen Datei, in der die übermittelten Daten dokumentiert sind, vorerst Abstand nehmen. Zur Begründung weist es darauf hin, die Tatsache der Datenübermittlung werde in der Akte festgehalten, die über die gängigen IT-Verfahren zu erschließen ist. Im übrigen sei es über Art und Umfang der von anderen deutschen Stellen, z. B. den Landeskriminalämtern, an EUROPOL übermittelten Daten unterrichtet. Ich werde mich bei einer weiteren Kontrolle von der Stichhaltigkeit der Argumente des BKA überzeugen.

11.12 Gemeinsame Geschäftsstelle für die Kontrollinstanzen von Schengen und EUROPOL

Am 17. Oktober 2000 hat der EU-Rat die Einrichtung einer gemeinsamen Geschäftsstelle für die auf der Grundlage des Schengener Durchführungsübereinkommens (s. o. Nr. 11.9), und des EUROPOL-Übereinkommens (s. o. Nr. 11.10) jeweils tätigen datenschutzrechtlichen Kontrollinstanzen beschlossen (s. Amtsblatt der EG Nr. L271/1 vom 24. Oktober 2000). Der Rechtsakt sieht vor, dass die Geschäftsstelle ihre Arbeit am 1. September 2001 aufnimmt. Sie wird die Aufgaben wahrnehmen, die in den jeweiligen Geschäftsordnungen der Gemeinsamen Kontrollinstanzen für die Sekretariate dieser Instanzen vorgesehen waren und dabei auch für die noch einzurichtende Gemeinsame Kontrollinstanz nach dem ZIS-Übereinkommen (s. u. Nr. 13.4) tätig werden.

Dem Beschluss waren langjährige Beratungen in den EU-Gremien, die durch eine Initiative Italiens im Mai 1998 angeregt worden waren, vorausgegangen. Italien hatte vor dem Hintergrund der immer intensiver werdenden intergouvernementalen Zusammenarbeit in der dritten Säule der EU die Zersplitterung der Datenschutzregelungen für verschiedene komplexe Informationssysteme, wie z. B. SIS und EUROPOL, als aufwendig und praxiserschwerend beklagt und die Ausbildung einheitlicher Standards, die auch bei neuen Systemen im Rahmen der dritten Säule als feststehende Elemente eingebaut werden könnten, sowie eine institutionelle Vereinheitlichung der Datenschutzkontrolle in diesem Bereich angeregt. Die Initiative Italiens wurde von den EU-Datenschutzbeauftragten, die sich mit der Thematik auf ihren Konferenzen im April 1998 und April 1999 befassten, unterstützt. Die Beratungen in den EU-Gremien wurden unter deutscher Präsidentschaft im ersten Halbjahr 1999 aufgenommen. Es stellte sich rasch heraus, dass neben der Harmonisierung der Datenschutzbestimmungen in den Rechtsakten der dritten Säule nur die Einrichtung einer gemeinsamen Geschäftsstelle als Vorstufe zu einer einheitlichen Kontrollinstanz durchsetzbar war. Hierauf konzentrierten sich daher die Arbeiten der nachfolgenden EU-Präsidentschaften, in die auch die Gemeinsamen Kontrollinstanzen von Schengen und EUROPOL mit einbezogen waren.

Im Hinblick darauf, dass die vorgesehene gemeinsame Geschäftsstelle organisatorisch eng an das Generalsekretariat des Rates angebunden werden sollte, legten die Gemeinsamen Kontrollinstanzen besonderen Wert darauf, dass durch die Integration der bestehenden Sekretariate in die Geschäftsstelle deren unabhängige Aufgabenerfüllung im Dienste der Kontrollinstanzen nicht beeinträchtigt wird. Dies ist nunmehr nach dem EU-Ratsbeschluss u. a. dadurch gewährleistet, dass der Leiter der gemeinsamen Geschäftsstelle nur auf Vorschlag der Gemeinsamen Kontrollinstanzen ernannt und seines Amtes enthoben

werden kann sowie bei der Ausübung seines Amtes nur deren Weisungen unterliegt.

Ich begrüße die Einrichtung einer gemeinsamen Geschäftsstelle für die Kontrollinstanzen von Schengen und EUROPOL, betrachte diese jedoch nur als einen ersten Schritt auf den Weg zu einer gemeinsamen Kontrollinstanz im Rahmen der dritten Säule, von der ich mir noch weitgehendere Synergien erwarte. Zudem hoffe ich, dass die Beratungen zu den materiellen Grundsätzen des Datenschutzes in der dritten Säule ebenfalls erfolgreich abgeschlossen werden. Die in den Übereinkommen der dritten Säule enthaltenen, verschiedenartig ausgestalteten datenschutzrechtlichen Vorschriften können nur dann ihre Wirkung entfalten, wenn sie harmonisiert werden und die Rechtsmittel und Garantien, die diese Übereinkommen dem betroffenen Bürger bieten, aufeinander abgestimmt sind.

12 Bundesgrenzschutz

12.1 Durchführung des Bundesgrenzschutzgesetzes

Nachdem ich Anhaltspunkte dafür erhalten hatte, dass Defizite bei der Durchsetzung datenschutzrechtlicher Anforderungen bei den Dienststellen des BGS aufgetreten sind, habe ich im Berichtszeitraum schwerpunktmäßig Kontrollen bei verschiedenen seiner Dienststellen durchgeführt.

Durch die seit 1990 veränderte politische Lage haben sich Aufgaben und Befugnisse des BGS geändert. Die Diskussionen über weitergehende Einsatzmöglichkeiten des BGS dauern noch an. Entsprechend ist auch die dortige Datenverarbeitung teilweise bereits den erweiterten Bedürfnissen angepasst worden. Zum Teil befindet sie sich noch in der Aufbauphase. Unter anderem ist über den Ausbau oder Umbau der integrierten Vorgangsbearbeitung – IPV – BGS (vgl. 17. TB Nr. 12.2) noch nicht abschließend entschieden worden. Hinzu kommt, dass durch die Umstellung des polizeilichen Informationssystems INPOL (s. o. Nr. 11.2), an dem der BGS teilnimmt, ebenfalls Neuerungen auf die Grenzschutzbehörden zukommen, die auch datenschutzrechtlich begleitet werden müssen. Insbesondere in den Bereichen Bahnpolizei und Verbrechensbekämpfung aber auch im Zusammenhang mit der organisierten Kriminalität, z. B. bei der Bekämpfung der Schleuserkriminalität hat die Datenverarbeitung erheblich zugenommen, wofür die vielen Errichtungsanordnungen für Spurendokumentationssysteme und Hinweisdokumentationsdateien sprechen, die ich gerade in letzter Zeit erhalten habe. Dies zeigt u. a. auch eine Datei, die vom Bundesgrenzschutzamt Frankfurt/Main zur Bekämpfung der Taschen-, Trick- und Handgepäckdiebstahlkriminalität auf den Betriebsanlagen der Deutschen Bahn AG geführt wird.

Wenngleich ich mit der Bundesgrenzschutzdirektion im Rahmen der Anhörung zu Errichtungsanordnungen für automatisiert betriebene Dateien nach § 36 BGSG nicht immer in allen Punkten übereinstimme, lässt sich feststellen, dass die Errichtungsanordnungen ein beachtliches datenschutzrechtliches Niveau aufweisen. Sie sind auch für mich eine nützliche Grundlage zur Durchführung datenschutzrechtlicher Kontrollen.

12.2 Kontrollen beim BGS

12.2.1 Die Datei „Aktennachweis des Bundesgrenzschutzes“

Ein Schwerpunkt der bei einem Bundesgrenzschutzamt durchgeführten datenschutzrechtlichen Kontrolle waren die Datei „Aktennachweis des Bundesgrenzschutzes“ (BAN) sowie die dazu geführten personenbezogenen Akten. Folgende Defizite habe ich festgestellt:

Nach der Errichtungsanordnung ist davon auszugehen, dass im BAN alle personenbezogenen Akten, deren Führung bei Dienststellen des BGS zur Erfüllung der ihm obliegenden Aufgaben auf den Gebieten der Strafverfolgung, der Ahndung von Ordnungswidrigkeiten und der Gefahrenabwehr erforderlich sind, nachgewiesen werden. Die Kontrolle hat jedoch gezeigt, dass ein Teil der Akten des BGS in der Datei KAN nachgewiesen wird. Bei dieser Datei handelt es sich um den beim BKA geführten zentralen Nachweis von Kriminalakten, die beim Bund und den Ländern in Fällen schwerer oder überregional bedeutsamer Straftaten im Sinne von § 2 Abs. 1 BKAG über Beschuldigte oder sonstige tatverdächtige Personen angelegt werden. Da die Errichtungsanordnung für den BAN keine Abgrenzungskriterien für die Fälle der Speicherung in der jeweils anderen Datei vorsieht, habe ich gefordert, dass in diesem Punkt die Errichtungsanordnung geändert wird.

Der Nachweis von BGS-Akten im KAN wird in den betreffenden Fällen damit begründet, dass diesen regelmäßig Straftaten zugrunde liegen, die an der Grenze begangen wurden und damit nach Auffassung des BGS überregionale Bedeutung erlangten. Ich halte diese Sichtweise für problematisch, zumal es in von mir festgestellten gleichgelagerten Fällen, in denen derartige Straftaten im Inland begangen wurden, zu keiner KAN-Speicherung gekommen ist. Meiner Ansicht nach ist die Anknüpfung allein an die Örtlichkeit einer Straftat nicht das geeignete Abgrenzungskriterium, um die für eine KAN-Speicherung erforderliche Erheblichkeit und überregionale Bedeutung dieser Tat zu begründen. So habe ich z. B. eine Speicherung im KAN gem. § 25 BDSG beanstandet, die einen Ausländer betraf, der mit einer gefälschten ausländischen Zugfahrkarte mit dem Zug in das Bundesgebiet einreisen wollte. Die Speicherung ist daraufhin gelöscht worden.

Die Aufnahme personenbezogener Daten im KAN hat nämlich zur Folge, dass sich die Aussonderungsprüffristen nach den für diese Datei geltenden Zehnjahresfristen richten, anstelle der für das Aktennachweissystem des BGS geltenden Fünfjahresregelung. Die gleiche Proble-

matik ergibt sich für solche Datensätze, bei denen Beschuldigte durch BGS-Dienststellen erkennungsdienstlich behandelt worden sind oder eine kurzfristige Untersuchungshaft verbüßt haben. Aus systemtechnischen Gründen werden diese Informationen ebenfalls in Dateien des BKA abgebildet mit der Folge, dass auch hier die Aussonderungsprüffrist für den BAN durch die längeren Fristen der BKA-Dateien verdrängt wird.

Ich habe den BGS aufgefordert, die Praxis der KAN-Speicherungen zu überprüfen, insbesondere in den Fällen, in denen die hierfür erforderliche besondere Bedeutung und Überregionalität im Sinne von § 2 Abs. 1 BKAG mit der Begehung einer Straftat allein an einer bestimmten Örtlichkeit, z. B. an der Grenze, begründet wird. Aus meiner Sicht ist es zudem problematisch, Daten zu Sachverhalten, die speziell die Aufgaben und Befugnisse des BGS betreffen, in Dateien einzustellen, auf die auch andere Polizeien des Bundes und die Polizeien der Länder Zugriff haben. Solange an dieser Systematik aber festgehalten werden soll, müssten wenigstens erheblich kürzere Aussonderungsprüffristen festgelegt werden, insbesondere bei der erstmaligen Speicherung personenbezogener Daten in einer dieser Dateien.

Die Kontrolle des BAN hat zudem ergeben, dass bei Speicherungen grundsätzlich die allgemeinen Aussonderungsprüffristen nach der Errichtungsanordnung angewandt werden. Ich halte es für geboten, von der schematischen Vergabe der Aussonderungsprüffristen abzugehen, da es sowohl sachlich gerechtfertigt als auch unter datenschutzrechtlichen Gesichtspunkten erforderlich ist, die Aussonderungsprüffristen am Einzelfall orientiert flexibel zu vergeben. Die bisherige Handhabung zeigt, dass in der überwiegenden Anzahl der Fälle die gespeicherten personenbezogenen Daten während dieser Zeit nicht auf die Erforderlichkeit der weiteren Speicherung überprüft werden. Eine Überarbeitung der Errichtungsanordnung BAN sollte darüber hinaus bei der Festlegung der Speicherungsdauer zu einer Differenzierung zwischen Personen kommen, die als Beschuldigte möglicherweise durch ein Gericht verurteilt wurden und Personen, bei denen das Verfahren im Wege der Einstellung nach § 153a StPO oder § 154b StPO beendet wurde.

Das BMI teilt meine Auffassung zur Ergänzung der Errichtungsanordnung für den BAN in den genannten Punkten. Eine überarbeitete Fassung der Errichtungsanordnung lag bei Redaktionsschluss noch nicht vor.

Bei der Kontrolle des BAN habe ich zahlreiche Fälle beanstandet, in denen entgegen den Regelungen über die Löschung personenbezogener Daten nach dem BGS-Gesetz in Verbindung mit der Errichtungsanordnung zum BAN Datensätze nicht gelöscht und BAN-Akten nicht vernichtet worden waren. Es handelte sich hierbei u. a. um Verfahren, die von den Justizbehörden gemäß § 170 Abs. 2 StPO eingestellt worden waren, z. B. weil sich im Rahmen eines zunächst eingeleiteten Ermittlungsverfahrens herausgestellt hatte, dass die dem Betroffenen zur Last gelegte Tat nur als Ordnungswidrigkeit verfolgt werden konnte. Zudem waren Fälle darunter, in denen die Aussonderungsprüffristen abgelaufen waren, die Dateispeicherung sowie die Akte ohne erkennbaren Grund aber weiter vorgehalten wurde. Schließlich wurden Akten weiterhin aufbewahrt, obwohl die entsprechenden Dateispeicherungen bereits gelöscht waren.

Das BMI hat die Beanstandungen zum Anlass genommen, in der betreffenden BGS-Dienststelle die Bereinigung des Daten- und Aktenbestandes anzuordnen.

12.2.2 Datenverarbeitung in einer BGS-Bußgeldstelle

Bei der Kontrolle der Datenverarbeitung der in der BGS-Dienststelle eingerichteten Bußgeldstelle habe ich folgende Mängel festgestellt:

Verstöße nach dem Ordnungswidrigkeitengesetz haben zu personenbezogenen Speicherungen und entsprechenden Aktenanlagen im BAN geführt. Es handelte sich in aller Regel um Fälle, denen ursprünglich ein Verwarnungs- bzw. ein Bußgeld zugrunde lag, welches nicht bzw. nicht fristgerecht gezahlt wurde. Sofern die Erfassung nicht erforderlich ist, um bei Wiederholung des Tatbestandes strafrechtliche Ermittlungen gegen den Betroffenen einleiten zu können, habe ich angeregt, in Anbetracht der niedrigen Deliktschwelle in diesen Fällen generell auf eine Erfassung im BAN zu verzichten. Auch insoweit halte ich eine Ergänzung der Errichtungsanordnung für den BAN für erforderlich.

In der Bußgeldstelle wurde eine (Excel-)Tabelle automatisiert geführt, in der personenbezogene Daten über verhängte Bußgelder verarbeitet wurden. Die Tabelle diente, wie mir erläutert wurde, ausschließlich statistischen Zwecken. Das BMI teilt meine Bewertung, dass für diese Zweckbestimmung die Speicherung personenbezogener oder personenbeziehbarer Informationen nicht erforderlich ist. Obwohl es die Löschung der besagten Tabelle anordnete, wurde diese – wie eine Nachkontrolle in dem BGS-Amt ergab – weiterhin in personenbeziehbarer Form geführt.

Personen, gegen die ein Verwarnungs- oder Bußgeld festgesetzt worden war, wurden bundesweit zur polizeilichen Fahndung ausgeschrieben. Dies wurde damit begründet, dass wegen des unbekannten Wohnsitzes der Betroffenen entsprechende Bescheide nicht zugestellt werden konnten. Betroffen waren auch Jugendliche. In einem Fall war gegen eine 17-jährige wegen des unberechtigten Aufenthalts auf freier Strecke der Deutschen Bahn AG ein Verwarnungsgeld von DM 20,– verhängt worden. Die Ausschreibungen stellen einen Verstoß gegen die Regelungen der einschlägigen Polizeidienstvorschrift dar, die im einzelnen die Voraussetzungen für Fahndungsausschreibungen festlegt. Zwar nimmt der BGS nach dem BGS-Gesetz auch die polizeilichen Aufgaben nach dem Gesetz über Ordnungswidrigkeiten wahr. Im Falle der Kostenbeitreibung von festgesetzten Verwarnungs- oder Bußgeldern handelt er jedoch als Verwaltungsbehörde, der das Instrument der Ausschreibung zur Fahndung nicht zur Verfügung steht.

Nachdem ich diese Fälle gem. § 25 BDSG beanstandet habe, sind die Tabelle und die Ausschreibungen mittlerweile gelöscht worden.

12.3 Videoüberwachung durch Polizeibehörden

In der Diskussion über die Videoüberwachung im öffentlichen Raum nahm vor allem der Einsatz der Videotechnik zum Zwecke der Gefahrenabwehr und der Kriminalitätsbekämpfung breiten Raum ein. Neben zahlreichen Vertretern der Polizei sieht auch die Ständige Konferenz der Innenminister und -senatoren der Länder mit ihrem Beschluss vom 5. Mai 2000 in dem offenen Einsatz von Videoüberwachungsmaßnahmen an Kriminalitätsbrennpunkten im öffentlichen Raum ein geeignetes Mittel, um die Wahrnehmung der polizeilichen Aufgaben wirksam zu unterstützen. In der Folge wurde eine Reihe von Landespolizeigesetzen um Regelungen ergänzt, auf deren Grundlage Videoüberwachung zulässig ist.

Im Hinblick auf die besonderen Risiken, die mit der Videoüberwachung für das Grundrecht auf informationelle Selbstbestimmung verbunden sind, haben die Datenschutzbeauftragten des Bundes und der Länder auf ihrer 59. Konferenz vom 14./15. März 2000 eine Entschließung (s. **Anlage 20**) gefasst. Sie fordern, dass bei einer gesetzlichen Regelung der Videoüberwachung durch öffentliche Stellen Einschränkungen nur aufgrund einer klaren Rechtsgrundlage erfolgen dürfen, die dem Grundsatz der Verhältnismäßigkeit Rechnung trägt. Aus meiner Sicht mag der Einsatz von Videotechnik an sog. Kriminalitätsschwerpunkten, an denen wiederholt Straftaten begangen worden sind und Anhaltspunkte dafür bestehen, dass auch künftig dort Straftaten begangen werden, gerechtfertigt sein, soweit mit der Beobachtung neben der Sicherung von Beweisen eine Präventionswirkung erreicht werden kann. Hingegen ist die Schaffung flächendeckender Beobachtungsmöglichkeiten durch Videokameras zur Verhinderung bloßer Störungen der öffentlichen Ordnung mit dem Grundsatz der Verhältnismäßigkeit nicht zu vereinbaren.

12.3.1 Videoüberwachung durch BGS und BKA

Videoüberwachungsmaßnahmen werden auch von den Polizeien des Bundes ergriffen. Sowohl das BKA-Gesetz als auch das BGS-Gesetz enthalten abschließende Befugnisregelungen zum Einsatz von Videotechnik zur Aufgabenerfüllung.

Nach Maßgabe des BKA-Gesetzes können Videoaufzeichnungen zur Eigensicherung von Bediensteten im Rahmen der Strafverfolgung durch das BKA sowie zum Zwecke der Durchführung von Personenschutz- und Zeugenschutzaufgaben vorgenommen werden. Der BGS kann im Zusammenhang mit vielen seiner Aufgaben Videoüberwachungsmaßnahmen durchführen. So kann er gem. § 26 BGSG bei Veranstaltungen oder Ansammlungen, die nicht unter das Versammlungsgesetz fallen, personenbezogene Daten auch durch Bildaufzeichnungen von Teilnehmern erheben. Die Befugnis ist jedoch begrenzt auf Veranstaltungen oder Ansammlungen an der Grenze oder in der Nähe von Objekten, die dem Schutz des BGS unterliegen. Es handelt sich dabei um Einrichtungen des BGS, der Eisenbahnen des Bundes oder des Luftverkehrs sowie um die Amtssitze von Verfassungsorganen und Bundesministerien und um Grenzübergangsstellen. Der BGS hat zudem die Befugnis, nach Maßgabe des § 27 BGSG selbständige Bildaufnahme- und Bildaufzeichnungsgeräte einzusetzen, um unerlaubte Grenzübertritte bzw. Gefahren für die Sicherheit an der Grenze oder Gefahren für die o.g. Objekte bzw. die dort befindlichen Personen oder Sachen zu erkennen.

Vor dem Hintergrund, dass Aufgaben der Gefahrenabwehr und der Strafverfolgung grundsätzlich Sache der Länder sind und dem Bund nur in bestimmten speziellen Bereichen ordnungsbehördliche oder vollzugspolizeiliche Aufgaben obliegen, sind die genannten Regelungen im BKA-Gesetz und im BGS-Gesetz zum Einsatz von Videotechnik im Hinblick auf die begrenzten Kompetenzen des BKA bzw. des BGS ausreichend. Es besteht kein Anlass, die bestehenden Befugnisse zur Nutzung der Videotechnik, die als spezialgesetzliche Regelung der allgemeinen Regelung des § 6 b der BDSG-Novelle (s. o. Nr. 2.1) vorgehen werden, auszuweiten.

12.3.2 Einsatz der Videoüberwachung an der deutsch-polnischen Grenze

Ich habe die Diskussion über die Videoüberwachung zum Anlass genommen, mich über den Einsatz der Videotechnik durch den BGS an der deutsch-polnischen Grenze zu informieren. Die Videokameras sind dort offen erkennbar, um den Grenzverkehr an den Grenzübergangsstellen zu überwachen. Zum Erkennen unerlaubter Grenzübertritte und deren Verhinderung in den Nachtzeiten werden zudem entlang der Grenze Spezialkameras, montiert auf Patrouillenbooten oder in Fahrzeugen des BGS, eingesetzt.

Datenschutzrechtliche Probleme bereitet die vom BGS praktizierte Aufbewahrung der Aufzeichnungen, die von den an einer Grenzübergangsstelle installierten Überwachungskameras übertragen werden. Ich habe festgestellt, dass das voll bespielte Videoband eine Woche aufbewahrt wird und die darauf gespeicherten Bilddaten erst nach Ablauf dieser Zeit durch Überspielen gelöscht werden. Die generelle Aufbewahrung der Videoaufnahmen über einen Zeitraum von einer Woche halte ich im Hinblick auf § 27 BGSG für problematisch, da das Gesetz als datenschutzrechtliches Korrektiv eine „unverzügliche“ Vernichtung der aufgezeichneten Bilddaten verlangt, soweit diese nicht zur Abwehr einer gegenwärtigen Gefahr oder zur Verfolgung einer Straftat oder Ordnungswidrigkeit benötigt werden.

Ich führe hierzu noch Gespräche mit dem BMI über eine gesetzeskonforme Anwendung des Einsatzes von Videoüberwachungsmaßnahmen an den Grenzübergangsstellen und anderen Schutzobjekten des BGS. Ein Ergebnis lag bei Redaktionsschluss noch nicht vor.

12.4 Zu viele Daten bei einer Abschiebung weitergegeben

Ein türkischer Staatsangehöriger hat sich nach der Abschiebung in sein Heimatland an mich gewandt, weil personenbezogene Daten bei der Abschiebung vom **BGS** an türkische Behörden übermittelt worden waren. Ich habe festgestellt, dass aufgrund BGS-interner Dienstvorschriften dem Empfängerstaat eine Aufzeichnung übergeben wurde, aus der sich die Gründe der Abschiebung, nämlich *„unerlaubter Aufenthalt in der Bundesrepublik Deutschland"* und *„kriminelle Handlungen"*, ergaben. Die Übermittlung zumindest der Information *„kriminelle Handlungen"* halte ich für unzulässig, weil personenbezogene Daten an öffentliche Stellen anderer Staaten nach den Bestimmungen des BGSG nur übermittelt werden dürfen, soweit dies u. a. zur Erfüllung einer dem BGS obliegenden Aufgabe erforderlich ist. Das betreffende Grenzschutzamt hat nicht dargelegt, dass die Weitergabe der Informationen gegenüber der türkischen Grenzschutzbehörde zur Durchführung der Abschiebung erforderlich war. Auch die internen Bestimmungen des BGS zur Abschiebung sind ein Indiz dafür, dass im vorliegenden Fall allenfalls *„unerlaubter Aufenthalt in der Bundesrepublik Deutschland"* hätte übermittelt werden dürfen. Bei dieser Sachlage gewinnt § 33 Abs. 3 BGSG besonderes Gewicht, wonach die Übermittlung personenbezogener Daten unterbleibt, wenn für den BGS erkennbar ist, dass unter Berücksichtigung der Art der Daten und ihrer Erhebung die schutzwürdigen Interessen des Betroffenen das allgemeine Interesse an der Übermittlung überwiegen. Diese Abwägung hatte der BGS im vorliegenden Fall nicht vorgenommen. Insoweit bewerte ich die Übermittlung des Merkmals „kriminelle Handlungen" als einen Verstoß gegen § 32 Abs. 3 i. V .m. § 33 BGSG.

Darüber hinaus hätte der BGS bei der Übermittlung den Empfänger auf die zweckgebundene Verwendung der Daten hinweisen müssen. Ebenso hätte nach den Bestimmungen des BGSG den türkischen Behörden der vorgesehene Löschungszeitpunkt mitgeteilt werden müssen, was ebenfalls unterblieben ist. Diese Verstöße gegen § 33 Abs. 6 Sätze 2 und 3 BGSG habe ich beanstandet. In seiner Stellungnahme hat mir das BMI entgegnet, der seinerzeit verwendete Vordruck sei nicht mehr in Gebrauch. Als Grund für Rückführungen sei lediglich ein Hinweis auf den illegalen Aufenthalt in der Bundesrepublik Deutschland anzugeben. Die „Bestimmungen über die Rückführung ausländischer Staatsangehöriger auf dem Luftweg" seien ebenfalls neu gefasst worden; so wurde festgelegt, dass ein Dokument mit den Abschiebungsgründen zwar mitzuführen sei, der ausländischen Grenzdienststelle aber nur auf deren Verlangen auszuhändigen ist. Weitergehende Angaben, wie z. B. zu in Deutschland begangenen Straftaten oder die Tatsache, dass der Rückzuführende einen Asylantrag gestellt hat, seien nicht darin aufzunehmen.

13 Zollfahndung

13.1 Zollfahndungsdienstgesetz – endlich – in Vorbereitung

Die Bundesregierung erarbeitet derzeit, 17 Jahre nach dem Volkzählungsurteils des Bundesverfassungsgerichts, einen Referentenentwurf für ein Zollfahndungsdienstgesetz, welches Aufgaben und Befugnisse des Zollkriminalamtes und des gesamten Zollfahndungsdienstes regeln soll. Es bleibt zu hoffen, dass das Gesetzgebungsverfahren zügig durchlaufen wird, damit endlich die Tätigkeit auch dieser Bundespolizeibehörde entsprechend den Vorgaben des Bundesverfassungsgerichts zum informationellen Selbstbestimmungsrecht auf eine bereichsspezifische und normenklare Rechtsgrundlage gestellt wird, die – unter Beachtung des Verhältnismäßigkeitsgrundsatzes – die Verwendung personenbezogener Daten auf einen gesetzlich bestimmten Zweck begrenzt. Die Bundesregierung käme damit im übrigen auch einer Forderung des Deutschen Bundestages anlässlich der Billigung einer Beschlussempfehlung des Innenausschusses zu meinem 16. TB nach (vgl. 17. TB Nr. 13.1).

13.2 INZOLL-VHG

Neben den Polizeibehörden des Bundes und der Länder sind auch der Zollfahndungsdienst und das ZKA zur Bekämpfung der Geldwäsche nach § 261 StGB zuständig, und zwar bei der Erforschung und Verfolgung der international organisierten Geldwäsche. Zur Unterstützung dieser Aufgabe ist beim ZKA eine Datenbank INZOLL-VHG (Verdacht, Hinweise, Geldwäsche) entwickelt worden, die im März 2000 nach jahrelangen Vorbereitungen ihren Wirkbetrieb aufgenommen hat. Mittlerweile läuft die Datei unter der Bezeichnung VHG. Bei der Anhörung zu der hierzu erforderlichen Errichtungsanordnung habe ich wie bei der Geldwäsche-Verbunddatei beim BKA (s. o. Nr. 11.4), datenschutzrechtliche Bedenken erhoben, die sich in erster Linie gegen den Kreis der zu erfassenden Personen richten. Denn in der Datei VHG sollen sämtliche dem Zollfahndungsdienst bekannt werdenden personenbezogenen Daten aus Verdachtsanzeigen nach § 11 GWG, aus Bargeldkontrollen nach § 12a FVG (s. u. Nr. 13.5) sowie von Zollbehörden übermittelte Daten mit Geldwäschebezug erfasst werden, ohne Rücksicht darauf, ob die jeweiligen Meldungen tatsächlich einen begründeten Verdacht auf strafbare Geldwäsche auslösen und ob die betroffene Person einer derartigen Tat in der Folge beschuldigt wird. Ferner habe ich gegen eine Speicherung solcher Fälle für die Dauer von sechs Jahren votiert, weil ich diese lange Frist für unverhältnismäßig erachte. Trotz meiner grundlegenden Vorbehalte gegen die Datei VHG, die ihrer Zwecksetzung nach zu einem erheblichen Teil der bloßen Verdachtsgewinnung bzw. -verdichtung dient, beharrt das BMF auf der Grundkonzeption der Datei und der darin vorgesehenen Speicherung aller Verdachtsanzeigen, weil nur so die Konzeption der Bundesregierung zur Geldwäschebekämpfung (sog. Puzzletheorie) umzusetzen sei. Es wird daher zu verifizieren

sein, ob diese Theorie wirklich zu praktischen Erfolgen führen wird, wenn mit der Datei längere Zeit gearbeitet wurde.

Da mittlerweile Einvernehmen über die Errichtungsanordnung zur Geldwäsche-Verbunddatei beim BKA erzielt wurde (s. o. Nr. 11.4), erscheint es mir angebracht, für die Datei INZOLL-VHG mit Bezug auf die besonderen Gegebenheiten beim ZKA – u. a. fehlen noch bereichsspezifische Datenschutzregelungen – eine ähnliche Regelung anzustreben. Zu den verbesserungsbedürftigen Tatbeständen zählen insbesondere die Beschränkung des Kreises der zu erfassenden Personen, also der „Verdächtigen", sowie eine Verkürzung der Speicherungsdauer unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes und in Anlehnung an die Regelung beim BKA.

13.3 Neapel II-Übereinkommen

Im 17. TB (s. Nr. 13.4) habe ich ausführlich über den Regelungsgehalt des Übereinkommens der EU-Mitgliedstaaten über gegenseitige Amtshilfe und Zusammenarbeit der Zollverwaltungen vom 18. Dezember 1997, des sog. Neapel II-Übereinkommens, berichtet. Der Vertrag bezweckt u. a., die Zusammenarbeit zwischen den Zollverwaltungen der EU-Mitgliedstaaten bei der Verhinderung, Ermittlung und Verfolgung von Zuwiderhandlungen gegen Zollvorschriften zu verbessern. Er soll für die Anwender durch einen Kurzleitfaden ergänzt werden, der allerdings noch nicht fertiggestellt wurde.

Das federführende BMF hat im Jahre 2000 den Arbeitsentwurf eines Vertragsgesetzes zu dem Übereinkommen nach Art. 59 Abs. 2 GG übersandt. Ich habe keine grundlegenden datenschutzrechtlichen Bedenken gegen den Entwurf vorgebracht, jedoch darauf hingewiesen, dass ich eine Verabschiedung, die zeitlich vor den notwendigen innerstaatlichen Regelungen im Zollbereich (s. o. Nr. 13.1) erfolgt, für problematisch halte. Nach den Reaktionen der Bundesressorts auf den Entwurf hat das BMF bis zum Redaktionsschluss noch keine Fortschreibung des Arbeitsentwurfs vorgelegt.

13.4 ZIS-Übereinkommen

Zu den wichtigen Vorhaben grenzüberschreitender Zusammenarbeit im Rahmen der dritten Säule der EU (Inneres und Justiz) gehört die Einrichtung eines Zollinformationssystems – ZIS – der Mitgliedstaaten (vgl. zuletzt 17. TB Nr. 13.5). Rechtsgrundlage ist das *Übereinkommen über die Nutzung der Informationstechnologie im Zollbereich* vom 26. Juli 1995. Das ZIS der dritten Säule soll im Auftrag der Mitgliedstaaten von der Europäischen Kommission (OLAF), die selbst für das ZIS der ersten Säule (Binnenmarkt) zuständig ist (s. o. Nr. 7.9), betrieben werden. Es ist nach seiner Grundkonzeption eine Ausschreibungsdatenbank, ähnlich dem Schengener Informationssystem SIS (s. o. Nr. 11.9), und greift bei

- nationalen Verboten und Beschränkungen des grenzüberschreitenden Warenverkehrs sowie
- Geldwäsche bei der Vortat „Rauschgiftschmuggel".

Trotz des langen Vorlaufs hat das ZIS seinen Wirkbetrieb noch nicht aufgenommen. Während das zeitgleich unterzeichnete EUROPOL-Übereinkommen (s. o. Nr. 11.10) bereits zum 1. Oktober 1998 in Kraft trat, kam es bei der Ratifizierung des ZIS-Übereinkommens zu Verzögerungen, weil es bisher nicht alle EU-Mitgliedstaaten, unter ihnen Deutschland, ratifiziert haben. Ergänzend zur Konvention wurde allerdings noch im Jahre 1995 eine *Übereinkunft über die vorläufige Anwendung des Übereinkommens zwischen einigen Mitgliedstaaten der EU* unterzeichnet. Diese ergänzende Regelung trat zum 1. November 2000 in Kraft, weshalb es jetzt – abgesehen von der Ratifizierung durch die restlichen Mitgliedstaaten – nur noch der technischen Realisierung des Projekts bedarf. Der Testbetrieb war bei Redaktionsschluss noch nicht aufgenommen.

Es gab vielfältige Gründe für die Verzögerung des Vorhabens, obwohl es nach dem Aktionsplan der EU zur Bekämpfung der organisierten Kriminalität vom April 1997 bereits Ende 1998 in Kraft treten sollte. Zu den rechtlichen Hürden zählte insbesondere ein Meinungsstreit unter den Mitgliedstaaten über die Zielsetzung des ZIS. Ursprünglich als Ausschreibungsdatenbank konzipiert, wollten einige Mitgliedstaaten das Vorhaben zu einem Aktennachweissystem für Zwecke der Recherche erweitern und hielten dies mit dem Wortlaut des Übereinkommens für vereinbar. Hiergegen hatte ich – ebenso wie die Bundesregierung – Bedenken, weil dies nur mit erweiterten Datenfeldern und mit zusätzlichen Zugriffsrechten realisierbar gewesen wäre. Ein von der Bundesregierung als Alternative vorgeschlagener weiterer Rechtsakt über die Einrichtung eines separaten Aktennachweissystems dürfte jedoch im Kreis der Mitgliedstaaten nicht mehrheitsfähig sein. Bei Redaktionsschluss waren diese juristischen Fragen noch nicht abschließend geklärt.

Unabhängig hiervon wurde im Rat auch über einen möglichen Zugriff von EUROPOL auf den ZIS-Datenbestand diskutiert. Diese Option war ebenfalls für EUROPOL in dem o. g. Aktionsplan vorgesehen. Ungeachtet der Regelung des Art. 7 Abs. 3 des ZIS-Übereinkommens, die eine solche Öffnung vorsieht, habe ich mich, ebenso wie im Falle des SIS (s. o. Nr. 11.10) gegen einen Direktzugriff von EUROPOL auf das künftige ZIS ausgesprochen, zumal auch der formale Aspekt in Gestalt einer vorherigen Anhörung der Kontrollinstanz nach Art. 18 des Übereinkommens noch nicht erfüllt war. Denn dieses Gremium hatte sich bei Redaktionsschluss dieses Berichts noch nicht konstituiert.

Die Bundesrepublik Deutschland ist dem ZIS-Übereinkommen noch nicht beigetreten, auch nicht dem zuvor erwähnten vorläufigen Verfahren. Zwar hat das federführende BMF bereits Ende 1998 den Arbeitsentwurf eines Ratifizierungsgesetzes vorgelegt, doch mangels bereichsspezifischer Regelungen im Zoll- und Zollfahndungsbereich wurde dieses Vorhaben bald wieder ad acta gelegt, bis die innerstaatlichen Voraussetzungen durch die Schaffung bereichsspezifischer Regelungen erfüllt sind (vgl. hierzu 15. TB Nr. 35.6 für die Zollverwaltung und s. o. Nr. 13.1 für den Zollfahndungsdienst).

In dem Kontrollgremium nach Art. 18 des ZIS-Übereinkommens, dessen erste Sitzung ich für Anfang 2001 erwarte, werde ich mich vor allem dafür einsetzen, dass die schutzwürdigen Interessen von Betroffenen auch bei der grenzüberschreitenden Zusammenarbeit im Zollbereich gewahrt bleiben.

13.5 Bargeldkontrollen an den Grenzen

Durch eine Eingabe sowie durch Berichte in den Medien bin ich auf die Problematik der intensiven Befragung Reisender an den deutschen Grenzen bezüglich der von ihnen mitgeführten Bargeldbeträge durch Bedienstete des Zolls und des BGS aufmerksam geworden.

Diese Befragungen, insbesondere an der deutsch-schweizerischen Grenze sowie an der deutsch-luxemburgischen Grenze, sind auf die Überwachung des grenzüberschreitenden Bargeldverkehrs zurückzuführen, mit der die Zollverwaltung und der BGS durch Artikel 4 des Gesetzes zur Verbesserung der Bekämpfung der Organisierten Kriminalität vom 4. Mai 1998 (BGBl. I S. 848) beauftragt worden sind. Diese sog. Bargeldkontrollen sollen die Maßnahmen des Geldwäschegesetzes zur Verhinderung des Einschleusens illegaler Gewinne in den Finanzkreislauf über Kredit- und Finanzinstitute ergänzen, indem nunmehr auch das körperliche Verbringen von Verbrechensgewinnen über die nationalen Grenzen erfasst wird. Aufgaben und Kontrollbefugnisse der Zollverwaltung sowie der Umfang der dabei zu erhebenden und zu verarbeitenden personenbezogenen Daten ergeben sich aus § 12a Finanzverwaltungsgesetz (FVG) i. V. m. § 10 Zollverwaltungsgesetz (ZollVG). Die Einzelheiten der Durchführung von Bargeldkontrollen sind zudem in der vom BMF erlassenen Verwaltungsvorschrift zur Überwachung des grenzüberschreitenden Bargeldverkehrs (BargeldVV) vom 27. Juli 1998 geregelt.

Danach haben Personen beim Grenzübertritt auf Verlangen Bargeld oder andere Zahlungsmittel, wie z. B. Wertpapiere, Schecks, Edelmetalle, die sie in die, aus der oder durch die Bundesrepublik Deutschland bringen wollen, nach Art, Zahl und Wert anzuzeigen, sofern deren Gesamtwert 30.000,- DM oder mehr beträgt. In diesem Fall muss über deren Herkunft, den wirtschaftlich Berechtigten und den Verwendungszweck Auskunft gegeben werden. Verneint hingegen der Betroffene die Frage nach Zahlungsmitteln und hat der Kontrollbeamte Zweifel an der Richtigkeit der Antwort, so hat er wiederholt den Betroffenen zur Anzeige unter Hinweis darauf aufzufordern, dass unrichtige Angaben eine Ordnungswidrigkeit darstellen und den Verdacht einer Geldwäschehandlung begründen können. Die Erhebung anderer, nicht auf mitgeführte Zahlungsmittel bezogener Daten ist auf der Grundlage des § 12a FVG nicht zulässig.

Die offenbar häufig über diesen Rahmen hinausgehende Befragung durch Kontrollbeamte an den Grenzen ist möglicherweise auf folgende Umstände zurückzuführen: Nach der ursprünglichen Fassung des § 12a FVG konnten bei Bargeldkontrollen erhobene personenbezogene Daten an andere Finanzbehörden nur übermittelt werden, wenn sich bei den Kontrollen Anhaltspunkte für eine Geldwäsche ergeben hatten und darüber hinaus die Übermittlung für steuerliche Zwecke erforderlich war. In der Praxis ergaben sich solche Anhaltspunkte nur in den seltensten Fällen. Im Interesse einer gesetzmäßigen, gleichmäßigen Besteuerung sah sich der Gesetzgeber daher veranlasst, die Möglichkeit der Datenübermittlung an Steuerbehörden zu modifizieren. Durch Artikel 23 des Steuerbereinigungsgesetzes 1999 (BGBl. I S. 2621) wurde § 12a Abs. 4 Satz 3 FVG mit Wirkung vom 1. Januar 2000 dahingehend geändert, dass auf das Vorliegen von Anhaltspunkten für die Geldwäsche als Voraussetzung einer Datenübermittlung an andere Finanzbehörden verzichtet wurde. Die Übermittlung personenbezogener Daten ist nach der neuen Rechtslage zudem schon dann zulässig, soweit ihre Kenntnis zur Durchführung eines Besteuerungsverfahrens oder eines Straf- oder Bußgeldverfahrens in Steuersachen lediglich von Bedeutung sein kann.

Aus den Beschwerden von kontrollierten Reisenden ist auch dem BMF bekannt geworden, dass die wesentlich erweiterten Befugnisse zur Datenübermittlung durch die Zollverwaltung zu einem geänderten Verhalten der Zoll- bzw. der Grenzschutzbediensteten bei der Durchführung von Bargeldkontrollen insofern geführt haben, als dazu übergegangen wurde, steuerlich möglicherweise relevante Fragen selbst dann zu stellen, wenn der Reisende keine höheren Geldbeträge mit sich geführt hat und auch andere Anhaltspunkte für einen geldwäscherelevante Sachverhalt nicht gegeben waren. Ich begrüße es daher, dass das BMF die Rechtslage bezüglich des zulässigen Umfangs der Datenerhebung im Zusammenhang mit den Bargeldkontrollen an den Grenzen durch Befragen der Reisenden gegenüber den Dienststellen der Zollverwaltung in mehreren Erlassen vom Juni und Juli dieses Jahres nochmals klargestellt hat.

Gleichwohl – und hierauf weisen die genannten Erlasse ausdrücklich hin – haben die Zoll- bzw. BGS-Bediensteten im Rahmen der Bargeldkontrollen aber auch die Befugnis, die Vorlage von Ausweispapieren zu verlangen, Beförderungsmittel und mitgeführte Sachen zu durchsuchen sowie – bei zureichenden Anhaltspunkten für einen geldwäscherelevanten Vorgang – die betreffende Person zu durchsuchen. Auch die Prüfung von Unterlagen, soweit diese erfahrungsgemäß Anhaltspunkte für die Beförderung von Zahlungsmittel enthalten können, ist zulässig. Hierzu zählen insbesondere Bankunterlagen, wie z. B. Kontoauszüge oder Überweisungsquittungen. Die Durchsicht privater Korrespondenz hat dagegen grundsätzlich zu unterbleiben. Selbst wenn sich im Rahmen dieser Kontrollen, etwa bei der Prüfung von Unterlagen, keine Anhaltspunkte auf Geldwäsche ergeben, können die Zoll- bzw. Grenzschutzbediensteten die daraus erlangten Kenntnisse an Finanzbehörden übermitteln, soweit deren Kenntnis zur Durchführung der bereits genannten Verfahren von Bedeutung sein kann.

Entgegen der erklärten Absicht des Gesetzgebers hinsichtlich einer effektiveren Bekämpfung der Organisierten Kriminalität dient die grenzüberschreitende Kontrolle des Bargeldverkehrs also in erster Linie dazu, ins Ausland abgewanderte Kapitalanleger mittels einer „mobilen

Steuerfahndung“ zu ermitteln. Gleichwohl sind die Zoll- und Grenzschutzbediensteten auch in diesen Fällen gehalten, bei ihrem Vorgehen das Prinzip der Verhältnismäßigkeit zu beachten.

14 Verfassungsschutz

14.1 Einführung des „Elektronischen Büros“ im BfV

Der Fortschritt in der Informationstechnik wird auch im BfV verstärkt genutzt. Für die Projektierung eines „Elektronischen Büros“ nach dem KBSt-Modell im Rahmen des Projektes der Bundesregierung „Moderner Staat – Moderne Verwaltung“, das auf weitere Sicht die Verarbeitung von Daten in Akten stark zurückdrängen soll, sind nach Auffassung des BfV einige Vorschriften des BVerfSchG, die die Speicherung, Veränderung und Nutzung personenbezogener Daten in Dateien regeln (§§ 6 und 10 bis 14 BVerfSchG), „überholungsbedürftig“ geworden. Sie entsprächen nicht den aktuellen Anforderungen an eine moderne Verwaltung und würden das BfV in seiner Aufgabenerfüllung erheblich behindern, weil die Verarbeitung von personenbezogenen Daten in textmäßiger Form nur eingeschränkt zulässig ist.

Bei einem papierarmen Büro ist es unvermeidlich, dass ganze Texte elektronisch gespeichert werden, nicht nur durch Textverarbeitung, sondern auch durch das Scannen von Unterlagen und Veröffentlichungen. Heute kann grundsätzlich jede Art von digital gespeicherten Informationen, d. h. nicht nur strukturierte Dateien, sondern auch Textverarbeitung und elektronisches Archiv nach vorgegebenen Kriterien ausgewertet werden. Diese gespeicherten Informationen enthalten zwangsläufig auch personenbezogene Daten von Personen, die nicht die Speicherkriterien des § 10 Abs. 1 Nr. 1 und 2 BVerfSchG erfüllen, die also vom BfV nicht dateimäßig erfasst werden dürfen. Solche Datensammlungen sind mit der geltenden Rechtslage nicht vereinbar. Da ich mich der technischen Entwicklung nicht verschließen kann, habe ich bis zu einer normenklaren Regelung einer Übergangslösung im Rahmen des Projektes „Elektronisches Büro“ zugestimmt, die die Speicherung und eingeschränkte weitere Verarbeitung und Nutzung dieser Datensammlungen ermöglicht. Um einen datenschutzrechtlichen Missbrauch auszuschließen, muss sichergestellt werden, dass nicht nach solchen Personen recherchiert wird, bei denen die Speicherungsvoraussetzungen des BVerfSchG nicht vorliegen. Dies soll durch eine lückenlose Protokollierung aller Abrufe unter Einschluss des Grundes der Recherche gewährleistet werden. Hierdurch erhalte ich die Möglichkeit, die Einhaltung der Datenschutzvorgaben zu überprüfen. Im Rahmen einer Dateianordnung ist der Kreis der betroffenen Personen, auf den sich die Recherche erstrecken darf, abschließend und für den Bearbeiter im BfV eindeutig festzulegen.

Das BfV hat bereits Vorschläge zur entsprechenden Änderung der restriktiven Vorschriften der §§ 6 und 10 bis 14 BVerfSchG gemacht und will sie in der zweiten Stufe der BDSG-Novellierung weiter verfolgen.

14.2 Datenschutzrechtliche Kontrolle und Quellenschutz

In meinem 17. TB (Nr. 14.1) hatte ich über eine 1998 geschlossene Vereinbarung mit dem BfV berichtet, die das Verfahren bei Kontrollen im Zusammenhang mit quellengeschützten Unterlagen regelt. Diese Vereinbarung hatte ein Verfahren zum Ziel, das beim Umgang mit Verschlusssachen einerseits den berechtigten Interessen des BfV nach größtmöglicher Geheimhaltung zu laufenden Operationen, verdeckten Mitarbeitern oder sonstigen Informanten, Quellen oder Hilfspersonen Rechnung trägt und andererseits mir eine umfassende Kontrolle entsprechend meinem gesetzlichen Auftrag ermöglicht.

Beim Abschluss dieser Vereinbarung war ich davon ausgegangen, dass das dort im Einzelnen beschriebene Verfahren nur selten angewandt wird. Wie sich jedoch zwischenzeitlich bei der Kontrolle einer Datei gezeigt hat, waren nahezu alle mit dieser Datei zusammenhängenden Unterlagen als quellengeschütztes Material eingestuft. Unter Hinweis auf die Vereinbarung von 1998 wurde meinen Mitarbeitern die Einsichtnahme in diese Unterlagen verwehrt. Eine umfassende Kontrolle wäre aber nur möglich gewesen, wenn meinen Mitarbeitern der Inhalt des quellengeschützten Materials von der Fachabteilung des BfV vorgetragen worden wäre oder ich persönlich Einsicht in die Vorgänge genommen hätte. Wegen des großen Umfangs des zu sichtenden Aktenmaterials waren aber beide Möglichkeiten für mich nicht akzeptabel. Da eine ordnungsgemäße Kontrolle nach § 24 Abs.1 BDSG unter diesen Umständen nicht möglich war, wurde sie abgebrochen.

Das im 17. TB beschriebene Verfahren hat sich für die Fälle als nicht praktikabel erwiesen, in denen nahezu der gesamte zu prüfende Aktenbestand aus quellengeschützten Informationen besteht. Ich habe dies mit dem BfV erörtert und konnte erfreulicherweise eine deutliche Verbesserung erreichen, was sich bei zwei danach folgenden Kontrollen zeigte. Hier wurden meinen Mitarbeitern mit wenigen Ausnahmen sämtliche quellengeschützten Unterlagen zur Einsichtnahme vorgelegt. Eine Einsichtnahme wurde aus Gründen des Quellenschutzes nur dann verweigert, wenn aus den Unterlagen direkt auf eine Quelle hätte geschlossen werden können.

Die letzten Kontrollen haben gezeigt, dass es möglich ist, die Interessen des BfV an einer Geheimhaltung nachrichtendienstlicher Verbindungen mit meiner umfassenden Kontrollbefugnis in Einklang zu bringen. Ich gehe davon aus, dass diese Praxis auch für die Zukunft Bestand haben wird.

14.3 Einsichtsrecht der Verwaltungsgerichte in geheimhaltungsbedürftige Unterlagen

Auf die Verfassungsbeschwerde eines Bürgers, der sich zuvor auch an mich gewandt hatte, hat das BVerfG mit seinem Beschluss vom 27. Oktober 1999 (BVerfGE 101, 106) eine weitere Entscheidung von datenschutzrechtlicher Bedeutung gefällt.

Der Beschwerdeführer hatte die Geschäftsführung einer Landeseinrichtung übernommen, die Aufträge der öffentlichen Hand, u. a. der Bundeswehr und weiterer sicherheitsrelevanter Einrichtungen, vermittelt und die der Rechtsaufsicht eines Landes-Wirtschaftsministeriums untersteht. Das zuständige Landesamt für Verfassungsschutz kam im Rahmen der Sicherheitsüberprüfung zu dem Ergebnis, dass Bedenken gegen eine Ermächtigung des Beschwerdeführers zum Umgang mit Verschlusssachen bestünden. Die Landesauftragstelle erklärte daraufhin dem Beschwerdeführer, eine Weiterbeschäftigung komme aus diesem Grund nicht in Betracht. Der Beschwerdeführer kündigte das Dienstverhältnis selbst, um Nachteile bei späteren Bewerbungen möglichst gering zu halten. Seine anschließenden Bewerbungen um gehobene Positionen sollen gleichwohl erfolglos geblieben sein, da er die eilige Kündigung nicht plausibel erklären konnte. Der Beschwerdeführer begehrte vom zuständigen Landesamt für Verfassungsschutz Auskunft über die Daten, die dem negativen Ergebnis der Sicherheitsüberprüfung zugrunde lagen. Dies wurde abgelehnt mit der Begründung, eine Auskunft würde „die ordnungsgemäße Erfüllung der Aufgaben der Behörde beeinträchtigen". Auch gegenüber den angerufenen Verwaltungsgerichten gab der Verfassungsschutz kaum mehr Informationen preis. In letzter Instanz bestätigte das oberste Verwaltungsgericht des Landes die gesetzlichen Voraussetzungen für die Verweigerung der Auskunft. Dagegen legte der Beschwerdeführer wegen Verstoßes gegen das Grundrecht der Gewährung effektiven Rechtsschutzes nach Art. 19 Abs. 4 GG Verfassungsbeschwerde ein, die zum Erfolg führte.

Nach dem Beschluss des BVerfG müssen Verfassungsschutzbehörden zumindest dem prüfenden Verwaltungsgericht die Akten und Unterlagen, die einer Beurteilung und Entscheidung in Angelegenheiten einer Sicherheitsüberprüfung zugrunde liegen, aushändigen. Dies ist jedoch auf die zuständige Kammer des Gerichts beschränkt (in-camera-Verfahren). Ist auch diese der Auffassung, dass es im Staatsinteresse liegt, den Vorgang geheim zu halten, wird dem Kläger der Inhalt der Vorgänge nicht zur Kenntnis gegeben. Anders liegt der Fall, wenn das Gericht keine einer Offenlegung entgegenstehende Gründe erkennen kann.

Das BVerfG hat dem Gesetzgeber den Auftrag erteilt, § 99 VwGO bis Ende 2001 neu zu regeln. Bis dahin müssen die Behörden die Akten an die Verwaltungsgerichte weitergeben, allerdings ohne dass ein Verfahrensbeteiligter von deren Inhalt Kenntnis erhält. Ich begrüße diese Entscheidung des BVerfG. Von der Änderung der VwGO erwarte ich eine größere Transparenz bei Gerichtsverfahren im Anschluss an eine Sicherheitsüberprüfung.

14.4 BfV verlangt Herausgabe von E-Mail-Adressen bei Zugangsprovidern

Durch eine Eingabe erhielt ich Kenntnis, dass das BfV einen Betreiber interaktiver Online-Dienste um die Herausgabe der Inhaberdaten zu einer bestimmten E-Mail-Adresse ersucht hatte. Die Behörde stützte ihr Ersuchen auf § 3 Abs. 1 BVerfSchG. Diese Regelung definiert den Aufgabenbereich des BfV; sie verleiht dem BfV aber nicht die Befugnis zu derartigen Ersuchen. Weil in diesem Fall eine nicht-öffentliche Stelle – ein Teledienstеanbieter – Daten übermitteln sollte, habe ich die Eingabe an die örtlich zuständige Aufsichtsbehörde des Landes abgegeben. Diese teilte dem Petenten mit, es bestehe keine Auskunftspflicht gegenüber dem BfV, da es sich bei Einrichtung und Betrieb eines E-Mail-Account um einen Teledienst im Sinne des TDG handele. Es bestehe weder eine Berechtigung noch eine Verpflichtung von Teledienstеanbietern zur Herausgabe von Bestandsdaten im Sinne des § 5 TDDSG an diese Sicherheitsbehörde.

Ich habe danach das BfV in dieser Angelegenheit kontrolliert und darauf hingewiesen, dass ich Einrichtung und Betrieb eines E-Mail-Account für einen Teledienst im Sinne des TDG halte (vgl. zu dieser strittigen Frage 17. TB Nr. 10.1.2) und die Übermittlung von Daten im Sinne des § 5 TDDSG an diese Sicherheitsbehörde nicht zulässig sei. Insbesondere sei auch § 3 BVerfSchG als Rechtsgrundlage für ein solches Auskunftsbegehren nicht geeignet. Nach langem Zögern teilte mir das vom BfV eingeschaltete BMI mit, Rechtsgrundlage für Auskunftsersuchen gegenüber E-Mail-Adresseninhabern sei § 8 Abs. 1 in Verbindung mit § 3 BVerfSchG. Die entsprechende Auskunftspflicht des Providers ergebe sich aus § 89 Abs. 6 TKG. Wegen der strittigen Anwendbarkeit des TKG auf solche Fälle sei jedoch das federführende BMWi um grundsätzliche Klärung gebeten worden. Bis Redaktionsschluss lag mir dessen Reaktion nicht vor.

Meines Erachtens handelt es sich im vorliegenden Fall um einen Zugangsprovider, der jedenfalls auch Teledienste im Sinne von § 2 Abs. 2 Nr. 3 TDG anbietet, zumal die Verwaltung von E-Mailadressen in der Regel nicht der alleinige Geschäftszweck solcher Unternehmen ist. Ich folge insoweit der Auffassung der zuständigen Aufsichtsbehörde. Somit ist das TDDSG einschlägige Rechtsgrundlage, das in § 2 Nr. 1 auch den Zugangsprovider als *„Diensteanbieter im Sinne dieses Gesetzes"* ansieht. Das Gesetz enthält keine Auskunftsverpflichtung der Provider gegenüber den Sicherheitsbehörden. Eine solche Verpflichtung war noch im Regierungsentwurf zum IuKDG vorgesehen, wurde jedoch in den parlamentarischen Beratungen nicht zuletzt auf Betreiben der Datenschutzbeauftragten des Bundes und der Länder nicht mehr aufrechterhalten. Auch in dem Novellierungsentwurf zum TDDSG, der derzeit vorbereitet wird (s. u. Nr. 8.1), ist eine solche Verpflichtung nicht vorgesehen; insbesondere datenschutzrechtliche Gründe sprechen dagegen, neben der derzeitigen Regelung, die Übermittlungen an die Straf-

verfolgungsbehörden zulässt, weitere Übermittlungen vorzusehen.

15 Militärischer Abschirmdienst – MAD –

15.1 Änderung des MAD-Gesetzes

Nach § 1 Abs. 1 des Gesetzes über den Militärischen Abschirmdienst (MADG) ist der MAD zuständig für die Sammlung und Auswertung von Informationen über verfassungsfeindliche Bestrebungen und sicherheitsgefährdende oder geheimdienstliche Tätigkeiten, wenn sich diese Bestrebungen oder Tätigkeiten gegen Personen, Dienststellen oder Einrichtungen im Geschäftsbereich des BMVg richten und von Personen ausgehen oder ausgehen sollen, die diesem Geschäftsbereich angehören oder in ihm tätig sind. Um bei eingehenden Erkenntnismitteilungen anderer Sicherheitsbehörden die Zuständigkeit des MAD zu prüfen und die rasche Identifizierung von Angehörigen der Bundeswehr zu ermöglichen, benötigt der MAD nach eigenen Angaben einen Zugriff auf das Personalinformationssystem der Bundeswehr (PERFIS). Dies geschieht derzeit in der Weise, dass dem MAD-Amt eine Unterdatei aus der Datei PERFIS mit einem eingeschränkten Datensatz zur Verfügung gestellt wird. Im Rechenzentrum des MAD-Amtes werden die monatlich aktualisierten Daten auf einer Festplatte installiert und als separat betriebene Datenbank geführt, zu der nur speziell ermächtigte Nutzer Zugriff haben.

Beim Zugriff auf die Datei PERFIS – auch in Form einer daraus abgeleiteten Unterdatei – handelt es sich um eine automatisierte Abfrage von Personaldaten. Hinsichtlich dieser Daten gilt damit das Personaldatengeheimnis, das nur – auch zu Gunsten der Sicherheitsbehörden – durchbrochen werden darf, wenn dies nach dem Bundesbeamtengesetz (BBG) bzw. dem Soldatengesetz (SG) zulässig ist. Da sowohl § 90 d Abs. 1 Satz 2 BBG als auch § 29 Abs. 2 und 3 SG die Übermittlung von Personaldaten nur auf konventionellem Wege – d. h. nach Einzelfallprüfung – erlauben, habe ich bereits vor Jahren eine spezialgesetzliche Regelung für den automatisierten Zugriff auf PERFIS für Zwecke des MAD gefordert. Im Hinblick auf die vom BMVg angekündigte Gesetzesänderung habe ich bislang von einer Beanstandung der bisherigen Praxis abgesehen und mich mit der oben erwähnten Zwischenlösung einverstanden erklärt.

Nunmehr hat mir das BMVg den Entwurf eines „Ersten Gesetzes zur Änderung des MAD-Gesetzes“ übermittelt, der § 10 Abs. 2 MADG dahingehend ergänzen soll, dass der MAD die zur Erfüllung seiner Aufgaben erforderlichen personenbezogenen Daten aus PERFIS im automatisierten Verfahren abrufen darf. Der Zugriff auf PERFIS soll jedoch auf einen aus zwölf Einzeldaten bestehenden Datensatz begrenzt werden, der ausschließlich der Identifizierung des Betroffenen dient. Zudem ist eine Protokollierung aller Datenabrufe vorgesehen. Der Gesetzentwurf berücksichtigt damit meine datenschutzrechtlichen Forderungen.

Mit dem vorgenannten Gesetzentwurf beabsichtigt das BMVg ferner, die Tätigkeit des MAD zum Schutz eines deutschen Bundeswehrkontingents im Auslandseinsatz auf eine zweifelsfreie rechtliche Grundlage zu stellen. In einem neuen § 14 soll die Zuständigkeit des MAD über § 2 Abs. 1 Nr. 2 MADG hinaus auch auf die Informationsgewinnung und -verarbeitung ausgedehnt werden, die anlässlich einer *„besonderen Auslandsverwendung der Bundeswehr..... oder anlässlich einer humanitären Maßnahme zur Sicherung der Einsatzbereitschaft der Truppe oder zum Schutz der Angehörigen, der Dienststellen und Einrichtungen des Geschäftsbereichs des BMVg erforderlich sind“*. Ich habe gegen diese Zuständigkeitserweiterung keine grundsätzlichen Bedenken, da die datenschutzrechtlichen Vorgaben des MADG auch für die bei diesen Auslandseinsätzen anfallenden personenbezogenen Daten in vollem Umfang gelten.

15.2 Änderung der Grundsatzweisung des MAD über die Anwendung nachrichtendienstlicher Mittel

Der wegen der akustischen Wohnraumüberwachung geänderte Artikel 13 GG (Gesetz zur Änderung des Art. 13 GG vom 26. März 1998 – BGBl. I S. 601), der auch für Abhörmaßnahmen der Nachrichtendienste in Wohnungen eine richterliche Anordnung voraussetzt, machte es erforderlich, die Grundsatzweisung des MAD über die Anwendung nachrichtendienstlicher Mittel zu überarbeiten (s. 17. TB Nr. 15.2). Dies ist bis heute nicht geschehen. Vielmehr gilt eine Anfang 1997 in Kraft gesetzte Fassung, die im wesentlichen mit der Fassung von 1993 in der von mir kritisierten Form identisch ist, immer noch.

Im Hinblick auf die durch Artikel 11 des Strafverfahrensänderungsgesetzes 1999 (StVÄG 1999 – BGBl. I S. 1253) geänderte Fassung des § 9 Abs. 2 BVerfSchG, der über § 5 MADG auch vom MAD anzuwenden ist, habe ich das BMVg dringend aufgefordert, die Grundsatzweisung entsprechend zu ändern und folgende Forderungen zu berücksichtigen:

- Vorrang gesetzlicher Zeugnisverweigerungsrechte,
- höhere Verhältnismäßigkeitsschwelle in Bezug auf Unbeteiligte,
- Erfüllung der Voraussetzungen des Art. 13 GG bei Eingriffen in die Unverletzlichkeit der Wohnung,
- Regelungen zur Zweckbindung und Löschung von Daten sowie zu Wiedervorlagefristen der Akten

Das BMVg hat mir im Oktober 2000 dazu mitgeteilt, die gesetzliche Neuregelung werde zur Aktualisierung der Grundsatzweisung führen. Meine Anregungen würden dabei sorgfältig geprüft und – soweit möglich – umgesetzt.

Der Vorschlag des BMVg zur Änderung der Grundsatzweisung lag bei Redaktionsschluss noch nicht vor; ich sehe ihm mit Interesse entgegen.

15.3 Übersicht über alle Errichtungsanordnungen ist für meine Aufgabenerledigung erforderlich

Der MAD hat für jede automatisierte Datei, in der personenbezogene Daten gespeichert sind, eine Dateianordnung zu erstellen, vor deren Erlass meine Anhörung vorgesehen ist (§ 8 MADG i. V. m. § 14 BVerfSchG). Nachdem ich bereits in meinem 15. TB (Nr. 27) deren schleppende Vorlage kritisiert hatte, hat mir das BMVg in der Zwischenzeit zahlreiche Dateianordnungen zur Anhörung übermittelt. Mit wenigen Ausnahmen, über die ich mit dem BMVg noch im Gespräch bin, haben sich zu den Dateianordnungen keine erörterungsbedürftigen datenschutzrechtlichen Bedenken ergeben.

Um mir einen Überblick über alle beim MAD geführten Dateien mit personenbezogenen Daten zu verschaffen, habe ich das BMVg bereits Mitte 1999 unter Hinweis auf die in § 24 Abs. 4 BDSG normierte Mitwirkungspflicht des Ministeriums bei der Erfüllung meines gesetzlichen Auftrags um Übersendung einer entsprechenden Auflistung gebeten. Das BMVg hat hierzu anlässlich eines Informationsbesuchs beim MAD-Amt erklärt, dass es selbst aus Gründen der Geheimhaltung bislang über eine solche Übersicht nicht verfüge.

Die von mir geforderte Übersicht ist für meine Aufgabenerfüllung erforderlich, weil sie mir einen Überblick darüber verschafft, ob sich die beim MAD geführten Dateien auf das erforderliche Maß beschränken. Sie erlaubt mir zudem die Prüfung, ob alle entsprechenden Dateianordnungen unter meiner Beteiligung erlassen wurden. Dazu erleichtert sie dem BMVg die ihm nach § 14 Abs. 2 BVerfSchG obliegende Pflicht, in angemessenen Abständen die Notwendigkeit der Weiterführung oder Änderung der Dateien zu überprüfen. Im übrigen werden solche Dateiübersichten auch bei den anderen Sicherheitsbehörden des Bundes geführt, weshalb die vom BMVg genannten Geheimhaltungsgründe nicht stichhaltig erscheinen.

Nach mehrmaliger Erinnerung und längerer Diskussion hat mir das BMVg kurz vor Redaktionsschluss die Übersendung einer solchen Übersicht doch noch zugesagt.

16 Bundesnachrichtendienst – BND –

16.1 Gesetz zu Art. 10 GG (G 10)

16.1.1 Entscheidung des Bundesverfassungsgerichts vom 14. Juli 1999 zur Fernmeldeaufklärung des BND

Mit Art. 13 des Verbrechensbekämpfungsgesetzes vom 28. Oktober 1994 (BGBl. I S. 3186) wurde das Gesetz zu Art. 10 GG (G 10) umfassend geändert. Unter rechtlichen Gesichtspunkten wurden die Aufgaben des BND durch die Novellierung zwar nicht erweitert. Er bekam aber die Befugnis, seine zuvor nur auf die Abwehr der Gefahr eines bewaffneten Angriffs begrenzte sog. strategische Kontrolle auf zusätzliche Gefahrenbereiche auszudehnen, wenn auch beschränkt auf den internationalen, nicht leitungsgebundenen Fernmeldeverkehr. Die hierbei anfallenden personen- und sachbezogenen Erkenntnisse sind im Rahmen dieser Befugniserweiterung an die für Maßnahmen der Gefahrenabwehr und der Strafverfolgung zuständigen Behörden – d. h. die Staatsanwaltschaften, Polizeibehörden und das Zollkriminalamt, aber auch die anderen Nachrichtendienste – zu übermitteln.

Bereits kurz nach Inkrafttreten wurden gegen § 3 G 10 Verfassungsbeschwerden aus dem Bereich von Presse und Wirtschaft erhoben. Das Bundesverfassungsgericht erließ am 5. Juni 1995 eine einstweilige Anordnung, wonach bei Durchführung der Abwehrmaßnahmen erlangte personenbezogene Daten nur dann verwendet und übermittelt werden dürfen, wenn **bestimmte Tatsachen** den Verdacht eines bewaffneten Angriffs, internationaler terroristischer Aktivität, der Proliferation oder Verbreitung von Kriegswaffen, des Waffen- oder Drogenhandels, der Geldfälschung oder Geldwäsche begründen (s. 17. TB Nr. 16.4). Ging es in der Entscheidung zum Volkszählungsgesetz 1983 noch um die zwangsweise Erhebung personenbezogener Daten für statistische Zwecke und deren mögliche Nutzung auch für Zwecke des Verwaltungsvollzugs, so betraf das Beschwerdeverfahren die **heimliche** Informationsbeschaffung durch den BND beim grenzüberschreitenden Fernmeldeverkehr. Solche Beschränkungsmaßnahmen als Eingriff in das Grundrecht nach Art. 10 GG auf unbeobachtete Kommunikation sind nur zulässig mit dem Ziel, Nachrichten zum Sachverhalt zu sammeln, deren Kenntnis notwendig ist, um der Gefahr der Begehung der oben genannten Straftaten rechtzeitig begegnen zu können.

Auf Ersuchen des Bundesverfassungsgerichts habe ich am 20. März 1995 und am 4. Dezember 1996 zu den Verfassungsbeschwerden schriftlich Stellung genommen. An der mündlichen Verhandlung am 15. und 16. Dezember 1998 habe ich gemeinsam mit einigen Landesbeauftragten für den Datenschutz Gelegenheit zu ergänzenden datenschutzrechtlichen Äußerungen bekommen.

Das Bundesverfassungsgericht hat am 14. Juli 1999 entschieden, dass das Gesetz zum Teil mit dem Grundgesetz unvereinbar ist. Es hat der weiterhin bestehenden grundsätzlichen Befugnis des BND, ohne Verdacht den internationalen nichtleitungsgebundenen Fernmeldeverkehr mit elektronischem Raster, den sog. Wortdatenbanken, zu überwachen, deutliche Schranken gesetzt. Die Rechte der Betroffenen bei der heimlichen Informationsbeschaffung werden gestärkt und der Übermittlungsbefugnis des BND an andere Behörden klare Grenzen gesetzt. Auch muss die Datenschutzkontrolle im G 10-Bereich den gesamten Prozess der Erfassung und Verwertung der Daten umfassen und personell entsprechend ausgestattet sein. Eine meiner Forderungen (s. 17. TB Nr. 16.4), eine effektive und lückenlose Datenschutzkontrolle im G 10-Bereich zu schaffen, ist damit aufgegriffen

worden. Der Gesetzgeber wurde verpflichtet, bis zum 30. Juni 2001 einen verfassungsmäßigen Zustand herzustellen, indem er die klaren Vorgaben des Gerichts zum Schutz des Grundrechts aus Art. 10 GG und anderer Grundrechte im Interesse der betroffenen Bürgerinnen und Bürger umsetzt (s. u. Nr. 16.1.2). Bis dahin ist das Gesetz nur entsprechend nach vom Gericht festgelegten Maßregeln anzuwenden.

Das Bundesverfassungsgericht hat mit seiner Entscheidung die Sicherheitsinteressen des Staates und die Rechte der Betroffenen wieder in ein vernünftiges, ausgewogenes Verhältnis gestellt und dabei die Grundsätze des Volkszählungsurteils von 1983 fortentwickelt, indem es die grundrechtlichen Vorgaben zum Schutz des Rechts auf informationelle Selbstbestimmung auf das Fernmeldegeheimnis nach Art. 10 GG übertragen hat. Insoweit bedeutet das Urteil einen Meilenstein für den Datenschutz.

16.1.2 Novellierung des Gesetzes zu Art. 10 GG

In Anbetracht der zeitlichen Vorgabe des Bundesverfassungsgerichts in seiner Entscheidung vom 14. Juli 1999 (s. o. Nr. 16.1.1) begann die Bundesregierung im Herbst 1999 mit den Vorbereitungen zur Novellierung des Gesetzes zu Art. 10 GG (G10). Zu den Ressortgesprächen, vor allem mit dem federführenden BMI, dem BK und dem BMJ, bin ich von Beginn an hinzugezogen worden. Ab Mai 2000 fanden Gespräche mit Innenpolitikern der Koalitionsfraktionen statt, an denen ich ebenfalls teilnahm.

Bei den Beratungen zeigte sich bald, dass die Bundesregierung das Gesetzgebungsvorhaben nutzen will, über die Vorgaben des Gerichts hinaus weitere Änderungen im G10-Bereich zu erreichen. Sie begründet dies mit der fortschreitenden technischen Entwicklung und zwischenzeitlich erkannten Lücken des bisherigen Gesetzes. So soll u. a. die strategische Fernmeldekontrolle des BND auf internationale Telekommunikation ausgedehnt werden, die durch Lichtwellenleiter gebündelt übertragen wird. § 3 Abs. 1 Satz 1 G10 in der geltenden Fassung beschränkt die Kontrolle auf nicht leitungsgebundene Telekommunikation, jedenfalls für die in Satz 2 Nr. 2 bis 6 genannten Gefahrenbereiche.

Der Referentenentwurf wurde Anfang 2001 im Bundeskabinett beraten und danach dem Bundesrat zugeleitet. Es ist beabsichtigt, das Gesetz innerhalb der vom BVerfG gesetzten Zweijahresfrist in Kraft zu setzen.

Für mich sind folgende Punkte bei der Novellierung von besonderer Wichtigkeit:

1. Lückenlose Datenschutzkontrolle im gesamten G10-Bereich:

   Der Entwurf stellt klar, dass sich die Kontrollkompetenz der G10-Kommission, die neben dem Parlamentarischen Kontrollgremium für die Kontrolle der G10-Maßnahmen im einzelnen zuständig ist, auf Bundesebene auf die gesamte Erhebung, Verarbeitung und Nutzung der G10-Erkenntnisse durch Nachrichtendienste des Bundes erstreckt. Die Kontrollkompetenz geht auf mich über, wenn Informationen aus dem G10-Bereich – z. B. um eine Straftat zu verhindern – von Nachrichtendiensten an andere Bundesstellen übermittelt und dort verarbeitet oder genutzt werden. Damit ist der Forderung des Bundesverfassungsgerichts, durch eine normenklare Regelung die Kontrolle des gesamten Prozesses der Erfassung und Verwertung der durch Beschränkungsmaßnahmen erlangten Daten klarzustellen, Genüge getan.

   Weiter regelt der Entwurf auf meine Anregung hin in Anlehnung an § 24 BDSG einzelne Befugnisse der G10-Kommission. Danach ist ihr insbesondere Auskunft zu ihren Fragen zu erteilen und Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und die Datenverarbeitungsprogramme, die im Zusammenhang mit der Beschränkungsmaßnahme stehen, zu gewähren. Außerdem hat sie jederzeit Zutritt in alle Diensträume. Bei der Durchführung der Kontrolle kann mir die Kommission *„Gelegenheit zur Stellungnahme in Fragen des Datenschutzes geben“*.

   Auch die Forderung des Gerichts nach einer ausreichenden Personal- und Sachausstattung der Kommission, gesondert ausgewiesen im Einzelplan des Deutschen Bundestages, bis hin zur Verpflichtung der Kommission, *„Mitarbeiter mit technischem Sachverstand“* zur Verfügung zu stellen, ist im Entwurf vorgesehen.

2. Evaluierung aller G10-Maßnahmen:

   Wie andere Gesetze auf dem Gebiet der Inneren Sicherheit wirft das G10-Gesetz die Frage nach der Geeignetheit der vorgesehenen Maßnahmen auf. Seit langem fordere ich bei tiefen und/oder häufigen Eingriffen in das Persönlichkeitsrecht, wie etwa bei der Telefonüberwachung nach § 100 a StPO, eine wirksame Evaluierung und Erfolgskontrolle (s. 17. TB Nrn. 6.1 und 11.2). Das BMJ hat, was ich sehr begrüße, inzwischen ein entsprechendes Forschungsvorhaben auf den Weg gebracht (s. o. Nr. 11.8).

   Die im Zusammenhang mit der akustischen Wohnraumüberwachung durch das Gesetz zur Änderung des Grundgesetzes (Art. 13) vom 26. März 1998 (BGBl. I S.610) jetzt in § 100 e StPO geregelten Berichtspflichten markieren einen maßgeblichen Schritt in Richtung einer Gesetzesevaluierung bei Eingriffsmaßnahmen. Solche Berichtspflichten ermöglichen bei entsprechender Umsetzung eine laufende parlamentarische Kontrolle dieser mit intensiven Grundrechtseingriffen verbundenen Maßnahmen. Sie sollen das Parlament in die Lage versetzen, die Angemessenheit und Eignung der angeordneten Maßnahmen zu überprüfen (s. o. Nrn. 6.4.2 und 11.8). In diesem Zusammenhang verweise ich auf die Entschließung der Datenschutzbeauftragten von Bund und Ländern vom 26. Juni 2000, mit der Forderungen erhoben bzw. Anregungen gegeben werden im Hinblick auf den gegenwärtig noch nicht ausreichenden Berichtsinhalt für nach § 100e Abs. 1 Nr. 3 StPO getroffene Maßnahmen (s. **Anlage 22**).

Der G10-Entwurf enthält zur Evaluierung zwar erfreuliche Verbesserungen; sie reichen aber noch nicht aus.

Ein wichtiger Fortschritt ist die Aufnahme **aller** Maßnahmen, auch der Individualmaßnahmen nach § 2 G10, in die Berichtspflicht an den Deutschen Bundestag. Hierüber wurde auf mein Drängen erst spät eine Einigung erzielt.

Entgegen der Regelung des § 100e StPO, wonach in den Bericht **Anlass, Umfang, Dauer, Ergebnis und Kosten der Maßnahmen** aufzunehmen sind, enthält der G10-Entwurf im Gesetzestext nur die Vorgabe, dass in den **jährlichen Bericht** an den Deutschen Bundestag über die Durchführung der G10-Maßnahmen auch deren **Art und Umfang** aufzunehmen sind. Die frühere Fassung der Begründung lautete auf meinen Vorschlag hin noch: *„Um eine effektive parlamentarische Kontrolle dieser mit intensiven Grundrechtseingriffen verbundenen Maßnahmen zu gewährleisten, sind in den Bericht Anlass, Umfang, Dauer, Ergebnis und Kosten der Maßnahmen aufzunehmen“*. Diese Formulierung enthielt damit in Anlehnung an § 100e StPO die Voraussetzungen der von mir immer wieder geforderten Evaluierung. Die Bundesregierung ist der Auffassung, der öffentliche Bericht an den Deutschen Bundestag dürfe aus Gründen des § 5 Abs. 1 des PKG-Gesetzes, d. h. aus Geheimhaltungsgründen, nicht alle diese Angaben enthalten. Sie ist mit mir allerdings – dies ist nunmehr der Begründung zum Gesetzentwurf zu entnehmen – der übereinstimmenden Auffassung, dass es in erster Linie auf die zugrundeliegenden Berichte des BMI an das Parlamentarische Kontrollgremium ankommt:

Diese Institution ist die kompetente Stelle, die auf der Grundlage der halbjährlichen Berichte des BMI, die die o. a. Aussagen hinsichtlich der G10-Maßnahmen enthalten müssen, im Hinblick auf die verfassungsmäßigen Kriterien der Erforderlichkeit und Verhältnismäßigkeit eine effiziente Evaluierung durchführen müsste. Erkenntnisse der G10-Kommission aus ihrer Kontrolltätigkeit sollten gegebenenfalls in die Überprüfung einbezogen werden. Das Parlamentarische Kontrollgremium müsste im Ergebnis die Frage beantworten, ob die Erwartungen des Gesetzgebers an die Eignung der Maßnahmen und deren Verhältnismäßigkeit bestätigt werden. Dies erfordert als eine der Grundlagen für die Evaluierung eine Rechtstatsachensammlung, wie sie in Ansätzen beim BKA für Maßnahmen der polizeilichen und strafprozessualen Eingriffbefugnisse eingerichtet worden ist (auch wenn sich dort Probleme zeigen – s. o. Nr. 11.8). In die Auswertung könnten Fachleute aus Bund und Ländern, ebenso wie unabhängige Sachverständige einbezogen werden. Ergebnis müsste eine umfassende, ergebnisoffene und gegebenenfalls wissenschaftlich begleitete Erfolgskontrolle sein. Der darauf aufbauende, dem Deutschen Bundestag zu erstattende jährliche Bericht könnte, ohne Geheimhaltungsvorschriften zu verletzen, das Ergebnis dieser Erfolgskontrolle auch für die Öffentlichkeit zugänglich machen.

3. Wiedereinführung der 5-Jahresfrist:

   Die Benachrichtigung Betroffener über Beschränkungsmaßnahmen nach dem G10-Gesetz war 1987 aufgrund einer Entscheidung des Bundesverfassungsgerichts (BVerfGE 30,1 ff.) in das Gesetz aufgenommen worden. Die in § 5 Abs. 5 G10 geltende Ausschlussfrist – eine Benachrichtigung des Betroffenen konnte endgültig unterbleiben, wenn nach Ablauf von 5 Jahren nicht absehbar war, ob eine Benachrichtigung ohne Gefährdung des Zwecks der Maßnahme möglich war – ist mit dem Inkrafttreten des Verbrechensbekämpfungsgesetzes 1994 entfallen.

   Durch das Volkszählungsurteil von 1983 wurde die grundsätzliche Pflicht zur Unterrichtung des Betroffenen nach Wegfall der Zweckgefährdung für Informationseingriffe generell bestätigt. Mit der vorgesehenen Neuregelung würde die Rechtsposition des Betroffenen, d. h. auch seine Möglichkeit, gegen die Maßnahme Gegenvorstellungen zu erheben, verschlechtert bis hin zum Ausschluss rechtlicher Möglichkeiten. Denn nach der aktuellen Fassung des G10 steht dem Betroffenen nach Mitteilung über die erfolgte G10-Maßnahme der Rechtsweg offen. Würde die Mitteilungspflicht nach 5 Jahren entfallen, wäre ihm diese Möglichkeit aber genommen, auch wenn die Mitteilung ohne Gefährdung des Zweckes der Maßnahme möglich wäre. Ich halte es für verfrüht, nach so relativ kurzer Zeit nach Wegfall der Frist zu behaupten, die Änderung von Dezember 1994 habe sich nicht bewährt. Vom BMI vorgetragene praktische Erwägungen – Vorhaltung der Vorgänge auf unabsehbare Zeit – beeinträchtigen die Rechtsschutzgarantie des Art. 19 Abs. 4 GG m. E. doch unangemessen.

   Da die Bundesregierung an der geplanten Neuregelung grundsätzlich festhalten will, habe ich mich mit einer Alternativlösung einverstanden erklärt, die mir als ein datenschutzrechtlich tragbarer Kompromiss erscheint:

   Danach bedarf es einer Mitteilung an den Betroffenen nicht, wenn die G10-Kommission festgestellt hat, dass

   - eine Mitteilung an den Betroffenen den Zweck der Beschränkungsmaßnahme auch nach fünf Jahren noch gefährdet und
   - diese Gefährdung des Zwecks der Beschränkungsmaßnahme mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft besteht.

   Liegen die Voraussetzungen dafür vor, dass eine Benachrichtigung unterbleiben kann, gleichwohl aber die über den Betroffenen erhobenen Daten weder bei der erhebenden Stelle noch beim Empfänger weiterhin benötigt werden, sind diese tatsächlich zu löschen. Ich habe darauf gedrängt, dies in die Begründung des Gesetzentwurfs aufzunehmen. In Anbetracht der auch mit diesem Kompromiss verbundenen Beeinträchtigungen der Rechtsschutzgarantie halte ich die Wiedereinführung der 5-Jahresfrist jedoch nach wie vor für problematisch.

4. Erweiterung des Straftatenkatalogs auf Einzeltäter und lose Gruppierungen:

   § 2 Abs. 1 Satz 1 Nr. 6 G10-Gesetz in der derzeit geltenden Fassung wurde 1978 als Spezialtatbestand und Auffangklausel für die Bekämpfung des Terrorismus in das G10-Gesetz eingefügt. Schon im Gesetzgebungsverfahren zum Verbrechensbekämpfungsgesetz 1994 hatte das BfV gefordert, Einzeltäter, die weder einer terroristischen Vereinigung angehören noch in deren Namen eine Straftat begehen, nach dem G10 überwachen zu dürfen.

   Diese anlässlich einer Anhörung vom BfV erhobene Forderung nach Erweiterung des Straftatenkatalogs auf Einzeltäter und lose Gruppierungen auch ohne Vorliegen einer terroristischen Vereinigung wurde in den Gesetzentwurf aufgenommen. Dies erfolgte allerdings mit der Einschränkung, dass die von extremistischen Einzeltätern oder losen Gruppierungen geplanten bzw. begangenen Straftaten, wie Mord und Totschlag, erpresserischer Menschenraub, Geiselnahme, Brandanschläge, gefährliche Eingriffe in den Bahnverkehr, sich gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes richten müssen.

   Diese Erweiterung im G10-Gesetz ist auch nach Auffassung der Datenschutzbeauftragten der Länder ein gravierender Eingriff in das Grundrecht nach Art. 10 GG. Damit soll ermöglicht werden, sowohl im Vorfeld, d. h. in der Planungsphase, als auch zum Zeitpunkt der Begehung der aufgeführten Straftaten und nach deren Durchführung mit den in § 1 G10 genannten Maßnahmen gegen einen Einzeltäter oder eine lose Gruppierung durch den Verfassungsschutz vorzugehen. Darüber hinaus wird das Trennungsgebot nach Art 87 Abs. 1 Satz 2 GG berührt, das sicherstellen soll, dass die Koppelung geheimdienstlicher Informationsmacht und polizeilicher Exekutivbefugnisse verhindert wird, um die Freiheitssphäre der Bürger nicht unverhältnismäßig zu beeinträchtigen. Verdeckte Ermittlungen von der Einsatzschwelle eines konkreten Anfangsverdachts zu lösen und – nach nachrichtendienstlicher Art – schon im Vorfeld zur Verdachtsgewinnung durchzuführen, würde die Gefahr unverhältnismäßig ausweiten, dass auch gegen Unbescholtene strafrechtlich ermittelt werden könnte (s. 15. TB Nr. 28.1). Neben diesen Bedenken habe ich die Frage nach dem Realitätsbezug des Vorhabens gestellt. Die Bundesregierung hat daraufhin zur Untermauerung der Erforderlichkeit dieser Gesetzesänderung eine Reihe von Rechtstatsachen in die Begründung des Entwurfs aufgenommen. Aber auch die dort genannten Gründe vermögen mich nicht davon zu überzeugen, dass die Erweiterung des Straftatenkatalogs vor allem auf Einzeltäter notwendig ist.

   Mit Rücksicht auf die Tatsache, dass im Berichtszeitraum die Extremismusgefahr weiter anstieg und ihr in erster Linie mit staatlichen Mitteln begegnet werden muss, habe ich vorgeschlagen, die geplante Erweiterung zumindest zu befristen und einer Erfolgskontrolle zu unterziehen. Mit dem ersten Teil des Vorschlages hat sich die Bundesregierung nicht einverstanden erklärt, obwohl solche Befristungen bei Eingriffen in Art. 10 GG bereits festgelegt wurden:

   Die mit dem 7. Gesetz zur Änderung des Außenwirtschaftsgesetzes vom 28. Februar 1992 (BGBl. I S. 273) eingeführte Ermächtigung an das Zollkriminalamt, zur Verhinderung schwerwiegender Kriegswaffen- und Ausfuhrdelikte das Brief-, Post- und Fernmeldegeheimnis einzuschränken (§§ 39 bis 43 AWG), wurde vom Gesetzgeber wegen der mit solchen Beschränkungen verbundenen Eingriffe in das Grundrecht des Art. 10 GG und der erforderlichen Erprobung solcher Maßnahmen auf ihre Wirksamkeit seinerzeit nur befristet in das AWG aufgenommen. Die Befristung wurde mehrmals verlängert und fiel erst nach einer Erfolgskontrolle weg, nachdem feststand, dass diese Überwachung des Brief-, Post- und Fernmeldeverkehrs durch das Zollkriminalamt ein wirksames Instrument zur Verhinderung und Aufdeckung von Außenwirtschaftsstraftaten ist.

   Mein Vorschlag sah auch vor, dass die Bundesregierung dem Parlament nach Ende der Befristung einen aussagefähigen Bericht vorlegen müsste, damit es qualifiziert über den Fortbestand der Regelung oder ihre Aussetzung entscheiden kann. Der Bericht sollte daher aussagekräftige Angaben zur Beurteilung der Eingriffsdimension enthalten, um Freiheitseinbußen gegen Gemeinnutzen abwägen und Entwicklungstendenzen erkennen zu können.

Abschließend ist hervorzuheben, dass im Entwurf Vorgaben des Bundesverfassungsgerichts betreffend den BND und die strategische Kontrolle im Hinblick auf Prüf-, Kennzeichnungs- und Löschungspflichten, Übermittlungsvorschriften und die Zweckbindung auch für Individualanordnungen nach § 2 G10 vorgesehen sind.

Das Gesetzgebungsvorhaben werde ich auch im Parlament weiterhin kritisch begleiten.

16.2 Kontrollen beim BND

16.2.1 Bessere Zusammenarbeit bei der Erstellung von Dateianordnungen

Meine frühere Kritik (s. 17. TB Nr. 16.1), der BND habe seine Verpflichtung zur Erstellung von Dateianordnungen für seine automatisierten Dateien mit personenbezogenen Daten nach § 6 BNDG i. V. m. § 14 BVerfSchG unter meiner Beteiligung vor deren Erlass nicht erfüllt, hat zu einer erfreulichen Entwicklung geführt. Im Berichtszeitraum ist der BND dazu übergegangen, mich schon zu einem relativ frühen Zeitpunkt bei der Erarbeitung von Dateianordnungen zu beteiligen. Hierdurch erhalte ich – auch zum Vorteil des BND – Gelegenheit, in der Entstehungsphase von Dateianordnungen beratend mitzuwirken. Inzwischen sind eine Reihe von Dateianordnungen unter meiner Beteiligung in Kraft gesetzt worden. Wie sich bei meinen beiden letzten Kontroll- und Informationsbesuchen beim BND gezeigt hat, waren in diesem Zusam-

menhang gut vorbereitete Präsentationen von DV-Vorhaben hilfreich. Die dadurch erzielte Transparenz erleichterte mir deren datenschutzrechtliche Beurteilung und Begleitung.

16.2.2 Erneut große Altdatenbestände entdeckt

In meinem 16. TB (Nr. 16.2 letzter Absatz) hatte ich über die Zusage des BND berichtet, seine Altdatenbestände bis Ende 1997 endgültig zu bereinigen. Diese Bereinigung alter, nicht (mehr) erforderlicher bzw. auch sonst nicht mehr zulässiger Datenspeicherungen hätte bis spätestens fünf Jahre nach Inkrafttreten des neuen BND-Gesetzes vom 20. Dezember 1990 abgeschlossen sein müssen, da das BNDG – wie das BVerfSchG – vorschreibt, dass personenbezogene Daten bei jeder Einzelfallbearbeitung, spätestens aber nach fünf Jahren, auf ihre Richtigkeit und Erforderlichkeit hin zu überprüfen sind (§ 5 BNDG i.V.m. § 12 BVerfSchG).

Der BND hat mir zwar im Februar 1998 (s. 17. TB Nr. 16.1) auf mein mehrmaliges Drängen mitgeteilt, dass die Datenbereinigung in seiner zentralen Datei abgeschlossen sei. Bei meinen letzten beiden Kontrollen habe ich aber festgestellt, dass bei einer Reihe von anderen Datensammlungen die gesetzlich vorgeschriebene Überprüfung und Bereinigung bisher weitgehend unterblieben ist. Der BND führte hierfür fehlende Personalkapazitäten an; er habe aus diesem Grund eine andere Prioritätenwahl vornehmen müssen.

Auch wenn ich nicht verkenne, dass – wie fast überall im öffentlichen Dienst des Bundes – Personaleinsparungen bei nicht geringer werdenden Aufgabenstellungen zu Engpässen bei der Durchführung obliegender Verpflichtungen führen können, bedarf es dennoch organisatorischer Überlegungen und Anstrengungen, wie die Akten- und Datenbereinigung – und sei es auch über einen aus diesen Gründen längeren Zeitraum – prioritär erfolgen soll. Der BND hätte mich vor allem schon zu früherer Zeit über noch ausstehende Datenbereinigungen in einer Reihe von Bereichsdokumentationen unterrichten sollen. Ich hoffe, dass, wie bei der Bereinigung der zentralen Datei, die Altdatenbereinigung auch in den anderen Fällen nun schnellstmöglich abgeschlossen wird.

16.2.3 Probleme beim Verfahren zur Sicherheitsanfrage weitgehend gelöst

Zur Sicherheit eines Nachrichtendienstes gehört es, dass er sich vor dem Hintergrund langjähriger Erfahrungen Instrumente mit dem Ziel schafft, im gesetzlichen Rahmen eine sicherheitliche oder geheimdienstliche Gefährdung seines gesamten Umfelds soweit wie möglich auszuschalten. In meinem 17. TB (Nr. 16.5) hatte ich dargelegt, dass das hierzu u. a. angewandte Verfahren der Sicherheitsanfrage, mit dem der BND zu seinem Schutz und dem seiner Mitarbeiter, Einrichtungen und Quellen zusätzliche Überprüfungen personenbezogener Daten anderer Personen vornimmt, z. B. derjenigen, die Zugang zu Dienstobjekten erhalten sollen wie Lieferanten oder Handwerker, dringend einer Neuregelung bedurfte.

Im 17. TB (Nr. 16.2) hatte ich auch ausgeführt, dass Datenerhebungen über den vom SÜG vorgesehenen Rahmen hinaus nur dann auf die Regelungen des BNDG gestützt werden dürfen, wenn tatsächliche Anhaltspunkte für eine konkrete Gefahr sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten gegen den BND bestehen. Der BND hingegen möchte eine sog. nachrichtendienstliche Gefährdung ausreichen lassen, wenn es nach nachrichtendienstlichem Erfahrungswissen die Situation einmal gegeben habe, dass z. B. ein gegnerischer Nachrichtendienst über den entsprechenden Personenkreis an BND-Mitarbeiter heranzukommen versucht hat. Nach eingehender Diskussion mit dem BK und dem BND habe ich meine Auffassung dahingehend geändert, dass ich die Anwendbarkeit des BNDG für zulässig erachte, wenn zumindest eine gewisse zusätzliche Gefährdung des Nachrichtendienstes vorliegt. Eine sicherheitliche Überprüfung im Rahmen des Verfahrens der Sicherheitsanfrage etwa eines außenstehenden Dritten, der durch eine Vertretung in persönlichen Angelegenheiten eines BND-Mitarbeiters einen näheren Einblick in dessen Privatsphäre erhält und von dem der BND weiß, dass er einen früheren nachrichtendienstlichen Hintergrund hat, beispielsweise Verdacht auf Mitarbeit bei einem gegnerischen Nachrichtendienst, ist demgemäss noch hinnehmbar.

Schon die mir Mitte 1999 übermittelte Entwurfsfassung der Verfügung zum Verfahren zur Sicherheitsanfrage erhielt im Vergleich zu der Fassung, die Gegenstand meiner Überprüfung im Jahr 1997 war, eine Reihe von datenschutzrechtlichen Verbesserungen. Dabei war vor allem unter dem Gesichtspunkt der Kriterien der Erforderlichkeit und Verhältnismäßigkeit der Kreis der zu überprüfenden Personen erheblich verkleinert worden. Nach weiteren Gesprächen mit dem BND seit Herbst 1999 wurde inzwischen ein Ergebnis erzielt, das meine datenschutzrechtlichen Forderungen weitgehend berücksichtigt. Allerdings dränge ich weiterhin darauf, dass bestimmte Berufsgruppen nicht pauschal in der Verfügung aufgelistet werden.

16.3 ENFOPOL – EU-Entschließung zur Überwachung des Fernmeldeverkehrs –

Als „Gespenst, das durch das Internet geistert“, geriet Anfang 1999, unter deutscher EU-Präsidentschaft, der Entwurf einer Ratsentschließung zur rechtmäßigen Überwachung der Telekommunikation und der Internet-Nutzung in die Medien. Das **ENFOPOL 19** genannte Dokument war das Ergebnis von Beratungen der EU-Ratsgruppe „Polizeiliche Zusammenarbeit“ im Bereich Überwachung des Telekommunikationsverkehrs. Von der Bundesregierung als zwingende Anpassung an die Entschließung des Rates der Europäischen Union vom 17. Januar 1995 über die rechtmäßige Überwachung des Fernmeldeverkehrs (ABl. 1996 Nr. C 329,1) gesehen und nach Auffassung der Verfasser erforderlich geworden durch innovative Techniken auf dem Telekommunikationssektor, wie Satelliten- und Individualkommunikation über das Internet (E-Mail), sahen die Kritiker in der Tagespresse, in Fachzeitschriften

und im Internet die Gefahr neuer Eingriffe in das Grundrecht auf unbeobachtete Kommunikation und das Fernmeldegeheimnis. Es gab sogar Vermutungen, die EU plane ein System zur totalen Überwachung jeglicher Art von Telekommunikation, das Grundrechte außer Kraft setzt, Prinzipien der Rechtsstaatlichkeit verletzt und der Telekommunikationsindustrie immense zusätzliche Kosten aufbürdet.

Der Entwurf einer Ratsentschließung mit der Dokumentenbezeichnung ENFOPOL 19 schreibt die Ratsentschließung vom 17. Januar 1995 fort, indem technische Anforderungen an die Betreiber von Telekommunikationsdiensten gestellt werden. Die Pflicht der Betreiber, notwendige technische Vorkehrungen zu treffen, um Überwachungsmaßnahmen zu ermöglichen, ergibt sich jedoch aus dem Recht der einzelnen Mitgliedstaaten. In Deutschland sind dies die Strafprozessordnung, das Außenwirtschaftsgesetz und das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses – Gesetz zu Artikel 10 GG. Diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen, müssen die berechtigten Stellen, z. B. Strafverfolgungsbehörden, durch rechtlich definierte Vorkehrungen in die Lage versetzen, die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen, also Schnittstellen bereit halten.

Auch die Datenschutzbeauftragten des Bundes und der Länder betonten die datenschutzrechtliche Bedeutung des Entwurfs der Ratsentschließung, ungeachtet der Tatsache, dass der Rechtsakt im Falle seiner Annahme für die Mitgliedstaaten nicht verbindlich ist. Nach derzeitigem Verhandlungsstand wird es sich um eine bloße Empfehlung handeln. Ihre Verabschiedung könnte jedoch zur Folge haben, dass die Bundesrepublik Deutschland ihre gesetzlichen Voraussetzungen zur Durchsetzung des Fernmeldegeheimnisses neu durchdenken muss.

Die Datenschutzbeauftragten haben auf ihrer 57. Konferenz am 25./26. März 1999 eine entsprechende Entschließung gefasst (s. **Anlage 11**), die ich dem BMI und dem BMJ im April 1999 mit der Bitte zugeleitet habe, die darin enthaltenen Aussagen in die Entscheidungen der Bundesregierung zum Entwurf der Ratsentschließung mit einzubeziehen und mich bei dem weiteren Verfahren rechtzeitig und umfassend zu beteiligen.

Die ursprünglich für Ende Mai 1999 im EU-Ministerrat vorgesehene Verabschiedung der Ratsentschließung ENFOPOL 19 ist bislang noch nicht erfolgt. Nach Aussage des BMI ist bisher noch von keiner der der deutschen ab 1. Juli 1999 nachfolgenden EU-Präsidentschaften die Initiative wieder aufgegriffen worden. Das BMI bekundet zwar Interesse an der Empfehlung, wird aber nach eigener Auskunft von sich aus nicht initiativ.

16.4 Abhörsystem ECHELON

In den Medien wurde im Berichtszeitraum immer wieder und ausführlich über die weltweiten Lauschaktivitäten, durchgeführt mit Hilfe des globalen Abhörnetzwerks **ECHELON** des amerikanischen Geheimdienstes NSA (National Security Agency), berichtet. Den Presseberichten zufolge wurde ECHELON entwickelt, um wichtige militärische Entscheidungen gegnerischer Staaten zu belauschen. Nach Expertenmeinung scannt die NSA seit Anfang der 80-er Jahre weltweit Telefonate, Faxe, Telexe und E-Mails, die über internationale Telekommunikationssatelliten, regionale Satelliten und Richtfunkverbindungen gesendet werden, ein. Computerprogramme sortieren nach Schlüsselbegriffen aus der Fülle der zwischengespeicherten Daten Begriffe, Namen oder Nummern aus, die für die NSA, aber auch für andere staatliche Stellen wie Polizeibehörden von Bedeutung sein können. Für dieses gigantische Netzwerk, an dem auch Großbritannien, Kanada, Australien und Neuseeland partizipieren, sollen allein bei der NSA weltweit mindestens 40 000 Mitarbeiter im Auftrag ihrer Regierung tätig sein und die Kommunikation Dritter belauschen und auswerten. Über 100 satellitengestützte Stationen in aller Welt, eine davon im bayerischen Bad Aibling, sollen ECHELON rund um die Uhr unterstützen. Damit wäre nicht auszuschließen, dass auch Bundesbürger, inländische Unternehmen oder öffentliche Stellen überwacht werden.

Die Bundesregierung hat allerdings in ihrer Antwort vom 17. April 2000 – Bundestagsdrucksache 14/3224 – auf eine Kleine Anfrage erklärt, ihr lägen *„keine Erkenntnisse über eine Gefährdung der Privatsphäre der Bürgerinnen und Bürger sowie der Wettbewerbsfähigkeit der deutschen Wirtschaft durch ECHELON vor“*. Die amerikanische Station in Bad Aibling werde nach ihrer Ansicht *„zur Erfassung militärischer Hochfrequenz- und Satellitenverkehre“* betrieben, die für die außen- und sicherheitspolitische Lage der Vereinigten Staaten von Amerika sowie ihrer europäischen Partner von Relevanz seien. Die Erkenntnisse würden auch dem BND zur Verfügung gestellt. Sie führt weiter aus: *„Die von der Station Bad Aibling ausgehende Aufklärung ist demnach grundsätzlich nicht auf private Telekommunikationsverkehre ausgerichtet. Die Arbeit der Station erfolgt auf der Grundlage des NATO-Truppenstatuts. Darin ist berücksichtigt, dass ein missbräuchliches Vorgehen gegen die Bundesrepublik Deutschland nicht stattfindet. Ein solcher Einsatz wäre daher unzulässig. Von amerikanischer Seite ist mehrfach versichert worden, dass von Bad Aibling keine gegen die Interessen der Bundesrepublik Deutschland gerichteten Aktivitäten ausgehen. Die Bundesregierung hat keinen Anlass, an diesen Versicherungen zu zweifeln.“*

Unter dem Schlagwort **Wirtschaftsspionage gegen die EU** beschäftigen die Aktivitäten der Lauscher inzwischen auch Gremien der EU. Beweise für eine Schädigung europäischer Firmen durch Wirtschaftsspionage mit Hilfe von ECHELON konnten zwar bisher nicht erbracht werden. Dennoch wird seitens der EU trotz Dementis aus den USA geargwöhnt, die ECHELON-Betreiber verletzten mit den Abhöraktionen europäische Rechtspositionen, wenn ihre Abhöraktionen zu möglichen Wettbewerbsnachteilen von europäischen Unternehmen führten.

Anstelle eines Untersuchungsausschusses – dieser wurde mit 350 gegen 200 Stimmen im Europäischen Parlament abgelehnt – wurde im Juli 2000 ein nicht ständiger Aus-

schuss mit 36 Mitgliedern eingerichtet. Seine Aufgabe ist es, zu prüfen und binnen Jahresfrist einen Bericht darüber abzugeben, inwieweit ein solches Abhörsystem mit EU-Recht vereinbar ist, welche Möglichkeiten die EU gegen einen Missbrauch – Wirtschaftsspionage und Verletzung der Privatsphäre der EU-Bürger – hat und welche politischen und gesetzgeberischen Initiativen gegebenenfalls zu treffen sind.

Die von Fakten und Behauptungen auf der einen, Dementis und Schweigen auf der anderen Seite bestimmte Szenerie kann in der Öffentlichkeit den Eindruck erwecken, mit ECHELON werde in elementare Persönlichkeitsrechte von Bürgern eingegriffen; das könnte durch Information und Transparenz vermieden werden. Es stellt sich dringend die Frage nach der Legitimität dieses Systems. Erster wichtiger Schritt bei dieser Prüfung ist eine objektive Bestandsaufnahme, die an die Stelle von Spekulationen, Mutmaßungen und Widersprüchen gesicherte Fakten setzt. Auf dieser Grundlage ist die Frage nach klaren gesetzlichen Regelungen für nachrichtendienstliche Lauschaktionen auf europäischer Ebene zu stellen. Vorbild hierfür könnte das deutsche Recht sein.

Die Gefahren, die nach den mir vorliegenden Erkenntnissen ein solches Abhörsystem in sich birgt, habe ich auf der 22. Internationalen Datenschutzkonferenz im September 2000 in Venedig (s. auch Nr. 32.4) problematisiert und eine Diskussion darüber angeregt, wie festgelegt werden kann, was Nachrichtendienste dürfen und mit welchen Mitteln sie welche Informationen und zu welchen Zwecken erheben und verarbeiten dürfen.

17 Sicherheitsüberprüfung

17.1 Erfreulich hoher Datenschutzstandard bei Sicherheitsüberprüfungen in der Privatwirtschaft

Mit dem Sicherheitsüberprüfungsgesetz (SÜG) vom 20. April 1994 ist mir die Zuständigkeit für die Kontrolle von Unternehmen der Privatwirtschaft übertragen worden, die rüstungsrelevante Aufträge erhalten und für die die Beschäftigten den Zugang zu sicherheitsempfindlichen Bereichen sowie zu Verschlusssachen benötigen und deshalb einer Sicherheitsüberprüfung zu unterziehen sind. Dabei habe ich bereits in den vergangenen Jahren einen hohen datenschutzrechtlichen Standard festgestellt. Im Jahre 2000 habe ich ein größeres Unternehmen kontrolliert, das aufgrund der Entwicklung militärischer Systeme der Hochtechnologie eine relativ große Zahl von sicherheitsüberprüften Mitarbeitern beschäftigt. Dabei hat sich der hohe datenschutzrechtliche Standard bestätigt.

Die betroffenen Mitarbeiter dieses Unternehmens sind überwiegend nach Ü 2 (erweiterte Sicherheitsüberprüfung), lediglich einige wenige Mitarbeiter – der Sicherheitsbevollmächtigte, sein Vertreter und der Leiter der Patentabteilung – sind nach Ü 3 (erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen) überprüft.

Für den Konzern ist ein Sicherheitsbevollmächtigter bestellt, der insgesamt sieben Zweigunternehmen betreut. Ich habe gegen die Geheimschutzbetreuung für mehrere Zweigunternehmen durch einen Sicherheitsbevollmächtigten dann keine Bedenken, wenn in entsprechenden Zusatzerklärungen zu den Arbeitsverträgen des Sicherheitsbevollmächtigten und der sonstigen mit Aufgaben des personellen Geheimschutzes betrauten Mitarbeiter aufgenommen wird, dass die bei der Tätigkeit für das verbundene Unternehmen sich ergebende Zweckbindung der Daten zu beachten und eine Übermittlung personenbezogener Daten zwischen dem Mutter- und dem Tochterunternehmen wie eine Datenübermittlung an Dritte zu behandeln ist. Leider lagen bei der Kontrolle keine entsprechenden Zusatzerklärungen für den Sicherheitsbevollmächtigten, seinen Stellvertreter und die mit Aufgaben des Geheimschutzes betraute Sachbearbeiterin vor. Das BMWi, das nach § 25 SÜG zuständige Stelle ist, hat zugesagt, das kontrollierte Unternehmen um Vorlage dieser Zusatzerklärungen zu bitten.

Ferner habe ich festgestellt, dass sich in den Sicherheitsakten zum Teil auch noch Sicherheitserklärungen befinden, die nach den Sicherheitsrichtlinien von 1960, 1971 bzw. 1988 abgegeben worden waren. Diese alten Sicherheitserklärungen sollten aus den Akten entfernt sein, da sie zum Teil Angaben enthalten, die nach dem SÜG von 1994 nicht mehr erforderlich und heute für eine sicherheitsmäßige Bewertung nicht mehr relevant sind. Das BMWi hat hierzu erklärt, dass es alle betroffenen Unternehmen darauf hinweisen wird, dass nur noch die aktuellen Erklärungen zur Sicherheitsüberprüfung aufzubewahren sind. Ich habe allerdings zusätzlich gefordert, die Unternehmen zu verpflichten, bei jeder Einzelfallbearbeitung die Sicherheitsakten danach durchzusehen, ob noch alte Sicherheitserklärungen vorhanden sind und diese aus den Akten zu entfernen.

In einigen Fällen habe ich festgestellt, dass der Sicherheitsbevollmächtigte Angaben des Betroffenen in der Sicherheitserklärung geändert oder auch gestrichen hat. Dies habe ich gerügt, wobei sich das BMWi meiner Auffassung angeschlossen hat. Denn für den Fall, dass der Sicherheitsbevollmächtigte nach Erörterung mit dem Betroffenen über sicherheitsrelevante Sachverhalte in der Sicherheitserklärung zu dem Ergebnis kommt, dass Angaben in dieser doch nicht sicherheitsrelevant sind, ist sie durch den Betroffenen selbst und nicht durch den Sicherheitsbevollmächtigten zu ändern. Darauf wird das BMWi das betroffene Unternehmen hinweisen.

Die mit Aufgaben des personellen Geheimschutzes betraute Sachbearbeiterin ist gleichzeitig Mitglied des Betriebsrates des Unternehmens. Nach § 25 Abs. 1 Satz 1 SÜG sind die Aufgaben der nicht-öffentlichen Stelle bei der Durchführung von Sicherheitsüberprüfungen grundsätzlich durch eine von der Personalverwaltung getrennten Organisationseinheit wahrzunehmen. Diese Bestimmung soll die Betroffenen davor schützen, dass Erkenntnisse aus der Sicherheitsüberprüfung in unzulässiger

Weise auch für Zwecke der Personalverwaltung genutzt werden. Dieser Grundsatz verbietet es auch, dass der Geheimschutzbevollmächtigte oder seine Mitarbeiter in Personalvertretungsgremien tätig sind. Auch hier stimmt das BMWi meiner Auffassung zu und wird das betroffene Unternehmen veranlassen, dass die für den personellen Geheimschutz tätige Mitarbeiterin ihre Betriebsratstätigkeit oder ihre Tätigkeit im personellen Geheimschutz aufgibt.

17.2 Sicherheitsüberprüfung beim BND

Der BND führt nach dem SÜG für Mitarbeiter und Bewerber die Sicherheitsüberprüfungen selbst durch. Er ist damit zugleich zuständige Behörde und mitwirkende Stelle im Sinne des SÜG. Zur Durchführung der Sicherheitsüberprüfungen führt der BND eine Datei, zu deren Errichtung ich nach § 6 BNDG i.V.m. § 14 BVerfSchG – wenn auch spät – angehört wurde. Denn diese Datei wird bereits seit 1977 betrieben, während mir der Entwurf der Dateianordnung erst im Jahre 1999 zur Anhörung übermittelt wurde.

In der Datei werden Daten gespeichert, die sowohl nach dem SÜG als auch nach dem BNDG für Zwecke der Eigensicherung erhoben werden. Es handelt sich um eine Datei i.S. des § 20 SÜG. Diese Vorschrift regelt abschließend, welche Daten im Rahmen einer Sicherheitsüberprüfung in Dateien gespeichert werden dürfen.

Die in dieser Datei gespeicherten Daten überschreiten den nach § 20 SÜG erlaubten Umfang bei weitem. Der BND argumentiert, dass es sich bei dieser Datei um ein *„Mischsystem“* handelt, in dem personenbezogene Daten nach unterschiedlichen Rechtsgrundlagen gespeichert werden. Personenbezogene Daten für Zwecke der Sicherheitsüberprüfung würden ausschließlich in dem nach § 20 SÜG erlaubten Umfang gespeichert, während die anlässlich der Sicherheitsüberprüfungen zusätzlich erhobenen Daten ihre Rechtsgrundlage im BNDG fänden. Eine Zusammenfassung dieser nach unterschiedlichen Rechtsgrundlagen erhobenen Daten in einer Datei sei zur Bewertung der Gesamtsicherheitslage der Mitarbeiter des BND erforderlich, da die gespeicherten Informationen in der Gesamtschau ein Sicherheitslagebild zu den Mitarbeitern ermögliche, das der BND für Zwecke der Eigensicherung nach § 2 Abs. 1 BNDG benötige.

Ungeachtet der weiterhin bestehenden unterschiedlichen Auffassungen zur rechtlichen Einordnung dieser Datei habe ich im Rahmen einer Kontrolle folgende Feststellungen getroffen:

- Bereits bei früheren Kontrollen ist mir aufgefallen, dass in dieser Datei Abschlussberichte der Sicherheitsüberprüfungen vollständig als recherchefähiger Text abgespeichert werden. Nachdem ich dieses Verfahren kritisiert hatte, sagte der BND zu, künftig nur noch die Schlussbewertung der Abschlussberichte zu speichern und die seit Inkrafttreten des SÜG im Jahre 1994 gespeicherten Schlussberichte bis Ende 1999 zu berichtigen. Die Kontrolle hat jedoch gezeigt, dass der BND seit 1998 zwar nur noch die Bewertung und Entscheidung zum Abschlussbericht speichert. Die weiterhin in voller Länge abgespeicherten Abschlussberichte sind bisher jedoch weitgehend noch nicht berichtigt worden. Dies führt der BND auf fehlende Personalkapazitäten zurück (s. o. hierzu Nr. 16.2.2). Die Berichtigungen sollen nunmehr dennoch bis Jahresmitte 2001 abgeschlossen werden.

- Auf den Bestand dieser Datei haben auch Mitarbeiter aus dem Bereich Personaleinsatz – wenn auch eingeschränkt – lesenden Zugriff. Ich halte einen Zugriff der Personalverwaltung auf diese Daten nicht für zulässig, da nach dem SÜG die Aufgaben bei der Durchführung der Sicherheitsüberprüfung grundsätzlich durch eine von der Personalverwaltung getrennte Organisationseinheit wahrzunehmen sind. Aus diesem wesentlichen Grundsatz folgt, dass der Personalverwaltung ein Zugriff auf Daten, die für Zwecke der Sicherheitsüberprüfung erhoben werden, verwehrt bleiben muss. Aufgrund meiner Bedenken hat der BND inzwischen, nach Klärung der technischen Realisierbarkeit, den Zugriff auf diese Daten gesperrt.

- In die Datei werden auch einzelne Daten aus der Personaldatei überspielt. Zu diesen Daten gehört auch die Religionszugehörigkeit der Mitarbeiter des BND. Ergebnis meiner Prüfung war, dass diese Speicherung auch nach Auffassung des BND sicherheitlich nicht erforderlich ist und daher unterbleiben muss. Da die Angaben zur Religionszugehörigkeit automatisch aus der Personaldatei überspielt werden, ist nach Aussage des BND zur Unterdrückung der Übermittlung eine Programmänderung erforderlich. Der BND hat zugesagt, das Problem bei der Erstellung des neuen Programms entsprechend zu berücksichtigen. Da dies noch einige Zeit in Anspruch nehmen wird, hat er den Lesezugriff auf das Datenfeld gesperrt.

- Der BND hat durch organisatorische und personelle Maßnahmen sicherzustellen, dass die Weiterspeicherung, Berichtigung oder Sperrung der gespeicherten Datensätze rechtzeitig nach Ablauf der in § 5 BNDG i. V. m. den §§ 12 und 13 BVerfSchG geregelten Fristen überprüft wird. Zu diesem Zweck wird in der Datei ein Wiedervorlagedatum verfügt, zu dem die Daten zur Überprüfung anstehen. Sofern die Voraussetzungen für eine Weiterspeicherung erfüllt sind, wird das Wiedervorlagedatum aktualisiert, ansonsten wird der Datensatz gelöscht. Neben der Überprüfung spätestens nach fünf Jahren regelt der Entwurf der Dateianordnung, dass die Überprüfung der Datensätze bei jeder Bearbeitung eines Vorgangs stattfindet. Die Kontrolle hierzu hat ergeben, dass die vorgefundenen Mängel – die überprüften Datensätze enthielten häufig kein Wiedervorlagedatum – auf Bearbeitungsfehler zurückzuführen sind, die inzwischen korrigiert und abgestellt wurden.

- Das Verfahren der Ab- bzw. Übergabe von Akten an das Bereichsarchiv ist nicht schriftlich geregelt. Es besteht jedoch eine Anweisung, die Akten vorher *„zu bereinigen“*. Der BND hat eingeräumt, dass eine Aktenbereinigung im Bereichsarchiv nicht in erforderlichem Umfang erfolgt ist, obwohl mir dies schon vor Jahren

zugesagt wurde. Auch hierfür seien in erster Linie Kapazitätsprobleme ausschlaggebend. Er hat mir versichert, die Bereinigung der Datenbestände zu ausgeschiedenen Mitarbeitern „verstärkt“ bei der laufenden Vorgangsbearbeitung im Bereichsarchiv durchzuführen und hierfür Personal bereitzustellen. Beim jetzigen Personalbestand wäre das Vorhaben auf Jahre hinaus nicht abzuschließen.

Die mir nach Redaktionsschluss zugegangene Stellungnahme zu meinem Kontrollbericht habe ich berücksichtigt. Über weitere Feststellungen kann hier aus Gründen der Geheimhaltung nicht berichtet werden.

18 Personalwesen

18.1 Arbeitnehmerdatenschutzgesetz

Zuletzt in meinem 17. TB habe ich unter Nr. 18.1.2 darauf hingewiesen, dass die Schaffung eines bereichsspezifischen Arbeitnehmerdatenschutzgesetzes dringlicher denn je ist.

Wegen fehlender gesetzlicher Regelungen zum Arbeitnehmerdatenschutz sind Arbeitnehmer und Arbeitgeber bis heute im wesentlichen darauf angewiesen, sich an der einschlägigen Rechtsprechung zu orientieren. Die Klärung offener Fragen kann aber nicht den Gerichten überantwortet bleiben, da diese letztlich nur über einen Einzelfall und damit auch nur punktuell entscheiden können. Die Entwicklung der Informations- und Kommunikationsgesellschaft, die damit einhergehende zunehmende Technisierung der Arbeitswelt und die dadurch gewachsenen Möglichkeiten einer umfassenden Leistungs- und Verhaltenskontrolle werfen neue Fragen auf. Auch insoweit ist es dingend notwendig, Rechtsklarheit und Rechtssicherheit für alle Beteiligten zu schaffen. Ziel eines Arbeitnehmerdatenschutzgesetzes muss es sein, das sich aus den Persönlichkeitsrechten des Arbeitnehmers ergebende Recht auf informationelle Selbstbestimmung unter Abwägung mit dem berechtigten Informationsbedürfnis des Arbeitgebers möglichst umfassend und wirksam zu gewährleisten.

Ich begrüße es daher, dass die Bundesregierung neuerlich angekündigt hat, in dieser Legislaturperiode ein entsprechendes Gesetz vorzulegen, das auch die Entwicklung der Informations- und Kommunikationsgesellschaft arbeitsrechtlich flankiert. Dies sollte alsbald geschehen, weil mir immer häufiger Fragen zum Umgang mit Daten von Arbeitnehmern vor allem im Zusammenhang mit E-Mail- und Internet-Nutzung gestellt werden. Auch daher wäre es im Interesse aller Betroffenen, wenn der Gesetzentwurf noch in der laufenden Legislaturperiode beraten und verabschiedet wird.

18.2 Bundesdisziplinargesetz

Im Sommer 1999 hat mir das BMI den „Entwurf eines Gesetzes zur Neuordnung des Bundesdisziplinarrechts (BDiszNOG)“ zugeleitet. Kernbestandteil des BDiszNOG ist ein neues Bundesdisziplinargesetz (BDG), das die bisherige Bundesdisziplinarordnung (BDO) ersetzen soll. Aus datenschutzrechtlicher Sicht ist insbesondere die Umgestaltung der bisher in § 119 BDO enthaltenen Tilgungsregelungen für Disziplinarvorgänge (künftig § 16 BDG) hervorzuheben.

Zunächst wird die Tilgungsfrist für die mildeste Disziplinarmaßnahme, den Verweis, künftig zwei statt bisher drei Jahre betragen; die Tilgungsfrist bei einer Kürzung der Dienstbezüge wird von fünf auf drei Jahre verkürzt. In dem ursprünglichen Gesetzentwurf des BMI war noch vorgesehen, auch sämtliche Disziplinarvorgänge, die im Ergebnis nicht zu einer Disziplinarmaßnahme geführt haben, erst nach zwei Jahren aus der Personalakte zu entfernen. Hier konnte ich in Gesprächen mit dem BMI erreichen, dass in den Fällen, in denen ein Disziplinarverfahren mangels Nachweis eines Dienstvergehens eingestellt wird, der entsprechende Vorgang bereits nach drei Monaten zu entfernen ist.

Nach Ablauf der genannten Fristen tritt ein Verwertungsverbot ein, d. h. eine verhängte Disziplinarmaßnahme darf dann nicht mehr bei weiteren Disziplinarmaßnahmen und bei sonstigen Personalmaßnahmen berücksichtigt werden. Der Beamte soll aber künftig selbst entscheiden können, ob ein ihn betreffender Disziplinarvorgang nach Eintritt des Verwertungsverbots entfernt und vernichtet wird. Er kann beantragen, dass die Entfernung aus der Personalakte unterbleiben oder der Vorgang gesondert aufbewahrt werden soll. Die Dienststelle ist verpflichtet, dem Beamten die bevorstehende Entfernung mitzuteilen und ihn auf sein Antragsrecht und die Antragsfrist von einem Monat hinzuweisen. Unterbleibt auf den Antrag des Beamten hin die Entfernung oder erfolgt eine von der Personalakte gesonderte Aufbewahrung, ist das eingetretene Verwertungsverbot von der Dienststelle zu vermerken. Ich halte dieses Verfahren für besonders geeignet, das informationelle Selbstbestimmungsrecht des Beamten umfassend zu gewährleisten.

Bei einem weiteren Punkt sehe ich allerdings noch Handlungsbedarf. Nach § 90e Abs. 1 Nr. 2 des Bundesbeamtengesetzes (BBG) sind in der Personalakte befindliche Unterlagen über Beschwerden, Behauptungen und Bewertungen, falls sie für den Beamten ungünstig sind oder ihm nachteilig werden können, auf Antrag nach drei Jahren zu entfernen und zu vernichten. Unter diese Vorschrift fallen u. a. sogenannte „missbilligende Äußerungen“ – das sind Zurechtweisungen, Ermahnungen oder Rügen –, die keine Disziplinarmaßnahmen im Sinne des Disziplinarrechts darstellen und damit auch nicht den disziplinarrechtlichen Tilgungsfristen unterliegen. Während künftig die Disziplinarmaßnahme „Verweis“ – wie erwähnt – bereits nach zwei Jahren zu tilgen ist, wäre eine weniger einschneidende Maßnahme – die missbilligende Äußerung – nach § 90e Abs. 1 Nr. 2 BBG erst nach drei Jahren zu entfernen. Trotz meines Hinweises auf diesen Widerspruch sieht sich das BMI leider nicht in der Lage, im Rahmen des BDiszNOG auch § 90e Abs. 1 Nr. 2 BBG zu ändern und den neuen disziplinarrechtlichen Regelungen anzupassen. Ich werde diese Angelegenheit weiter verfolgen.

18.3 Personalaktenführung nach „Alter Väter Sitte“

Zahlreiche Eingaben zu Personalakten haben mich veranlasst, bei verschiedenen größeren Behörden der Bundesverwaltung Personalakten einzusehen. Mit dem Neunten Gesetz zur Änderung dienstrechtlicher Vorschriften, das nunmehr seit 8 Jahren in Kraft ist, wurden Form und Inhalt von Personalakten erstmals umfassend geregelt. Hierzu habe ich mich in meinem 15. TB ausführlich geäußert (Nr. 9.1.2 ff.). Für alle Personalakten (Grund-, Teil- und Nebenakten) gilt, dass sie nur Unterlagen enthalten dürfen, die den Mitarbeiter betreffen und mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten); andere Unterlagen dürfen in die Personalakte nicht aufgenommen werden (vgl. § 90 Abs. 1 Satz 2 BBG). Des weiteren darf für jeden Mitarbeiter nur eine Personalakte geführt werden, d. h. „geheime“ Personalakten sind verboten.

Der dem Personalaktenbegriff zugrundeliegende unmittelbare innere Zusammenhang zwischen dem Mitarbeiter und dem Dienstverhältnis erfordert eine generelle Umstellung aller Personalakten vom früher geltenden Vollständigkeits- zum Erforderlichkeitsprinzip. Personalakten, bei denen diese Umstellung als gelungen bezeichnet werden kann, konnte ich bei den kontrollierten Behörden nur vereinzelt vorfinden. Leider wurden die von mir eingesehenen Personalakten noch nach „alter Väter Sitte“ geführt, d. h. sie enthielten vollständig alle Unterlagen, die beim Dienstherren über den Mitarbeiter anfallen – unabhängig davon, ob sie den beruflichen Werdegang betreffen oder mehr sachlichen oder auch privaten Charakter haben.

Die nachfolgend beschriebenen Mängel bei der Personalaktenführung wurden bei der Bundesanstalt für Arbeit (BA), beim Bundesamt für die Anerkennung ausländischer Flüchtlinge, einem Hauptzollamt und einem Bundesvermögensamt festgestellt.

18.3.1 Grundakte

Viele Unterlagen, beispielsweise Lebensläufe, Schriftverkehr über die Beteiligung von Personalvertretungen, Übersichten über den persönlichen und beruflichen Werdegang, Anforderung von Beurteilungen, Beurteilungsbeiträge, Gesprächsvermerke, Kurzbriefe waren in den bei der Hauptstelle der BA geführten Personalakten bis zu 10-facher Ausfertigung in Grundakten vorzufinden.

Sowohl im Zusammenhang mit Beteiligungsverfahren der Personalvertretungen als auch in Vermerken, in denen Vorüberlegungen für mögliche Personalentscheidungen festgehalten wurden, sind häufig die Namen mehrerer Mitarbeiter genannt. Dies ist mit dem Personalaktengeheimnis (vgl. § 90 Abs. 3 BBG) nicht vereinbar; mit der Aufnahme dieser Unterlagen in die Personalakte nimmt z. B. der betroffene Mitarbeiter bei Einsichtnahme gleichzeitig Personalaktendaten seiner Kollegen zur Kenntnis. Auch Auszüge aus dem Bundeszentralregister, die nach Maßgabe des § 90e Abs. 2 BBG aus der Personalakte zu entfernen sind, waren noch in den meisten der eingesehenen Akten. Eine Paginierung war in den Grundakten nur teilweise, jedoch immer unvollständig vorzufinden. Teil- und Nebenakten waren überhaupt nicht paginiert. In großer Zahl vorgefundene Bewertungen ließen auch in Fällen, in denen diese ungünstig sind oder dem betroffenen Mitarbeiter nachteilig werden können, nicht erkennen, inwieweit eine Anhörung erfolgte. Äußerungen der Betroffenen zu den Wertungen (vgl. § 90b BBG) wurden jedenfalls in den Personalakten nicht vorgefunden.

Beurteilungsbeiträge oder vorbereitende Stellungnahmen sind, soweit sie nicht förmlich in die Beurteilung einfließen oder mit ihr eröffnet werden, nicht Bestandteil der Personalakte. Sie sind daher ebenso, wie der vorbereitende Schriftverkehr, nicht zur Personalakte zu nehmen. In den eingesehenen Grundakten fehlten auch das Inhaltsverzeichnis sowie das vollständige Verzeichnis aller Teil- und Nebenakten (vgl. § 90 Abs. 2 Satz 4 BBG), die einen Überblick über die insgesamt für jeden Mitarbeiter geführten Personalunterlagen erst ermöglichen.

18.3.1.1 Teilakten

Bei der Anlage von Teilakten ist auch zu beachten, dass sachliche Gesichtspunkte eine Trennung bestimmter Unterlagen von der Grundakte erforderlich machen müssen (vgl. § 90 Abs. 2 Satz 1 BBG). Dies ist beispielsweise der Fall bei der Erfüllung einer Aufgabe (z. B. Besoldung) durch eine andere Behörde, der Beihilfe und auch bei Vorgängen, die nach einer bestimmten Zeit wieder aus der Personalakte zu entfernen sind (z. B. Arbeitsunfähigkeitsbescheinigungen).

Die bei der BA in Teilakten „Bezüge“ vorgefundenen Kopien von Kassenanordnungen, Schriftverkehr zur „Verbeamtungsuntersuchung“, Laborarztrechnungen mit detaillierter Darstellung der Blutwerte des Betroffenen sowie Unterlagen über Beitragssätze von Ersatzkassen haben in der Bezügeakte nichts zu suchen.

In einer Personalteilakte für „Unterlagen von vorübergehender Bedeutung“ wurden zahlreiche Arbeits-/Dienstunfähigkeitsbescheinigungen vorgefunden, die acht bis zehn Jahre alt waren. Krankheitsblätter und Urlaubskarten, die als nicht-automatisierte Dateien ebenfalls als Personalteilakten anzusehen sind, enthielten die entsprechenden Nachweise vom Beginn des Beschäftigungsverhältnisses bis zum Kontrollzeitpunkt, obwohl sie spätestens fünf Jahre nach Ablauf zu vernichten sind (vgl. § 90f Abs. 2 Satz 1 BBG).

18.3.1.2 Nebenakten

Nebenakten dürfen nur geführt werden, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist oder wenn mehrere personalverwaltende Behörden für den Mitarbeiter zuständig sind; sie dürfen nur solche Unterlagen enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerfüllung der betreffenden Behörde erforderlich ist und die sich auch in der Grundakte oder in Teilakten befinden (§ 90 Abs. 2 Satz 3 BBG). Allgemeiner Schriftverkehr darf in Nebenakten grund-

sätzlich nicht abgelegt werden. Nebenakten sind zu vernichten, sobald sie nicht mehr benötigt werden (vgl. BT-Drs. 12/544 zu § 90 f Abs. 1 BBG, 3. Abs.).

In der Zentralregistratur der BA befinden sich ca. 50.000 Akten („Personalteilakte-N“) von Mitarbeitern, die nicht bei der Hauptstelle beschäftigt sind. Sie enthalten Vorgänge, die Mitarbeiter betreffen und in der Hauptstelle angefallen sind (z. B. allgemeiner Schriftverkehr). Darüber hinaus aber auch Unterlagen, die der Grundakte oder einer Teilakte zuzuordnen sind, wie Lebensläufe, Bewerbungsunterlagen p.p. Sie erfüllen weder die gesetzlichen Vorgaben von Teil- noch die von Nebenakten.

Auch die zahllos vorhandenen BA-internen Stellenausschreibungsakten enthalten Unterlagen mit Personalaktenqualität (Lebensläufe, Zeugnisse, Darstellungen zum beruflichen Werdegang usw.), obwohl die Stellenbesetzungen zum Teil seit Jahren abgeschlossen sind.

Die Personalaktenführung der BA habe ich insgesamt gem. § 25 BDSG wegen Verstoßes gegen zahlreiche gesetzliche Vorgaben der §§ 90 bis 90f BBG beanstandet. Die Verstöße wiegen um so schwerer, als eine Änderung der dargestellten Praxis zwar immer wieder zugesagt, jedoch nicht umgesetzt wurde (vgl. 16. TB Nrn. 18.10.2 und 18.10.3 und 17. TB Nr. 18.2.5).

18.3.1.3 Personalaktenrichtlinie

In meinem 17. TB (Nr. 18.2.5) hatte ich u. a. kritisiert, dass die BA ihre Personalakten immer noch nach internen Vorgaben aus dem Jahre 1989 führte, neue Regelungen, zwar immer wieder zugesagt, jedoch nicht erstellt wurden. Dieser Kritik ist die BA mit der Neufassung ihrer Personalaktenrichtlinien vom Februar 1999 nachgekommen.

Die vorgefundene Personalaktenführung zeigt jedoch, dass die Umstellung der Personalakten nach diesen neuen Vorgaben lediglich dadurch vollzogen wurde, dass der Aufdruck „Personalhauptakte“ mit einem Aufkleber, auf dem der Aufdruck „Personalgrundakte“ aufgebracht ist, überklebt wurde. Nach der gleichen Methode wurden die in der BA besonders umfangreichen „Personalbeiakten“, in Teilakten (Teilakte A bis Teilakte Z) umbenannt. Diese „Umstellung“ erfolgte sukzessive durch Registratoren und ist mit den gesetzlichen Vorgaben nicht vereinbar. Beratungsgespräche mit der BA haben bereits stattgefunden und werden fortgesetzt.

Diese Praxis musste ich auch bei anderen Bundesbehörden feststellen. Personalaktenrichtlinien sind oft so missverständlich formuliert, dass es als ausreichend angesehen wird, die bereits vorhandenen Personalunterlagen lediglich umzuetikettieren.

Es ist zu überlegen, inwieweit gemeinsam mit dem für das öffentliche Dienstrecht zuständigen BMI Lösungen – etwa in Form einer Muster-Personalaktenrichtlinie – gefunden werden, die helfen, die gesetzlichen Vorgaben zur Personalaktenführung endlich korrekt umzusetzen.

18.3.2 Personalaktenführung in der Bundesfinanzverwaltung beanstandet

Nach Verabschiedung der Vorschriften zum Umgang mit Personalaktendaten im Jahre 1992 kontrollierte ich die Zulässigkeit der Führung von Personalnebenakten nach § 90 BBG bei nachgeordneten Dienststellen des BMF (vgl. 14. TB Nr. 9.8). Seinerzeit bat ich das BMF, schnellstmöglich eine einheitliche, datenschutzgerechte Regelung zum Personalaktenrecht für den gesamten Geschäftsbereich in Kraft zu setzen, was im März 1998 dann geschah. Im Berichtszeitraum kontrollierte ich diese Regelung in einem Bundesvermögens- und einem Hauptzollamt.

Zur Kontrolle in einem Bundesvermögensamt:

Bei der Kontrolle eines Bundesvermögensamtes musste ich feststellen, dass diese Richtlinie, bezogen auf die dort geführten und von mir stichprobenartig geprüften Personalnebenakten der Beschäftigten, nicht umgesetzt war. So enthielten die Personalnebenakten u. a. Unterlagen, die zur rechtmäßigen Personalverwaltung des Bundesvermögensamtes nicht oder nicht mehr erforderlich waren, also nach § 90f Abs. 2 BBG bereits hätten vernichtet sein müssen, wie z. B. Krankmeldungen und Krankheitsangaben, sowie Unterlagen über Erholungsurlaub ab dem Jahre 1978 oder solche mit Informationen über andere Mitarbeiter.

Die in Personalnebenakten offen abgelegten Unterlagen mit Diagnoseangaben, etwa zu Erkrankungen von Kindern der Beschäftigten, oder ein ärztliches Zeugnis aus dem Jahre 1977 habe ich besonders bemängelt. Die festgestellte Praxis verstieß in zahlreichen Punkten gegen die Regelungen der §§ 90 ff. BBG und stand darüber hinaus nicht im Einklang mit den Richtlinien des BMF zum Personalaktenrecht. Ich habe diesen mangelhaften Umgang mit besonders schützenswerten Daten – Personalaktendaten – gegenüber dem BMF gem. § 25 Abs. 1 BDSG als Verstoß gegen die Regelungen der §§ 90 ff. BBG beanstandet.

Zur Kontrolle eines Hauptzollamtes:

Bei der Prüfung von nach dem Zufallsprinzip ausgewählten Personalnebenakten musste ich leider auch dort umfangreiche Verstöße gegen die §§ 90 ff BBG im Umgang mit Personalaktendaten der Mitarbeiter feststellen. Darüber hinaus fand ich bei einem Sachgebietsleiter neben einer automatisiert geführten Personaldatei mit zahlreichen Personalaktendaten auch eine nicht-automatisierte Personaldatei mit von ihm über jeden seiner Mitarbeiter angelegten Karteikarten. Beide Dateien führte er zur seiner Verwendung als Fachvorgesetzter. Daneben waren bei ihm weitere Unterlagen mit Personal-/Personalaktendaten, etwa Ablichtungen vollständiger Beurteilungen seiner Mitarbeiter aus früheren Jahren, vorhanden.

Die Führung von Vorgängen zu jedem Mitarbeiter ist eine ausschließliche Aufgabe der Personalverwaltung. Personalaktendaten sind in die Personalakte oder in die Personalnebenakte aufzunehmen und dürfen in Da-

teien nur für Zwecke der Personalverwaltung oder Personalwirtschaft gespeichert werden. Die Aufbewahrung von Personalaktendaten im Fachreferat ist unzulässig. Auch Ablichtungen von dem Mitarbeiter eröffneten Beurteilungen dürfen bei Fachvorgesetzten nicht gesammelt werden.

Ich habe die dargestellte Verarbeitung von Personal-/Personalaktendaten durch den Sachgebietsleiter als einen schweren Verstoß gegen die Regelungen des Bundesbeamtengesetzes (§§ 90 ff.) bewertet.

Weiterhin habe ich auf dem PC einer nicht der Personalstelle angehörigen Schreibkraft unzulässigerweise noch alle den Mitarbeitern bereits eröffneten und zu deren Personalakte genommenen vollständigen Beurteilungen zu einem über 16 Monate zurückliegenden Zeitpunkt vorgefunden.

Ebenfalls als Personalnebenakten anzusehen war eine in einer Dienststelle des Hauptzollamtes geführte Personaldatei, bestehend aus sog. Personal-Karteikarten mit Personalaktendaten der Mitarbeiter. Gegen die Führung dieser Datei habe ich grundsätzlich keine Bedenken erhoben, da sie für Personalverwaltungsaufgaben dieser Dienststelle notwendig war. Die Karteikarten enthielten jedoch zu umfangreiche, für die Aufgabenerfüllung der Dienststelle nicht erforderliche und damit unzulässige Personalaktendaten, wie Angaben zu Zeiten des Grundwehrdienstes, zu Ernennungen, Bestellungen und Beschäftigungszeiten von Beamten ab 1971.

In dieser Dienststelle habe ich ferner festgestellt, dass vertrauliche Personalaktendaten, etwa Unterlagen über Unfall-/Krankmeldungen, zu dienstlichen Verwendungen, Nebentätigkeiten, Fortbildungsmaßnahmen sowie ärztliche Bescheinigungen in einem offenen und somit für jedermann zugänglichen Schrank aufbewahrt wurden, was nicht den gesetzlichen Vorgaben des § 90 Abs. 3 BBG entsprach.

Auch diese zahlreichen Mängel im Umgang mit Personalaktendaten (manuell und automatisiert) habe ich gegenüber dem BMF als einen Verstoß gegen die Regelungen der §§ 90 ff BBG förmlich beanstandet.

Das BMF hat im geprüften Bundesvermögens- und Hauptzollamt umgehend notwendige Maßnahmen, etwa die Vernichtung unzulässig geführter Unterlagen oder die erforderliche Löschung von Daten und Dateien umgesetzt und zur gesetzesmäßigen Personalaktenführung im gesamten Geschäftsbereich erforderliche Schritte eingeleitet.

18.4 Nutzung von Personaldaten zu anderen Zwecken

Über die Nutzung von Personaldaten zu Werbezwecken habe ich bereits in meinem 17. TB (Nr. 18.3.4) berichtet. Im Berichtszeitraum hatte ich die Gelegenheit, die Deutsche Post AG in zwei weiteren Bereichen der Nutzung von Personaldaten zu Werbezwecken datenschutzrechtlich zu beraten.

18.4.1 Beteiligung der Mitarbeiter der Deutschen Post AG am Börsengang

Im Zusammenhang mit ihrem Börsengang hat die Deutsche Post AG ein umfangreiches Mitarbeiter-Beteiligungsprogramm aufgelegt. Hierüber wurden alle Mitarbeiter bereits informiert, als über die konkrete Gestaltung der Mitarbeiterbeteiligung noch nicht abschließend entschieden war. Zielgruppe des Mitarbeiter-Beteiligungsprogramms waren rund 300 000 Beschäftigte.

Um der besonderen Dimension des Programms bereits im Vorfeld gerecht zu werden und eine spätere Umsetzung sicherzustellen, sollten für interessierte Mitarbeiter schon frühzeitig entsprechende Konten/Depots bei der Postbanktochter EasyTrade.AG eingerichtet werden. Hierfür benötigte die Postbank EasyTrade.AG Daten der Beschäftigten (wie Vorname, Name, Geburtsdatum, Privatanschrift, Personalnummer und Gehaltskontoverbindung). Diese Daten sollten sowohl der Vorbereitung von persönlichen Depotkonten, als auch der späteren Übersendung der Zeichnungsunterlagen dienen.

Einige Mitarbeiter der Deutschen Post AG hatten sich an mich gewandt, weil sie befürchteten, dass die Personaldaten ohne ihre Mitwirkung in dem dargestellten Zusammenhang genutzt würden. Außerdem befürchteten sie für den Fall, dass sie einer Übermittlung dieser Daten an die Postbank EasyTrade.AG widersprochen hätten, dienstliche Nachteile. Dieser Eindruck entstand wohl aufgrund einer Information an alle Beteiligten vom Juli 2000, wonach Mitarbeiter, die sich nicht als Aktionär an „ihrer“ Deutschen Post beteiligten, auch nicht zum Erfolg des Unternehmens beim Börsengang beitrügen; auch würden sie wegen ihres Widerspruchs gegen eine Übermittlung ihrer Daten an die Bank von einer späteren Teilnahme am Mitarbeiterprogramm ausgeschlossen werden.

In mehreren Gesprächen habe ich sowohl gegenüber der Deutschen Post AG als auch gegenüber der Postbank auf ein möglichst transparentes Verfahren gedrängt, das nicht nur umfassende Hinweise zum Datenschutz im Zusammenhang mit den einzelnen Verfahrensschritten des Mitarbeiter-Beteiligungsprogramms umfassen müsse, sondern auch entsprechende Hinweise zum Online- und Telefonbanking. Dabei sei insbesondere zu berücksichtigen, dass

- die Mitarbeiter bis zur rechtsverbindlichen Zeichnung jederzeit aus dem Verfahren aussteigen können,
- Daten derjenigen Mitarbeiter, die kein Depot eröffnen oder durch entsprechende Erklärung aus dem Programm ausgeschieden sind, gelöscht werden und schließlich
- die Abschottung des Verfahrens zur Personalstelle sowohl im Vorfeld als auch nach Zeichnung der P-Aktie gewährleistet sein muss.

Dementsprechend wurden die mit dem Auftakt zum Mitarbeiter-Beteiligungsprogramm verteilten Informationsunterlagen um wichtige Informationen zum Datenschutz ergänzt:

„Die persönlichen Angaben in den Unterlagen zum Mitarbeiter-Beteiligungsprogramm beruhen auf Ihren Daten im Bezügezahlungssystem, die an die Postbank EasyTrade.AG weiter geleitet wurden, soweit Sie keinen Widerspruch eingelegt haben. Diese Unterlagen dürfen dort nicht für andere Zwecke genutzt und auch nicht an Dritte weitergegeben werden. Mit Ihren Daten wurde zunächst die Voraussetzung dafür geschaffen, dass Sie am Mitarbeiter-Beteiligungsprogramm teilnehmen können.

Wenn Sie sich entscheiden, weiter am Mitarbeiter-Beteiligungsprogramm teilnehmen zu wollen, ist für die weitere Teilnahme erforderlich:

- *jetzt ein Depot zu eröffnen und*
- *den Zeichnungsschein, der Ihnen in ca. vier Wochen zugesandt wird, ausgefüllt und unterschrieben an die hierfür vorgesehene Adresse zurückzusenden.*

Wenn Sie sich entscheiden, nicht weiter am Mitarbeiter-Beteiligungsprogramm teilzunehmen, so brauchen Sie nichts weiter zu tun. Ihre Daten werden nach Versand der Zeichnungsunterlagen nicht weiter verwendet und spätestens mit Ablauf des 31. Dezember 2000 gelöscht. Wegen Fristüberschneidung erhalten Sie den Zeichnungsauftrag in jedem Fall zugesandt, auch wenn Sie kein Depot eröffnet haben. Für den Fall, dass Sie eine Löschung ihrer Daten vor dem 31. Dezmeber 2000 wünschen, wenden Sie sich bitte schriftlich an die Postbank EasyTrade.AG, Customer Management, Eduard-Rumpler-Str. 3 in 51149 Köln.

Wir weisen an dieser Stelle nochmals ausdrücklich daraufhin, dass eine Weitergabe von Informationen über das Ob und Wie Ihrer Teilnahme am Mitarbeiter-Beteiligungsprogramm an die Personalabteilungen ausgeschlossen ist. Eine Nichtteilnahme hat keinen Einfluss auf ihr Beschäftigungsverhältnis.“

Sowohl das erzielte Ergebnis als auch die Tatsache, dass sich im Anschluss an die Information an die Mitarbeiter und Anlauf des Mitarbeiter-Beteiligungsprogramms keine Mitarbeiter der Deutschen Post AG in dieser Angelegenheit mit Eingaben an mich gewandt haben, zeigt, dass die von mir immer wieder geforderte Transparenz bei der Verarbeitung von Personaldaten unabdingbare Voraussetzung für die Akzeptanz bei Mitarbeitern ist.

18.4.2 Dürfen Betriebsräte/Personalräte Gewerkschaften zu Werbezwecken mit Personaldaten versorgen?

Durch Mitarbeiter der Deutschen Post AG habe ich erfahren, dass Werbematerial der Deutschen Postgewerkschaft (DPG) mit einer Beitrittserklärung an deren Privatanschrift gesandt wurde, obwohl sie nicht Mitglied waren. Gleichzeitig wurde gebeten zu prüfen, wie die DPG an die Privatanschriften von Beschäftigten der Niederlassung gelangt ist.

Nach Mitteilung der Zentrale der Deutschen Post AG wurden von Seiten der Niederlassung keine Personaldaten an die DPG weitergeleitet. Auf eine entsprechende Nachfrage habe auch die DPG bestätigt, dass die Niederlassung keine Anschriften für eine Werbekampagne zur Verfügung gestellt habe.

Eine Kontrolle durch die für die Bezirksverwaltung der DPG zuständige Aufsichtsbehörde nach dem BDSG hat zwischenzeitlich ergeben, dass dort eine Datei „Nichtmitglieder“ zu Werbezwecken erstellt worden war. Dies erfolgte durch den Abgleich der Mitgliederdatei mit einer Personalliste der Deutschen Post AG, die der örtliche Betriebsrat zur Verfügung gestellt hatte.

Die Aufsichtsbehörde hat die Übermittlung von Personaldaten – hier: Name, Adresse, Amtsbezeichnung und Dienststelle – durch den Betriebsrat an die DPG als unzulässig bewertet. Dies wird damit begründet, dass die personalisierte Werbung für eine bestimmte Gewerkschaftsmitgliedschaft oder ähnliches nicht im Rahmen der Zweckbestimmung des Arbeitsvertrages der Beschäftigten liege und für den Betriebsrat auch nicht durch das Betriebsverfassungsgesetz abgedeckt sei. Darüber hinaus stünden überwiegende schutzwürdige Interessen des Betroffenen einer Weitergabe von Personaldaten an Dritte zu Werbezwecken entgegen (vgl. § 12 Abs. 4 in Verbindung mit § 28 Abs. 1 Nr. 1 und 2 BDSG).

Die Personaldaten der Mitarbeiter der Deutschen Post AG wurden der DPG vom Betriebsrat ohne Rechtsgrundlage zur eigenen Verfügbarkeit übermittelt. Die unzulässige Erhebung und Nutzung der Personaldaten durch die DPG wurde von der Aufsichtsbehörde förmlich beanstandet.

Die Datenerhebung und damit auch die anschließende Nutzung der Adressdaten zu Werbezwecken waren unzulässig. Der datenschutzrechtlichen Bewertung der Aufsichtsbehörde ist nichts hinzuzufügen. Aus meiner Sicht liegt jedoch der Weitergabe der Personaldaten durch den Betriebsrat der Niederlassung der Deutschen Post AG ein weiterer, **dienstrechtlicher** Aspekt zugrunde. Hier hat nämlich ein Mitarbeiter der Deutschen Post AG von der Personalverwaltung Personaldaten für seine Aufgabenerfüllung als Betriebsrat erhalten. Zu den Aufgaben des Betriebsrates gehört es nicht, verbandspolitische Interessen – hier Mitgliederwerbung für die DPG – zu vertreten. Damit hat ein Mitarbeiter die in seiner Funktion als Betriebsrat zu Recht erhaltenen Personaldaten für seine privaten Zwecke – sein Engagement als Gewerkschaftsfunktionär – genutzt. Dieses verstößt gegen das Personalaktengeheimnis.

Die Deutsche Post AG hat den dargestellten Sachverhalt zum Anlass genommen, die Betriebsräte in ihrem Bereich dahingehend zu belehren, dass die Nutzung der dem Betriebsrat zu seiner Aufgabenerfüllung anvertrauten Personaldaten nur im Rahmen der vom Betriebsverfassungsgesetz dargestellten Aufgaben zulässig ist.

18.5 Beihilfe

18.5.1 Immer noch Probleme bei der Abschottung der Beihilfebearbeitung von der Personalverwaltung

Mit dem 9. Gesetz zur Änderung dienstrechtlicher Vorschriften, das bereits zum 1. Januar 1993 in Kraft trat, forderte der Gesetzgeber erstmals in § 90a des Bundesbeam-

tengesetzes (BBG) eine organisatorische Trennung von Beihilfe- und Personalstelle. Danach soll die Beihilfe in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden; Zugang sollen nur Beschäftigte dieser Organisationseinheit haben. Die Ausgestaltung der gesetzlichen Vorgabe als „Soll-Vorschrift“ wurde vorgenommen, um insbesondere kleineren Behörden die Möglichkeit zu geben, Sachbearbeiter, die mit der Bearbeitung von Beihilfevorgängen nicht ausgelastet sind, auch anderweitig einsetzen zu können (vgl. BT-Drs. 12/544, S. 17). Hierauf habe ich in der Vergangenheit mehrfach hingewiesen (vgl. zuletzt 17. TB Nrn. 18.5.2 und 18.5.3).

Immer wieder erstaunlich ist jedoch, dass sich ausgerechnet große Stellen – wie das BMWi oder die Bundesanstalt für Arbeit – offenbar mit Problemen bei der Umsetzung dieser gesetzlichen Vorgabe plagen.

Im BMWi war die Bearbeitung von Beihilfeangelegenheiten ebenso dem Personalreferat zugewiesen wie der Ärztliche und Soziale Dienst. Als Begründung für ein Verbleiben der Beihilfebearbeitung und des Ärztlichen und Sozialen Dienstes in der Personalstelle wurde u. a. angeführt, dass durch den Umzug eines Teils des Ministeriums nach Berlin eine organisatorische Trennung faktisch dadurch erfolgt sei, dass der Arbeitsbereich Beihilfen und der Ärztliche und Soziale Dienst zum Dienstbereich Bonn gehöre. Damit seien aufgrund der räumlichen Trennung die Anforderungen des § 90a BBG erfüllt. Dass aber wegen der organisatorischen Einbindung im Personalreferat und des hierarchischen Verwaltungsaufbaus – Fachaufsicht von Referatsleiter und Stellvertreter – letztlich nicht ausgeschlossen werden kann, dass die Gesundheitsdaten der Mitarbeiter und deren Familienangehörige ohne deren Kenntnis letztlich Personalentscheidungen im BMWi beeinflussen können, wurde nicht gesehen.

Obwohl auf meine Initiative hin bereits 1993 die Abschottung der Beihilfebearbeitung von der Personalverwaltung für den Geschäftsbereich des BMWi angeordnet wurde, bedurfte es für die eigene Organisation eines monatelangen Schriftverkehrs, mehrerer intensiver Gespräche und der Androhung einer förmlichen Beanstandung, bevor mir nunmehr mitgeteilt wurde: *„..., wird die Position des Bundesbeauftragten für den Datenschutz zur Bearbeitung der Beihilfevorgänge im BMWi weder in fachlicher noch in rechtlicher Hinsicht geteilt. Dennoch wird gegenwärtig geprüft, ob und durch welche organisatorische Änderung Ihrem Anliegen Rechnung getragen werden könnte.“*

In der Zentrale der Bundesanstalt für Arbeit versteht sich das Personalreferat auch als Servicestelle für besonders schwierige Beihilfefragen. Dies wurde damit begründet, dass zahlreiche Kollegen ihre Beihilfeanträge nicht bei der für die Bearbeitung zuständigen besonderen Dienststelle der Bundesanstalt für Arbeit, sondern in der Personalstelle abgeben würden. Hier fände dann eine Vorprüfung statt, bevor die Unterlagen an die Abrechnungsstelle weitergeleitet würden. Gleiches gilt für Unterlagen über Heilfürsorge und Heilverfahren.

Die vom Gesetzgeber gewollte Abschottung von der übrigen Personalstelle – Zugang nur durch Beschäftigte dieser Organisationseinheit – wird von der dargestellten Praxis nicht umgesetzt. Zur Umsetzung des Abschottungsgebotes ist auch die (Teil-) Bearbeitung von Beihilfeangelegenheiten aus dem Personalreferat auszugliedern. Ich habe der Bundesanstalt für Arbeit empfohlen, alle Mitarbeiter über die Organisationsänderung entsprechend zu unterrichten. Damit auch nicht versehentlich Beihilfeunterlagen in der Personalverwaltung abgegeben werden, sollte ein entsprechender Aufdruck auf den Beihilfevordrucken verhindern. Eine weitere Möglichkeit wäre, den Mitarbeitern entsprechend vorbereitete, adressierte Umschläge für den Versand der Beihilfeunterlagen an die zuständige Stelle an die Hand zu geben.

18.5.2 Doch noch eigenes Antragsrecht für Familienangehörige?

Ein eigenes Antragsrecht für Familienangehörige wurde in der Vergangenheit oft und kontrovers diskutiert (s. zuletzt 15. TB Nr. 9.5.1). Die im folgenden kurz dargestellten Fälle aus Eingaben zur rechtlichen und tatsächlichen Situation volljähriger Familienangehöriger im Beihilfeverfahren haben mich veranlasst, die Problematik eines eigenen Antragsrechtes für volljährige Familienangehörige in Beihilfeverfahren erneut mit dem BMI zu erörtern:

- Eine von ihrem Ehemann getrennt lebende Petentin beschwerte sich darüber, dass sie gezwungen sei, im Rahmen des Beihilfeverfahrens ihrem beihilfeberechtigten Ehemann die ärztlichen Befundunterlagen mit hochsensiblen Gesundheitsdaten zugänglich zu machen. Dieser nutzte die ihm für Beihilfezwecke gegebenen Arztunterlagen und das Beihilfeverfahren selbst, um seine Ehefrau zu schikanieren.

- Eine Fachärztin für Psychiatrie teilte mir mit, dass der Ehemann ihrer Patientin das über diese im Rahmen des Beihilfeverfahrens erstattete und ihm übergegebene Gutachten zur Grundlage einer Scheidungsklage gemacht habe.

- Volljährige Kinder äußerten ihr Unverständnis, wenn sie die Inanspruchnahme ärztlicher Leistungen dem beihilfeberechtigten Elternteil offenbaren müssen, weil sie eine Kostenerstattung nur im Rahmen eines vom beihilfeberechtigten gestellten Beihilfeantrags erlangen können. In einem Fall sollte sich das volljährige Kind auf ärztlichen Rat einer psychotherapeutischen Behandlung unterziehen. Folglich musste dieses den beihilfeberechtigten Elternteil bitten, die Anerkennung seiner psychotherapeutischen Behandlungsbedürftigkeit zu beantragen. Welche Rückfragen und Konflikte dieses Verfahrens zur Folge haben kann, ist leicht nachzuvollziehen.

Das BMI hatte für seinen Bereich seinerzeit entschieden, dass Familienangehörige ihre Belege unmittelbar der Beihilfestelle zuleiten können, während der Beihilfeberechtigte hierauf lediglich pauschal Bezug nimmt, indem er z. B. angibt, dass es sich um ein Rezept für ein Familien-

mitglied handelt. Hieraus kann dann der Beihilfeberechtigte keine weiteren Rückschlüsse ziehen. Desgleichen werden die Belege unmittelbar an das betroffene Familienmitglied zurückgesandt (s. zuletzt 15. TB Nr. 9.5.1). Die Praxis des BMI ist jedoch nur ein kleiner Schritt in die richtige Richtung. Sie lässt, wie die dargestellten Eingaben belegen, auch mit Blick auf andere Ressorts, die diese Praxis nicht übernommen haben, weitere Fragen offen. Insbesondere sind auch all die Fälle nicht berücksichtigt, in denen beispielsweise die Beihilfefähigkeit **vor** der Leistungserbringung von der Festsetzungsstelle festgestellt werden muss (vor allem bei bestimmten zahnärztlichen, kieferorthopädischen oder Sanatoriums-Behandlungen, Psychotherapien, Kuren, Pflegebedürftigkeit).

Wenn auch die Beihilfe eine die Grundalimentation des Beamten ergänzende Fürsorgeleistung ist, die allein dem Beamten selbst einen originären Beihilfeanspruch zugesteht und die Familienangehörigen lediglich mit einschließt, halte ich die praktizierte Verfahrensweise für nur teilweise geeignet, datenschutzrechtlichen Anforderungen gerecht zu werden. Ein Festhalten an der bisherigen Argumentation halte ich auch mit Blick auf die Leitsätze „Moderner Staat – Moderne Verwaltung“ nicht mehr für zeitgemäß. Die bisherige Diskussion lässt auch nicht erkennen, warum eine Trennung von **Beihilfeanspruch** und **Antragsrecht** nicht möglich sein soll. Ein eigenes Antragsrecht für volljährige Familienangehörige berührt nach meiner Auffassung nicht die Rechtsposition des anspruchsberechtigten Beamten.

In der gesetzlichen Krankenversicherung, die bei der Fortentwicklung der Beihilferichtlinien teilweise als Vorbild diente, wurde den dargestellten gesellschaftlichen Entwicklungen mit dem 2. SGB-ÄndG und der damit verbundenen Ergänzung des § 10 SGB V Rechnung getragen. Hier wird der Leistungsanspruch des Versicherungsnehmers (Mitglied der Versicherung) in der Familienversicherung auf den mitversicherten Ehegatten und die (volljährigen) Kinder ausgedehnt.

In der privaten Krankenversicherung können Ehegatten, die verhindern wollen, dass der Partner und Versicherungsnehmer von Vorerkrankungen oder Diagnosen erfährt, in der Regel eine Vertragstrennung vereinbaren.

Durch die derzeitige Fassung des § 17 Beihilfeverordnung sind volljährige (berücksichtigungsfähige) Angehörige gezwungen, dem Anspruchsberechtigten besonders sensible Daten zu offenbaren, die dieser selbst nicht zu erfahren braucht, jedoch zur Abrechnung für die Beihilfestelle vorlegen muss.

Die von mir gegenüber dem BMI vorgeschlagene Änderung des § 17 der Beihilfevorschriften würde dem Selbstbestimmungsrecht des Betroffenen dadurch gerecht werden, dass ihm zugestanden wird, selbst Anträge zu stellen. Dies entspräche auch dem datenschutzrechtlichen Grundsatz der Ersterhebung beim Betroffenen selbst.

Ich freue mich, dass die Leitung des BMI zugesagt hat, meinen Vorschlag eines eigenen Antragsrechtes für Familienangehörige im Beihilfeverfahren erneut aufzugreifen. Sollte in absehbarer Zeit keine Einigung mit den Ländern gefunden werden, würde es dem Bund aufgrund seiner Zuständigkeit für das Dienstrecht sicher gut anstehen, ein entsprechendes Zeichen zu setzen.

18.5.3 Automatisierte Beihilfebearbeitung

Auch in diesem Berichtszeitraum haben mich Bundesbehörden gebeten, sie aus datenschutzrechtlicher Sicht bei der Umstellung ihrer Beihilfebearbeitung auf automatisierte Verfahren zu beraten.

Bei der automatisierten Bearbeitung von Beihilfe sind u. a. § 90a BBG sowie § 90g Abs. 2 BBG zu beachten. Nach letztgenannter Vorschrift dürfen Unterlagen über Beihilfen automatisiert nur im Rahmen ihrer Zweckbestimmung und nur von den übrigen Personaldateien technisch und organisatorisch getrennt verarbeitet und genutzt werden.

Die in den Bundesbehörden hierfür konkret zu treffenden Maßnahmen richten sich danach, in welchem technischen und organisatorischen Umfeld das Verfahren der automatisierten Beihilfebearbeitung betrieben werden soll. Dies kann beispielsweise in der Beihilfestelle selbst („Insellösung“) auf einem stand-alone PC oder in einem separierten Netz dieser Organisationseinheit, aber auch über das allgemeine Netz der Behörde erfolgen, falls die notwendigen Sicherheitsmaßnahmen umgesetzt sind.

Ferner halte ich es für erforderlich, für die automatisierte Beihilfebearbeitung konkrete Weisungen zu erlassen und deren Einhaltung stichprobenweise zu überprüfen. Diese Vorgaben, die z. B. in einer Dienstanweisung enthalten sein können, sollten insbesondere auch datenschutzrechtliche Regelungen wie Datenkatalog, Zugriffsrechte, Löschungsregelungen, Maßnahmen zur Datensicherheit enthalten.

Datenschutzverstöße im Bereich der automatisierten Beihilfebearbeitung sind mir bisher nicht bekannt geworden.

18.6 Automatisierte Personaldatenverarbeitung

18.6.1 Beratungen und Entwicklungen in der Bundesverwaltung

Zahlreiche Bundesbehörden planen in jüngster Zeit verstärkt für Zwecke der Personalverwaltung und -wirtschaft neue Personalinformations-/ Personalverwaltungssysteme einzuführen oder solche bestehenden Systeme in eine neue technische Umgebung zu überführen oder durch neue Programme zu ersetzen (vgl. hierzu auch Nr. 8.6.4).

Es ist zu begrüßen, dass ich bei einigen dieser Projekte, so beispielsweise beim BMVBW, BMZ, BVA oder der PTB, und der Planung und Einführung von sonstigen neuen Systemen der automatisierten Verarbeitung von Mitarbeiterdaten, etwa zur Durchführung der gleitenden Arbeitszeit, frühzeitig um Unterstützung gebeten wurde. Dies ist auch im Hinblick auf die mit einer automatisierten Verar-

beitung von Personal-/ Personalaktendaten verbundenen Risiken für die Persönlichkeitsrechte der Beschäftigten wichtig, was meine nachfolgenden Kontrollfeststellungen eindrucksvoll belegen.

18.6.2 Personaldatenverarbeitung des BAFl erneut beanstandet

Veranlasst durch die bei einer früheren Datenschutzkontrolle von mir beanstandeten Mängel (vgl. 17. TB Nr. 18.9.1) habe ich im Berichtszeitraum eine Anschlusskontrolle der automatisierten Personaldatenverarbeitung in der Zentrale des BAFl durchgeführt.

Dort werden im Personalreferat die Personalverwaltungssysteme „INFO-Z“ im Wirkbetrieb und parallel hierzu im Testbetrieb das Personalverwaltungssystem „EPOS“, das nach der Einführung das vorgenannte System ablösen soll, eingesetzt. An den Arbeitsplätzen der mit der Datenbankadministration der Systeme betrauten Mitarbeiter wurden zum Teil auch Arbeiten zur Weiterentwicklung von Programmen bzw. Programmteilen vorgenommen. Dabei fand ich u. a. auf den lokalen Laufwerken dieser PC's teilweise vollständige Datenbankkopien der vorgenannten Personalverwaltungssysteme, die dort auch längerfristig gespeichert waren. Mittels auf diesen PC abgelegter Programmroutinen konnten die Bearbeiter jederzeit aktuelle Datenbankkopien von dem im Rechenzentrum befindlichen Datenbankserver herunterladen und lokal abspeichern. Die aus „INFO-Z“ gewonnene Datenbestände wurden dann für referatsinterne Auswertungen, aber auch ohne erforderliche Anonymisierung zu Testzwecken verwendet. Die Speicherung dieser Datenbestände auf dem PC entsprach weder technisch noch organisatorisch den gesetzlichen Anforderungen. So war etwa die geforderte physische Trennung der Datenbestände nach Echt- und Testbetrieb nicht erfolgt.

Die zahlreichen Mängel im Bereich der Datensicherheit im Umgang mit Mitarbeiterdaten habe ich gegenüber dem BMI erneut als Verstoß gegen § 9 sowie Anlage zu § 9 Satz 1 BDSG beanstandet.

Im Personalverwaltungssystem „INFO-Z“ habe ich auch Datensätze von mehr als 1 500 ehemaligen Mitarbeitern, bis in das Jahr 1994 zurückreichend, vorgefunden. Hierbei handelte es sich nicht etwa um wenige ausgewählte Stammdaten, sondern um den kompletten Datensatz (Personalaktendaten), wie er in diesem System auch über die aktiv Beschäftigten des BAFl geführt wird.

In geringerem Umfang enthielten auch „EPOS“ und die automatisierte Fortbildungsdatei ausgewählte Personalaktendaten von ehemaligen Beschäftigten. Daneben waren noch in einer nicht-automatisierten Personaldatei Passfotos und umfangreiche Personalaktendaten von allen ehemaligen Mitarbeitern vorhanden.

Demnach hatte das BAFl zum Zeitpunkt der Kontrolle noch umfangreiche Personalaktendaten aller ehemals dort beschäftigten Mitarbeiter gespeichert. Es handelte sich hierbei um Personalnebenakten im Sinne des § 90 Abs. 2 Satz 3 BBG, für deren Führung die gesetzlichen Voraussetzungen (vgl. Nr. 18.3.1.2) nicht gegeben waren. Ich habe diese Speicherung deshalb als unzulässig bewertet und deren umgehende Löschung gefordert. Keine Bedenken bestehen aus meiner Sicht, für einen bestimmten Zeitraum einen sehr eingeschränkten Datensatz über ausgeschiedene Mitarbeiter zur notwendigen Abwicklung von „Personalmaßnahmen“ bei der ehemaligen Beschäftigungsbehörde zu speichern, wenn die Betroffenen hierüber informiert werden.

Weiterhin fand ich an einem der Administrator-Arbeitsplätze im Personalreferat in Ordnern, die der Dokumentation des Personalverwaltungssystems „INFO-Z“ dienten, unzulässigerweise Personalaktendaten von Mitarbeitern, wie z. B. Listen aus früheren Jahren mit Beurteilungsnoten, Angaben zu Behinderungen oder Personalstammblätter, die als „Muster“ aufbewahrt wurden sowie, für jedermann zugänglich, hunderte Abdrucke von alten, sensiblen Schreiben an Mitarbeiter zu Personalmaßnahmen, etwa Kündigungen. Diese hätten nach Aufnahme in die Personalakte und Zustellung längst vernichtet sein müssen.

Ich habe die vorgefundenen Mängel im Umgang mit Personalaktendaten im BAFl (automatisiert und nicht-automatisiert) gegenüber dem BMI als einen Verstoß gegen die Regelungen der §§ 90 ff BBG beanstandet.

Das BAFl hat bereits zahlreiche meiner Forderungen und Empfehlungen, etwa die erforderliche Löschung personenbezogener Daten der dort ehemals Beschäftigten, umgesetzt bzw. notwendige Maßnahmen eingeleitet.

18.6.3 Personaldaten sind besonders schutzbedürftig

Fast alle Behörden des Bundes nutzen heute sogenannte Personalinformations- bzw. Personalverwaltungssysteme, die die Personalverwaltung und Personalwirtschaft unterstützen. Mit den Systemen werden in erster Linie Personal**akten**daten im Sinne des § 90 Abs. 1 Satz 2 Bundesbeamtengesetz (BBG) verarbeitet. Dies sind alle Informationen über den Beamten, soweit sie mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen. Sie unterliegen dem **Personalaktengeheimnis** und sind besonders schützenswert: Nach § 90 Abs. 1 Satz 1 Halbsatz 2 BBG ist die Personalakte (hierzu gehören auch Personalaktendaten, die automatisiert verarbeitet werden) vertraulich zu behandeln und vor unbefugter Einsichtnahme zu schützen. Bei der Verarbeitung dieser besonders schützenswerten Daten sind auch besonders wirksame technische und organisatorische Maßnahmen i. S. § 9 BDSG – wie u. a. zum Schutz gegen unbefugte Kenntnisnahme – vorzusehen.

§ 90 ff BBG, insbesondere § 90g BBG sind spezialgesetzliche datenschutzrechtliche Vorschriften – etwa zum Zugang zur Personalakte. Sie sind auch in den Systemen sicherzustellen. Darüber hinaus werden in den Personalverwaltungs- und Personalinformationssystemen auch sonstige Mitarbeiterdaten verarbeitet, die nicht unter die Definition des BBG für Personal**akten**daten fallen.

Leider gibt es bei meinen Kontrollen immer wieder Anlass, auf Verstöße und Mängel bei der Erhebung und Verarbeitung von Personaldaten oder von Daten, die dem

Personalaktengeheimnis unterliegen, hinzuweisen oder sogar förmlich zu beanstanden (s. o. Nr. 18.6.2).

18.7 Kontrolle der E-Mail und Internet-Aktivitäten der Mitarbeiter

Im Zuge der fortschreitenden IT-Ausstattung von Arbeitsplätzen haben auch immer mehr Mitarbeiter in der Bundesverwaltung unmittelbaren Zugang zum Internet. Sie können die vielfältigen Informationsangebote des World Wide Web (WWW) nutzen sowie Texte und Dokumente per E-Mail versenden und empfangen.

In diesem Zusammenhang erhebt sich immer öfter die Frage, ob und ggfs. wie der Dienstherr die Nutzung des Internetzugangs kontrollieren darf. Ein berechtigtes Interesse an einer solchen Kontrolle ist grundsätzlich nicht zu bestreiten. Ist die Internetnutzung nämlich nur zu dienstlichen Zwecken erlaubt, stellt jede Nutzung zu privaten Zwecken eine Pflichtverletzung des Beschäftigten dar. Aber auch dann, wenn die private Nutzung ausdrücklich oder konkludent erlaubt ist, versteht es sich von selbst, dass dies nicht ein zeitlich „ausgedehntes“ Surfen im Internet oder den Abruf von Seiten mit strafbarem oder sittenwidrigem Inhalt umfasst.

Eine lückenlose Auswertung aller Einzelzugriffe der Mitarbeiter im WWW wäre unverhältnismäßig und somit unzulässig. Eine stichprobenweise Auswertung bzw. eine Auswertung bei einem konkreten Verdacht einer unzulässigen Nutzung halte ich dagegen für zulässig. Bei dienstlichen E-Mails ist der Dienstherr berechtigt, diese einzusehen – unabhängig davon, ob die E-Mail an ein Postfach der Dienststelle oder an das Postfach eines bestimmten Beschäftigten gerichtet ist. Private E-Mails – sofern sie zugelassen sind – unterliegen dagegen dem Fernmeldegeheimnis mit der Folge, dass der Dienstherr von diesen keine Kenntnis nehmen darf. Wie realisiert werden kann, vergleichbar Telefonaten, zwischen dienstlichen und privaten E-Mails zu unterscheiden, ist noch nicht gelöst. Anders als bei Telefonaten kann mit E-Mails dem Netz einer Behörde Schaden zugefügt oder auch der Server mit strafbaren oder sittenwidrigen Dokumenten belastet werden.

Die Protokollierung und Auswertung der E-Mail und der Internet-Aktivitäten der Mitarbeiter zu Kontrollzwecken bedarf gem. § 75 Abs. 3 Nr. 17 BPersVG ausnahmslos der vorherigen Zustimmung der zuständigen Personalvertretung, da diese Maßnahmen immer zu einer Verhaltens- und Leistungskontrolle geeignet sind. In der zu schließenden Dienstvereinbarung sollte auch im einzelnen geregelt werden, ob eine private Nutzung des Internet erlaubt wird und in welchem Rahmen dies ggfs. zulässig ist.

Besonders wichtig ist es, die Mitarbeiter rechtzeitig und umfassend über die Modalitäten der Internetnutzung zu informieren. Dem einzelnen Mitarbeiter muss bekannt sein, was er darf und was nicht und welche Kontrollmöglichkeiten sich der Dienstherr vorbehält.

Vor dem Hintergrund, dass sich zu den im Zusammenhang mit der Internetnutzung am Arbeitsplatz ergebenden Fragen in Rechtsprechung und Literatur bisher keine feste Meinung gebildet hat, halte ich gesetzliche Regelungen zu diesem Komplex für dringend notwendig. Es bietet sich an, solche Regelungen in das von der Bundesregierung angekündigte Arbeitnehmerdatenschutzgesetz (s. o. Nr. 18.1) aufzunehmen.

18.8 Kosten- und Leistungsrechnung

§ 7 Abs. 3 der Bundeshaushaltsordnung verpflichtet die Bundesverwaltung, in geeigneten Bereichen eine Kosten- und Leistungsrechnung (KLR) einzuführen. KLR soll als Ergänzung der Haushaltsflexibilisierung Bestandteil eines umfassenden Controllingsystems werden und als Grundlage einer längerfristig geplanten, stärker an Leistungen und Produkten orientierten Mittelbereitstellung dienen.

Da im Rahmen einer KLR auch personenbezogene Daten der Mitarbeiter – nämlich insbesondere deren zeitlicher Aufwand bei der Erstellung eines Produkts bzw. bei der Erbringung einer Dienstleistung – erhoben werden, habe ich mehrere Dienststellen auf deren Wunsch hinsichtlich einer datenschutzgerechten Ausgestaltung des entsprechenden Zeiterfassungsverfahrens beraten. Dabei ist von mir auf folgende Punkte besonderer Wert gelegt worden:

- Die erhobenen personenbezogenen Zeitdaten müssen so früh wie möglich anonymisiert bzw. aggregiert werden; Rückschlüsse auf die Leistungen einzelner Mitarbeiter müssen danach ausgeschlossen sein.
- Die KLR ist in einer von der Personalstelle räumlich und organisatorisch getrennten Organisationseinheit zu bearbeiten.
- Im Rahmen der KLR erhobene Daten dürfen nicht zum Zweck einer Verhaltens- oder Leistungskontrolle einzelner Mitarbeiter verwendet werden.
- Das KLR-Zeiterfassungsverfahren muss in einer Dienst- bzw. Betriebsvereinbarung im einzelnen festgelegt werden.
- Die Mitarbeiter sollten aus Gründen der Transparenz rechtzeitig und umfassend über das neue Verfahren informiert werden.

Meine Empfehlungen sind erfreulicherweise in die entsprechenden Dienstvereinbarungen eingeflossen. Eine entsprechende Ausgestaltung neuer Verfahren erhöht sicherlich auch die Akzeptanz bei den betroffenen Mitarbeitern, was zugleich im Interesse einer Dienststelle liegt.

18.9 Telearbeit

Im Zuge der Erprobung und Einführung neuer Arbeitsformen gewinnt die Telearbeit auch in der öffentlichen Verwaltung zunehmend an Bedeutung. Zwar gab es bereits in der Vergangenheit vereinzelt Arbeitsplätze, bei denen die Arbeitsleistung zumindest teilweise nicht in den Diensträumen, sondern zuhause erbracht wurde. Erst die moderne Informations- und Kommunikationstechnologie ermöglicht es aber, in größerem Umfang dienstliche

Tätigkeiten in den häuslichen Bereich der Beschäftigten zu verlagern.

Datenschutz als Schutz des Rechts auf informationelle Selbstbestimmung steht nicht im Gegensatz zur Telearbeit. Das erklärte Ziel der Bundesregierung, Telearbeit zu fördern und die Anzahl der Telearbeitsplätze in der Bundesverwaltung signifikant zu erhöhen, wird daher selbstverständlich von mir mitgetragen und beratend unterstützt.

Die Verlagerung dienstlicher Aufgaben in den häuslichen Bereich birgt allerdings Risiken. Die Kontroll- und Einflussmöglichkeiten der Dienststelle werden erheblich erschwert, wenn nicht sogar unmöglich, und zugleich nehmen die Einflussnahme- und Missbrauchsmöglichkeiten durch Dritte deutlich zu. Vor diesem Hintergrund muss bei der Beurteilung der Frage, ob und gegebenenfalls unter welchen Umständen Telearbeit in Betracht kommt, nach der Art der zu verarbeitenden Daten und ihres Verwendungszusammenhanges unterschieden werden:

- Bei der Verarbeitung nicht personenbezogener Daten ist der Datenschutz im Sinne des Rechts auf informationelle Selbstbestimmung nicht tangiert.
- Daten mit allgemeinem Personenbezug können im Rahmen von Telearbeit dann verarbeitet werden, wenn – abhängig von der Schutzwürdigkeit dieser Daten und ihres Verwendungszusammenhanges – angemessene Schutzmaßnahmen zur Vermeidung bzw. Minimierung der genannten Risiken getroffen werden. Hierbei werden vielfach – bezogen auf die konkrete Aufgabe – differenzierte und intelligente Lösungen möglich sein.
- Besonders schutzwürdige personenbezogene Daten sind meiner Auffassung nach grundsätzlich nicht für die Telearbeit geeignet, da sich die entsprechenden Risiken in der Praxis kaum gänzlich vermeiden lassen. Zu den besonders sensiblen Daten gehören vor allem solche über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gesundheit sowie Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen (vgl. auch Art. 8 der EG-Datenschutzrichtlinie).

Soweit nach den dargestellten Grundsätzen Telearbeit zulässig ist, muss durch geeignete technisch-organisatorische Maßnahmen der Schutz personenbezogener Daten gewährleistet werden. Hierbei sind insbesondere folgende Gesichtspunkte zu beachten:

- Der Transport von Akten und Datenträgern zwischen Dienststelle und häuslichem Arbeitsplatz muss in verschlossenen Behältnissen der Dienststelle erfolgen, wobei die Daten auf elektronischen Datenträgern stets zu verschlüsseln sind. Ferner ist der Telearbeiter durch entsprechende Regelungen im Telearbeitsvertrag zu verpflichten, beim Transport von Unterlagen diese nicht unbeaufsichtigt zu lassen.
- Werden Daten durch Datenfernübertragung zwischen der Dienststelle und dem Telearbeitsplatz ausgetauscht, sind diese Daten ebenfalls zu verschlüsseln.
- Der Telearbeiter muss verpflichtet werden, Akten und Datenträger im häuslichen Bereich so aufzubewahren, dass eine Kenntnisnahme bzw. eine Entwendung durch Dritte ausgeschlossen ist. Die hierfür erforderlichen verschließbaren Einrichtungsgegenstände sind von der Dienststelle zur Verfügung zu stellen.
- Eine private Nutzung der von der Dienstelle gestellten IT-Ausstattung ist zu untersagen.
- Der Telearbeiter und seine in häuslicher Gemeinschaft lebenden Familienangehörigen haben sich vertraglich ausdrücklich zu verpflichten, sowohl dem Beauftragten der Dienstelle als auch mir zu Kontrollzwecken Zugang zum häuslichen Arbeitsbereich zu gewähren. Wegen des Grundrechts auf Unverletzlichkeit der Wohnung (Art. 13 GG) wäre ansonsten eine wirksame datenschutzrechtliche Kontrolle nicht möglich. Bei einem Widerruf der erteilten Einwilligung durch den Telearbeiter ist die Telearbeit zu beenden.

Die mir bekannt gewordenen Dienstvereinbarungen zur Telearbeit, z. B. die des BMI und BMU, berücksichtigen diese Grundsätze. Ob die Datenschutzregelungen in der Praxis eingehalten werden, habe ich noch nicht kontrolliert. Im Berichtszeitraum gab es noch keine nennenswerte Zahl von Telearbeitsplätzen.

18.10 Personaldaten im Internet

Immer mehr Bundesbehörden nutzen die Möglichkeit, sich mit ihren Aufgaben im Internet nach außen darzustellen. Dabei werden häufig auch Daten der Mitarbeiter veröffentlicht.

Die Veröffentlichung von Mitarbeiterdaten einer öffentlichen Stelle ist aber nur zulässig, wenn sie zu deren ordnungsgemäßen Aufgabenerfüllung erforderlich ist. Dazu zählt grundsätzlich auch die Information, welcher Mitarbeiter der richtige Ansprechpartner für das Anliegen eines Bürgers oder eines Bediensteten einer anderen Behörde ist und wie dieser Mitarbeiter erreicht werden kann. Für eine Veröffentlichung im Internet kommen daher Daten folgender Personenkreise in Betracht:

- Mitarbeiter, die mit der Leitung von Referaten oder übergeordneten Organisationseinheiten beauftragt sind,
- Mitarbeiter mit Außenkontakten, die als offizielle Ansprechpartner fungieren,
- weitere Mitarbeiter (z. B. solche mit lediglich innerdienstlichen Aufgaben wie Registratur, Botendienst oder zentraler Schreibdienst) nur mit deren Einwilligung; der Einwilligung muss eine ausreichende Unterrichtung über die vorgesehenen Nutzungsmöglichkeiten und die damit verbundenen Risiken vorausgehen.

In einem weiteren Schritt ist zu prüfen, welche Daten im einzelnen veröffentlicht werden sollen. Grundsätzlich zulässig sind nur folgende Angaben:

- Name,
- Amts- und Dienstbezeichnung,
- Funktion und Tätigkeitsbereich,
- dienstliche Haus-, Post- und E-Mail-Adresse,
- dienstliche Telefon- und Faxnummern.

Weitergehende Daten oder Fotos dürfen nur mit Einwilligung des Mitarbeiters im Internet veröffentlicht werden, soweit hierfür eine Notwendigkeit erkennbar ist.

Aus Gründen der Transparenz sind die betroffenen Mitarbeiter vor einer Veröffentlichung rechtzeitig und umfassend zu informieren. Ihnen sollte auch die Möglichkeit eingeräumt werden, einer Veröffentlichung möglicherweise entgegenstehende individuelle Gründe geltend zu machen. Über die Berücksichtigung solcher Gründe müsste die Dienststelle im Rahmen pflichtgemäßen Ermessens entscheiden. Zur Veröffentlichung von Mitarbeiterdaten im Intranet (Verzeichnisdienste) siehe Nr. 8.9.

19 Sozialwesen – Allgemeines –

19.1 Erfolgskontrollierende wissenschaftliche Begleitung des Sozialhilfedatenabgleichs

In meinem 17. TB (Nr. 19.3) hatte ich über die Einführung eines automatisierten regelmäßigen Datenabgleichs der Sozialhilfeträger mit anderen Leistungsträgern (andere Sozialämter, Bundesanstalt für Arbeit, gesetzliche Renten- und Unfallversicherung) sowie das entsprechende Verfahren ausführlich berichtet. Rechtsgrundlage für diesen Datenabgleich sind § 117 BSHG und die am 1. Januar 1998 in Kraft getretene Sozialhilfedatenabgleichsverordnung. Ziel des Sozialhilfedatenabgleichs ist es, vom Sozialhilfeempfänger nicht angegebene Beschäftigungsverhältnisse oder konkurrierende Bezüge anderer Sozialleistungen aufzudecken.

Auf meine Anregung hin hatte das BMA das Institut für Sozialforschung und Gesellschaftspolitik (ISG) mit der wissenschaftlichen Begleitung einer rund eineinhalbjährigen Umsetzungsphase dieser Neuregelung während der Jahre 1998/99 beauftragt. Der Abschlussbericht des ISG wurde im Juni 2000 vorgelegt. Er beruht im wesentlichen auf der Befragung von 177 Sozialhilfeträgern, die sich an dem automatisierten Datenabgleich in der Sozialhilfe beteiligt haben. Die befragten Sozialhilfeträger, unter denen zu 38 % kreisfreie Städte und zu 62 % (Land-)Kreise vertreten waren, repräsentieren ca. 39 % aller Sozialhilfeempfänger mit laufender Hilfe zum Lebensunterhalt. Die Ergebnisse der Begleitstudie dürften daher zu verallgemeinern sein.

Aufschluss gibt die Studie zunächst zu der Frage, wie häufig und mit welchem Schaden den Sozialhilfeträgern durch den Datenabgleich bis dahin nicht bekannte sog. schadhafte Parallelbezüge bekannt geworden sind. „Schadhaft“ bedeutet, dass Leistungen nach dem Bundessozialhilfegesetz – ganz oder teilweise – unrechtmäßig bezogen wurden und dem Sozialhilfeträger dadurch ein materieller Schaden entstanden ist. Die Befragung der Sozialhilfeträger hat ergeben, dass die weit überwiegende Mehrheit der Sozialhilfeempfänger anderweitige Einkünfte korrekt angibt. Schadhafte Parallelbezüge wurden nur bei rund 2,5 % aller Empfänger (mit Bezug von Hilfe zum Lebensunterhalt außerhalb von Einrichtungen) festgestellt. Die Schadenshöhe belief sich auf ca. 0,5 % der Gesamtausgaben. Die Studie des ISG enthält allerdings keine absoluten Zahlen hinsichtlich der Schadenshöhe. Legt man zugrunde, dass im Jahr 1997 rund 1,49 Millionen Empfänger Sozialhilfe in Form von Hilfe zum Lebensunterhalt außerhalb von Einrichtungen mit einer durchschnittlichen monatlichen Höhe von 787 DM erhielten (Quelle: Statistisches Bundesamt, Statistisches Jahrbuch 1999), ergeben sich jährliche Gesamtausgaben von etwas über 14 Milliarden DM bzw. ein durch den Datenabgleich aufgedeckter jährlicher Schaden von rund 70 Millionen DM.

Neben der Aufdeckung der missbräuchlichen Inanspruchnahme von Sozialhilfe zielt der automatisierte Datenabgleich nach § 117 BSHG auch darauf ab, die Antragsteller präventiv dazu zu bewegen, eventuelle anderweitige Einkünfte vollständig zu offenbaren. Nach der Einschätzung bzw. den Erfahrungen von zwei Drittel der befragten Sozialhilfeträger führt allein das Wissen darüber, dass das Sozialamt (möglicherweise) einen Datenabgleich vornimmt, dazu, dass Sozialhilfeempfänger vollständigere Angaben bezüglich ihrer Einkünfte machen.

Angesichts der aufgezeigten Ergebnisse – insbesondere des aufgrund des Datenabgleichs zu Tage getretenen nicht unbeträchtlichen Schadensvolumens von rund 70 Millionen DM jährlich – und der wohl nicht zu unterschätzenden Präventivwirkung erscheint mir der automatisierte Sozialhilfedatenabgleich nach § 117 BSHG zur Aufdeckung und Verhinderung von Leistungsmissbrauch noch vertretbar. Gleichwohl muss zukünftig beobachtet werden, ob der Datenabgleich im Interesse des Gemeinwohls weiterhin gerechtfertigt ist.

19.2 Automatisierte Mitteilung von Rentenänderungen durch Rentenversicherungsträger an Krankenkassen

Mehrere Rentner, die freiwillig bei gesetzlichen Krankenkassen versichert sind, haben sich mit Eingaben an mich gewandt und bemängelt, dass ihr Rentenversicherungsträger ihrer Krankenkasse bei Änderungen der Rentenhöhe ohne ihre vorherige Zustimmung automatisch die neue Rentenhöhe mitgeteilt hat. Selbst eine vorherige Information über diese automatisierte Datenübermittlung sei nicht erfolgt.

Der AOK-Bundesverband, der in dieser Angelegenheit die Spitzenverbände der Sozialversicherung vertritt, hat mir auf eine entsprechende Anfrage hin nachvollziehbar erläutert, der automatisierte Datenaustausch sei mit erheblichen Vorteilen sowohl für die Renten- und Kranken-

versicherungsträger als auch für die – ohnehin auskunftspflichtigen – betroffenen Rentner verbunden. Vor dessen Einführung mussten die Krankenkassen regelmäßig die freiwillig krankenversicherten Rentner nach der aktuellen Höhe ihrer Rente befragen. Aufgrund deren Auskunft wurde ihnen dann eine Bescheinigung über die zu zahlenden Krankenversicherungsbeiträge übersandt und der Rentner musste anschließend gegebenenfalls selbst eine Anpassung des ihm zustehenden Beitragszuschusses bei seinem Rentenversicherungsträger beantragen. Durch den automatisierten Datenaustausch müssen die Krankenkassen kein aufwendiges System für die Nachfrage bei den Rentnern und die Überwachung der Antwort mehr vorhalten; den Rentnern wird erspart, eine Anfrage der Krankenkasse zu beantworten, die Beitragsbescheinigung abzuwarten und sich selbst um die Anpassung des Beitragszuschusses zu kümmern.

Obwohl die Vorteile des unmittelbaren Datenaustauschs zwischen Renten- und Krankenversicherungsträgern für alle Beteiligten nicht zu bestreiten sind, habe ich Zweifel, ob die vom AOK-Bundesverband insoweit angeführte Vorschrift des § 201 Abs. 4 SGB V eine eindeutige und damit ausreichende Rechtsgrundlage für dieses Verfahren ist. Ich habe deshalb das BMG gebeten, durch eine klarstellende Änderung des § 201 SGB V Rechtssicherheit für die Beteiligten zu schaffen; dieses Anliegen wird auch vom AOK-Bundesverband mitgetragen.

Im übrigen wäre der bei einigen Rentnern entstandene Unmut wohl zu vermeiden gewesen, wenn eine rechtzeitige und vollständige Information der Betroffenen über das neue Verfahren Transparenz geschaffen hätte.

19.3 Datenschutzbeauftragte bei Sozialleistungsträgern

Sozialleistungsträger müssen einen internen Datenschutzbeauftragten bestellen. Er unterstützt die Geschäftsführung bei der Sicherstellung des Datenschutzes und ist Ansprechpartner für Mitarbeiter. Das Gesetz gibt ihm eine starke Stellung, die von fachlicher Weisungsfreiheit, Verschwiegenheitspflicht, Abberufungsschutz und unmittelbarer Unterstellung unter dem Vorstand gekennzeichnet ist (§ 81 Abs. 4 SGB X in Verbindung mit §§ 36, 37 Abs. 1 BDSG).

Schon vor zwei Jahren hatte ich die Bahnbetriebskrankenkasse kritisiert, weil der dem internen Datenschutzbeauftragten zur Verfügung stehende Zeitanteil nicht dem Arbeitsanfall im Bereich Datenschutz entsprach. Mit Blick auf die Anzahl der Versicherten hatte ich deshalb gefordert, die Arbeitskapazität des Datenschutzbeauftragten vollständig für seine Aufgaben nach § 81 SGB X in Verbindung mit § 37 Abs. 1 BDSG freizuhalten und ihm ggf. auch personelle Unterstützung zu gewähren (vgl. 17. TB Nr. 21.4).

Die Bahnbetriebskrankenkasse hat zwischenzeitlich einen hauptamtlichen Datenschutzbeauftragten bestellt.

Ich verkenne nicht, dass ein interner Datenschutzbeauftragter allein mit den Aufgaben eines Datenschutzbeauftragten nicht immer voll ausgelastet ist. Vor allem bei kleineren Sozialleistungsträgern kann es angebracht sein, ihm weitere Aufgaben zu übertragen, solange seine Aufgaben als Datenschutzbeauftragter dabei nicht zu kurz kommen und Interessenskonflikte vermieden werden.

Nicht selten ist auch eine Lösung anzutreffen, bei der die Funktion des Datenschutzbeauftragten einer vorstandsnahen Führungskraft formal übertragen ist, die tatsächlichen Aufgaben jedoch von einem seiner Mitarbeiter wahrgenommen werden. Damit wird die gesetzliche Vorgabe unmittelbarer Unterstellung unter den Vorstand formal erfüllt. Problematisch ist bei dieser Lösung jedoch, dass der besondere gesetzliche Schutz des Datenschutzbeauftragten nur für diesen selbst, nicht aber für einen etwa von ihm bestellten Vertreter oder das vom Gesetz sogenannte „Hilfspersonal“ gilt. Die Aufgabenteilung zwischen dem förmlich bestellten Datenschutzbeauftragten, der gleich einem Lobbyisten Themen des Datenschutzes lediglich an die Geschäftsführung heranträgt und anderen Mitarbeitern, die die inhaltliche Arbeit des Datenschutzbeauftragten wahrnehmen, hat zur Folge, dass für diese Mitarbeiter die **besondere** Verschwiegenheitspflicht über die Identität von Betroffenen, der Abberufungsschutz und die fachliche Weisungsfreiheit nicht gelten. Auch das Recht, sich in Zweifelsfällen an die externe Datenschutzkontrollinstanz zu wenden, räumt das Gesetz nur dem Beauftragten für den Datenschutz selbst ein. Die Entscheidung, einen solchen Schritt zu gehen, wird bei einer leitungsnahen Führungskraft von der nachvollziehbaren Zurückhaltung, Interna nach außen zu tragen, begleitet sein. Auch die Einräumung des unmittelbaren Vorspracherechts gegenüber dem Vorstand oder dem Geschäftsführer eines Sozialleistungsträgers ist nach der Rechtslage dem formal bestellten Datenschutzbeauftragten vorbehalten.

Bei der BA musste ich u. a. feststellen, dass den Mitarbeitern der Personalabteilung in der Hauptstelle, die für die Führung der Personalakten zuständig sind, der interne Datenschutzbeauftragte sowie dessen Mitarbeiter überhaupt nicht bekannt waren. Nach eigenen Angaben wurden sie von Kollegen aus dem Personalreferat oder in ihrer Ausbildung auf die besondere Schutzwürdigkeit von Personaldaten hingewiesen. Das mir vorliegende Organigramm der Hauptstelle der BA enthält ebenfalls keinen Hinweis auf den Datenschutzbeauftragten der Bundesanstalt für Arbeit.

Ich habe die BA um Mitteilung gebeten, welche Maßnahmen sie zur Umsetzung der Vorgaben des § 81 Abs. 4 SGB X in Verbindung mit §§ 36, 37 Abs. 1 BDSG treffen wird. Beratungsgespräche hierzu haben zwischenzeitlich stattgefunden und werden fortgesetzt.

Bei der Bundesversicherungsanstalt für Angestellte (BfA) ist es beispielsweise seit Jahren Praxis, dass ein Abteilungsleiter der förmlich bestellte Datenschutzbeauftragte ist, während die mit dieser Funktion verbundene Arbeit vom Datenschutzreferat der BfA wahrgenommen wird.

Aufgrund der unterschiedlichen Erfahrungen in der Praxis neige ich der Auffassung zu, dass bei größeren Sozialleistungsträgern der förmlich bestellte Datenschutzbeauftragte diese Aufgabe auch wahrnehmen sollte. Es dürfte

der Vorstellung des Gesetzgebers auch wenig entsprechen, wenn der interne Datenschutzbeauftragte in Personalunion weitere datenschutzfremde Aufgaben hätte und deswegen die eigentlichen Angelegenheiten des Datenschutzes auf „Hilfspersonal“ übertragen müsste.

19.4 Diskretion auch beim BAföG-Antrag

Ein Petent bat um meine Unterstützung bei seiner Auseinandersetzung mit dem Studentenwerk. Er wollte verhindern, dass detaillierte Angaben über seine persönlichen Verhältnisse, die er zur Neuberechnung von Sozialleistungen nach dem Bundesausbildungsförderungsgesetz (BAföG) für seinen Sohn machen musste, diesem bekannt werden. Seine vorgetragenen Gründe dafür waren nachvollziehbar und überzeugend. Das Formular der Neuberechnung sah so viel Diskretion aber nicht vor, obwohl das Problem im Prinzip schon länger erkannt und sinnvoll gelöst war.

Bei dem normalen Antrag auf BAföG-Leistungen („Erklärung“ nach Formblatt 3/98) enthält das Formblatt nämlich den folgenden Hinweis für die Unterhaltspflichtigen der Auszubildenden: *„Diese Erklärung kann dem Amt auch getrennt vom Antrag der/des Auszubildenden übersandt werden. Sollen Angaben über das Einkommen nicht in den Bewilligungsbescheid aufgenommen werden, teilen Sie dies bitte dem Amt für Ausbildungsförderung unter Angabe von Gründen schriftlich mit.“*

Weil eine solche Möglichkeit auf dem Formular für die Neuberechnung nicht vorgedruckt war, bestand das Studentenwerk darauf, dass dem Studenten nicht nur die persönlichen Angaben des Vaters aus dem Änderungsantrag zur Prüfung, sondern darüber hinaus – zum Vergleich – auch noch die Angaben aus der früheren Erklärung nach Formblatt 3/98 zu überlassen seien. Und obwohl der Unterhaltsverpflichtete (Vater) einsichtige Gründe für sein Verhalten, das ihm in dem vorangegangenen Antrag 3/98 zugebilligt war, vortrug, lehnte das Amt die weitere Bearbeitung ab.

Ich habe daraufhin gegenüber dem für BAföG-Regelungen zuständigen Bundesministerium für Bildung und Forschung (BMBF) auf die unterschiedliche und widersprüchliche Berücksichtigung persönlicher Belange in den Vordrucken 3/98 und 7/98 hingewiesen. Das BMBF teilte meine Auffassung, dass die unterschiedliche Behandlung des Unterhaltsverpflichteten unvereinbar mit der in § 50 Absatz 2 Satz 3 BAföG eröffneten Möglichkeit der Diskretion sei. Es setzte sich unverzüglich mit dem zuständigen Landesministerium in Verbindung, welches das Studentenwerk anwies, die geänderten Einkommensdaten direkt beim Petenten zu erheben. Zur Klarstellung für den Verwaltungsvollzug soll der Vordruck entsprechend geändert werden.

Der Vorgang verdeutlicht, dass trotz datenschutzgerechter Grundsatzregelung Mängel beim Verwaltungsvollzug auftreten können. Dabei wirken Mängel auf Formblättern oder Vordrucken besonders nachhaltig, weil die Berücksichtigung schutzwürdiger Belange nicht nur in einem Einzelfall unterbleibt, sondern bei allen Nutzungen dieses Formblatts. Denn die ausführenden Ämter bearbeiten die Anträge strikt nach den – von höherer Stelle – vorgeschriebenen Formblättern. Vordrucke von Behörden erheben – aufgrund ihres amtlichen Charakters – von sich aus den Anspruch der Richtigkeit, die vom Bürger „vor Ort“ nur schwer in Zweifel gezogen werden kann.

Wie der Sachverhalt zeigt, sollten Bürger bei Bedenken die Richtigkeit auch von amtlich vorgeschriebenen Formblättern hinterfragen und ihr Recht auf Datenschutz in Anspruch nehmen, wenn sie sich in ihren schutzwürdigen Belangen beeinträchtigt fühlen.

In diesem Zusammenhang begrüße ich die Initiative des BMBF, über die schnelle Reaktion im Einzelfall hinaus auch alle anderen beim BAföG verwendeten Formblätter – in Zusammenarbeit mit den ausführenden Ländern und unter meiner Beteiligung – auf datenschutzgerechte Fassung zu überprüfen.

20 Arbeitsverwaltung

20.1 Weitgehende Kontrollmöglichkeiten der Arbeitsämter wegen Leistungsmissbrauchs

Einen Schwerpunkt bei Eingaben aus dem Bereich der Arbeitsverwaltung bildeten im Berichtszeitraum Fragen zu den Kompetenzen der Arbeitsämter bei Außenprüfungen nach den §§ 304 ff. SGB III, 107 SGB IV zur Bekämpfung von Leistungsmissbrauch und illegaler Beschäftigung. Danach ist es Aufgabe der Arbeits- und Hauptzollämter zu prüfen, ob

- Sozialleistungen zu Unrecht bezogen wurden,
- ausländische Arbeitnehmer ohne die erforderliche Arbeitserlaubnis oder zu ungünstigeren Bedingungen als deutsche Arbeitnehmer beschäftigt werden,
- Angaben des Arbeitsgebers, die für Sozialleistungen erforderlich sind, zutreffend bescheinigt werden,

  oder

- der Arbeitgeber seinen Meldepflichten gegenüber der Einzugsstelle für die Sozialversicherung nachgekommen ist.

Zur Durchführung dieser Aufgabe hat der Gesetzgeber den Arbeits- und Hauptzollämtern (zur Außenprüfung durch ein Hauptzollamt s. o. Nr. 7.8) Befugnisse erteilt, die tief in die Grundrechte der Bürger eingreifen. Dazu gehören weitgehende Betretungs- und Prüfungsrechte nach § 305 SGB III sowie nach § 306 SGB III Duldungs- und Mitwirkungspflichten von Arbeitgebern, Arbeitnehmern und jedem Dritten, der bei einer Außenprüfung angetroffen wird. Im Gegensatz zu Ermittlungen der Staatsanwaltschaft, bei denen nach § 152 Abs. 2 StPO *„zureichende tatsächliche Anhaltspunkte“* für eine

Straftat vorliegen müssen, bevor sie ihre Ermittlungen aufzunehmen hat, ist die Außenprüfung der Arbeits- und Hauptzollämter völlig unabhängig davon zulässig, ob überhaupt ein Verdacht auf das Vorliegen einer rechtswidrigen Handlung eines Arbeitgebers bzw. eines Arbeitnehmers besteht. Als Arbeitgeber im Sinne dieser Vorschriften gilt dabei auch ein Auftraggeber, der Selbständige (z. B. auf Honorarbasis tätige Dozenten, freiberufliche Vermögensberater oder Versicherungsvermittler) beauftragt hat.

Tatsächlich dienen die Datenerhebungen zu Beginn einer Außenprüfung in der Regel dazu, Anhaltspunkte für das Vorliegen von Leistungsmissbrauch, illegaler Beschäftigung oder der Verletzung von sozialrechtlichen Meldepflichten zu finden, denen dann im Rahmen der weiteren Prüfung im einzelnen nachgegangen werden kann. Erhoben werden daher von den mit der Außenprüfung beauftragten Beamten nicht nur personenbezogene Daten von Bürgern, die im Verdacht stehen, gegen Bestimmungen des Sozialgesetzbuches verstoßen zu haben, sondern – in weitaus größerem Umfang – personenbezogene Daten unbescholtener Bürger, deren Unschuld erst durch die vorgenommenen Datenabgleiche nachgewiesen wird.

Außenprüfungen nach den §§ 304 ff. SGB III, 107 SGB IV werden überwiegend auf Baustellen vorgenommen. In solchen Fällen ergehen die notwendigen Prüfungsverfügungen mündlich. Datenschutzrechtlich von Bedeutung ist, dass die erhobenen Daten in der Regel nur dann gespeichert und weiterverarbeitet werden, wenn sich bei der Erhebung die Relevanz der Daten für ein weiteres Tätigwerden der Kontrollbehörde herausstellt, etwa weil sich der Verdacht einer rechtswidrigen Tat ergeben hat.

Zahlreiche Unternehmen haben sich an mich gewandt, von denen die Arbeitsverwaltung eine Auflistung der dort auf Honorarbasis tätigen Auftragnehmer anforderte, um festzustellen, ob Personen, die Sozialleistungen beziehen, freiberuflich tätig sind und möglicherweise Einnahmen beim Arbeitsamt nicht angeben. In diesen Fällen erhebt und speichert die Kontrollbehörde zunächst eine Vielzahl personenbezogener Daten, deren Relevanz für ein weiteres Tätigwerden des Arbeits- oder Hauptzollamtes erst später geprüft wird. Den Petenten musste ich mitteilen, dass ich zwar Verständnis für ihr Unbehagen habe, dem Arbeitsamt Listen in maschinell auswertbarer Form mit personenbezogenen Daten ihrer Auftragnehmer zu übergeben – in einem Fall betraf dies mehrere tausend Auftragnehmer, von denen möglicherweise nur wenige oder gar keine gleichzeitig Arbeitslosenhilfe und Honorar aus freiberuflicher Tätigkeit bezogen –, dass die gesetzlichen Bestimmungen dieses Vorgehen der Arbeitsämter aber grundsätzlich zulassen.

Allerdings habe ich mich gegen die vom jeweiligen Arbeitsamt auf der Basis einer Musterprüfungsverfügung erlassene umfassende Prüfungsverfügung gewandt, mit der die Außenprüfung begonnen wurde. Dabei richten sich meine Bedenken gegen die inhaltliche Unbestimmtheit der Musterprüfungsverfügung. Ich teile die Auffassung der hierzu ergangenen Rechtsprechung, dass der besonderen Gefährdung des Rechts auf informationelle Selbstbestimmung in diesem Bereich durch den Einsatz der automatischen Datenverarbeitung durch darauf bezogene rechtliche Vorkehrungen begegnet werden muss. Dies gilt vor allem unter Berücksichtigung der weitgehenden Kontrollkompetenzen von Arbeits- und Hauptzollämtern bei der verdachtslosen Prüfung. Nur bei ausreichenden Vorkehrungen zum Datenschutz halte ich daher entsprechende Regelungen für verfassungsgemäß. Je unbestimmter die gesetzlichen Regelungen sind und mit Rücksicht auf den Normzweck und die Eigenart des zu regelnden Sachverhalts auch sein dürfen, um so erforderlicher muss der Schutz des Rechts auf informationelle Selbstbestimmung durch die Bestimmtheit der Regelung des Einzelfalls durch Verwaltungsakt sein. Das Arbeits- oder Hauptzollamt hat daher schon in der schriftlichen Prüfungsanordnung alle Regelungen zu treffen, die möglich sind, ohne den Prüfungszweck zu gefährden. Insbesondere hat es sich vor Erlass der Prüfungsverfügung über den Umfang der Außenprüfung klar zu werden und zunächst nur die Daten zu erheben, die erforderlich sind, um Personen herauszufiltern, bei denen der Verdacht von Leistungsmissbrauch oder illegaler Beschäftigung besteht.

In den o. g. Fällen, in denen sich Unternehmen an mich gewandt hatten, habe ich erreicht, dass die jeweiligen Arbeitsämter ihre Prüfungsverfügung soweit konkretisiert haben, dass einerseits die Datenerhebung auf das erforderliche Maß beschränkt blieb und andererseits der Kontrollauftrag des Arbeitsamtes nicht gefährdet wurde.

Da sich damit gezeigt hatte, dass die Prüfungsverfügung des Arbeitsamts datenschutzgerecht formuliert werden kann, habe ich der BA empfohlen, die in den mit dem BMF herausgegebenen Gemeinsamen Richtlinien für den Außendienst abgedruckte Musterprüfungsverfügung den rechtsstaatlichen Erfordernissen anzupassen. Die mit der Hausleitung der BA geführten Gespräche verliefen erfolgversprechend, weil von allen Seiten die Notwendigkeit der gesetzlichen Regelungen zur Bekämpfung von Leistungsmissbrauch und illegaler Beschäftigung bejaht und eine Lösung gefunden wurde, die sowohl dem Persönlichkeitsrecht des einzelnen als auch dem Kontrollzweck der gesetzlichen Regelungen gerecht wurde. Es kommt nunmehr darauf an, auch auf Arbeitsebene die rechtsstaatlich erforderliche Anpassung der von den Arbeits- und Hauptzollämtern benutzten Musterprüfungsordnung zu erreichen.

20.2 Post vom Arbeitsamt

20.2.1 Kundennummer im Sichtfenster

Immer wieder wenden sich Petenten an mich, weil sie es für datenschutzrechtlich bedenklich halten, dass Arbeitsämter in ihren Briefen neben den Adressdaten auch die Kundennummer im Anschriftenfeld (Sichtfenster) angeben.

Die BA hat mir hierzu mitgeteilt, dass jeder Kunde, unabhängig davon, ob er Leistungen beansprucht, eine

Kundennummer erhält. Die Kundennummer setzt sich zusammen aus der Arbeitsamtsnummer und einer Ordnungsnummer, die maschinell vergeben wird. Es ist nicht möglich, aus der Kundennummer auf persönliche Daten des Betroffenen zu schließen. So können insbesondere auch keine Rückschlüsse gezogen werden, ob und ggf. welche Leistungen beansprucht bzw. gezahlt werden.

Aufgrund der Vorausverfügung auf den Briefumschlägen der Arbeitsämter werden Poststücke, die nicht zustellbar sind, weil der Kunde unter der angegebenen Adresse nicht mehr erreichbar ist, nicht an das Arbeitsamt zurückgesandt, sondern bei wirksamem Nachsendeantrag an den Kunden weitergeleitet. Das Arbeitsamt erhält in diesem Fall eine sogenannte Anschriftenberichtigungskarte mit der neuen Anschrift und – zur Erleichterung der Zuordnung im Arbeitsamt – der Kundennummer des Adressaten. Diese aus Sicht der Arbeitsverwaltung kundenfreundliche und kostensparende Handlungsweise erfordert die Angabe der Kundennummer im Anschriftenfeld. Die Zuordnung der Anschriftenberichtigungskarte im Arbeitsamt wäre anderenfalls deutlich erschwert und bisweilen sogar unmöglich.

Diese Verfahrensweise ist datenschutzrechtlich nicht zu beanstanden. Die Kundennummer ist „nicht sprechend“, d. h. sie lässt keine Rückschlüsse auf die Sozialdaten des betreffenden Kunden zu. Die Befürchtung einiger Petenten, das Arbeitsamt könne aufgrund der Angabe einer dem Sichtfenster eines Briefes entnommenen fremden Kundennummer unzulässigerweise an Außenstehende Informationen weitergeben, halte ich nahezu für ausgeschlossen. Denn das von der BA in einem Runderlass geregelte Verfahren der Auskunftserteilung sieht vor, dass sowohl Betroffene als auch Dritte, soweit an diese eine Übermittlung nach dem Sozialgesetzbuch zulässig ist, ihre Identität vor einer Auskunftserteilung ausreichend nachzuweisen haben. So hat sich der auskunftserteilende Mitarbeiter auch bei telefonischen Anfragen stets zu vergewissern, ob der Anrufer selbst zum Empfang der Auskunft berechtigt ist. Dies kann durch gezielte Fragen aber auch durch einen Rückruf erfolgen. Bei Zweifeln an der Identität des Anrufenden sind die Mitarbeiter der Arbeitsämter angewiesen, die Auskunft zunächst zu verweigern und dem Anrufer anheim zu stellen, persönlich vorzusprechen oder sein Anliegen schriftlich vorzutragen. Allein die Angabe der Kundennummer berechtigt jedenfalls nicht, Auskünfte zu erhalten.

Auch die Gefahr, dass ein Dritter, der über die Kundennummer hinaus bereits einige Kenntnisse über einen Kunden des Arbeitsamtes hat, zusätzliche Sozialdaten ausforschen kann, erscheint mir gering. Das von Petenten geforderte Verbot der Angabe der Kundennummer im Anschriftenfeld halte ich aus datenschutzrechtlicher Sicht daher nicht für erforderlich. Auch beim Schutz des Persönlichkeitsrechts ist ein angemessenes Verhältnis zwischen dem angestrebten Schutzzweck einer Maßnahme und dem damit einhergehenden Aufwand zu berücksichtigen. Die BA benötigt die Angabe der Kundennummer im Sichtfenster von Briefumschlägen, um – wie oben beschrieben – ein kundenfreundliches, kostensparendes und der Arbeitserleichterung dienendes Nachsendeverfahren durchführen zu können. Würde die Kundennummer nicht im Sichtfenster angegeben, ließe sich dieses Verfahren nicht mehr durchführen. Der zusätzliche Schutz von Sozialdaten durch den Verzicht auf Angabe der Kundennummer im Anschriftenfeld wäre – wenn es ihn denn überhaupt gäbe – sehr gering.

Ich teile die Auffassung der BA, dass die Angabe der Kundennummer im Sichtfenster von Briefumschlägen keinen Verstoß gegen das Sozialgeheimnis darstellt.

20.2.2 Post für einen anderen Kunden

Daneben haben sich Petenten an mich gewandt, weil Ihnen gemeinsam mit dem für sie bestimmten Schriftstück in demselben Umschlag ein weiteres für einen anderen Kunden des Arbeitsamtes bestimmtes Schreiben zugestellt wurde.

Nach Darstellung der BA wurden die für unterschiedliche Empfänger bestimmten Schreiben in diesen Fällen versehentlich gemeinsam kuvertiert und versandt. Da die BA hierbei von bedauerlichen Einzelfällen ausging, habe ich mir den Verfahrensablauf beim Postversand sowohl bei einem großen Arbeitsamt (einschließlich Geschäftsstelle) als auch direkt bei der Hauptstelle der BA angesehen. Einen Verstoß gegen datenschutzrechtliche Vorschriften konnte ich dabei nicht feststellen. Dass bei dem im Bereich der Arbeitsverwaltung in großem Umfang anfallenden Schriftverkehr versehentlich einmal Schreiben falsch kuvertiert und versandt werden, halte ich zwar für bedenklich, andererseits wird sich für den Postversand jedoch kein Verfahren finden lassen, das mit absoluter Sicherheit jeden menschlichen wie maschinellen Fehler ausschließt. Betrachtet man die geringe Anzahl der tatsächlich unzutreffend kuvertierten Schreiben im Verhältnis zu dem außerordentlich umfangreichen Schriftverkehr der Arbeitsämter, so lässt dies den Schluss zu, dass die für den Postversand verantwortlichen Mitarbeiter ihrer Sorgfaltspflicht nachkommen.

Aufgrund der im Rahmen der Kontrollbesuche gewonnenen Erfahrungen kann ich die Auffassung der BA bestätigen, dass es sich bei den genannten Fehlzustellungen tatsächlich um bedauerliche Einzelfälle handelt.

20.3 Arbeitsamt 2000 – ein schwieriges Projekt

Bereits in meinem 16. Tätigkeitsbericht (Nr. 20.4) hatte ich auf das unter der Bezeichnung „Arbeitsamt 2000“ entwickelte Konzept der BA aufmerksam gemacht, das unter anderem den Wegfall der traditionellen Abteilungsstruktur vorsieht. Die Kunden können ihre Angelegenheiten danach bei einem einzigen Arbeitsamtsmitarbeiter erledigen, unabhängig davon, ob es um Arbeitsvermittlung, Berufsberatung, berufliche Fortbildung oder den Bezug von Leistungen geht. Die BA erhofft sich dadurch mehr Kundenfreundlichkeit, wenn künftig „nicht mehr die Menschen, sondern die Daten laufen“ und infolgedessen Wartezeiten verkürzt werden können.

Die Neuorganisation umfasst auch die Gestaltung der Innenbereiche der Dienstgebäude. So werden in den Arbeitsämtern große, offene, gut überschaubare, häufig nur durch Stellwände voneinander abgetrennte Kundenbereiche (Clearing-Stellen) eingerichtet. Aus mehreren datenschutzrechtlichen Eingaben ist jedoch ersichtlich, dass die Kunden die Umgestaltung zu sog. Thekenlösungen nicht immer für kundenfreundlich halten. So finden viele es äußerst unangenehm und sie fühlen sich in ihrem Recht auf informationelle Selbstbestimmung verletzt, wenn ihre Gespräche mit den Arbeitsamtsmitarbeitern aufgrund der offenen räumlichen Gestaltung häufig gar nicht anders geführt werden können, als dass Sozialdaten von anderen Kunden mitgehört werden.

Der bei diesem Projekt im Vordergrund stehende Servicegedanke darf nicht dazu führen, dass das Sozialgeheimnis nach § 35 SGB I „auf der Strecke bleibt", weil ein angemessener Schutz der personenbezogenen Daten nicht mehr gewährleistet ist. Ich habe die BA daher aufgefordert, geeignete Vorkehrungen zu treffen, damit das unbefugte Mithören von Sozialdaten im „Arbeitsamt 2000" künftig kein Thema mehr ist.

Dementsprechend wird jetzt versucht, durch geeignete Möblierung und raumgestalterische Maßnahmen (Diskretionszonen, Trennwände usw.) den Anforderungen des Datenschutzes Rechnung zu tragen. Darüber hinaus werden an den Clearing-Stellen nur Kurzanliegen (Abgabe von Anträgen bzw. Bescheinigungen u. ä.) bearbeitet; umfangreichere Beratungen werden weiterhin in Kundenbüros durchgeführt.

Bei einem Kontroll- und Beratungsbesuch eines bereits neu gestalteten Arbeitsamtes habe ich feststellen müssen, dass ein „Arbeitsamt 2000" – was die unberechtigte Kenntnisnahme personenbezogener Daten im Kundenbereich anbelangt – trotz dieser Maßnahmen kein vergleichbar hohes Datenschutzniveau bietet wie ein herkömmliches Arbeitsamt mit geschlossenen Büroräumen. Das Mithören der Gespräche wird teilweise zwar erschwert, leider reichen die Maßnahmen jedoch nicht aus, um die Kenntnisnahme durch Dritte immer zu verhindern.

Letztlich kann ich die Neuorganisation der Arbeitsämter aus datenschutzrechtlicher Sicht aber mittragen, weil den Kunden auch weiterhin die Möglichkeit geboten wird, ihr Anliegen auf Wunsch in einem Büro vorzutragen. Dadurch dass der Kunde durch Hinweisschilder auf diese datenschutzgerechte Möglichkeit der Klärung seines Anliegens aufmerksam gemacht wird, kann er selbst entscheiden, ob die Thekenlösung seinem Anspruch an den Datenschutz gerecht wird.

Die BA hat sich u. a. für die Umgestaltung ihrer Dienststellen entschieden, weil sie der Ansicht ist, Kundenfreundlichkeit zeichne sich durch kürzere Wartezeiten und mehr Service aus. Ob die Kunden dies genauso sehen, wird sich auch daran messen lassen, wie häufig sie sich stattdessen für mehr Datenschutz entscheiden.

20.4 Beurteilung von Arbeitsuchenden bei Fortbildungs- und Trainingsmaßnahmen

Die Arbeitsämter bieten ihren Kunden eine Reihe von Maßnahmen an, um deren Chancen zur Wiedereingliederung in das Berufsleben zu erleichtern. Bei diesen Maßnahmen handelt es sich um

- Trainingsmaßnahmen nach §§ 48 ff. SGB III,
- Maßnahmen zur Förderung der beruflichen Weiterbildung nach §§ 77 ff. SGB III

  und
- berufsvorbereitende Bildungsmaßnahmen nach §§ 61 ff. SGB III.

Zunehmend lassen die Arbeitsämter die Arbeitslosen von Maßnahmeträgern hinsichtlich des individuellen Erfolges einer Maßnahme beurteilen, was zu einem deutlichen Anstieg der Anzahl der Eingaben führte. In einem Fall war die Beurteilung der Teilnahme an einer vom Arbeitsamt veranlassten Maßnahme sogar in Form eines psychologischen Gutachtens erfolgt.

Bei den Maßnahmen handelt es sich um Sachleistungen der BA an bestimmte Kundenkreise. Die Beurteilung der Kunden erfolgt im Auftrag des jeweiligen Arbeitsamtes. Das Arbeitsamt benötigt die Beurteilungen, um die betreffenden Kunden leistungs- und eignungsgerecht in Arbeit oder Berufsausbildung vermitteln zu können. Soweit von den Trägern ausschließlich vermittlungsrelevante Angaben übermittelt werden, habe ich an deren Erforderlichkeit keine Zweifel. Ich habe die BA jedoch darauf hingewiesen, dass es an einer rechtlich einwandfreien Regelung für die Erstellung der Beurteilung durch den Maßnahmeträger und deren Übermittlung an das Arbeitsamt mangelt. Denn die bestehenden gesetzlichen Regelungen sind hierfür nicht ausreichend:

- bei den Trainingsmaßnahmen sieht § 48 Abs. 3 SGB III lediglich eine **Bescheinigung über die Teilnahme** an einer solchen Maßnahme für den Arbeitslosen vor, aus der sich mindestens Art und Inhalt der Maßnahme ergeben,
- bei den Maßnahmen zur Förderung der beruflichen Weiterbildung nach den §§ 77 ff. SGB III wird ein Maßnahmeträger u. a. nur dann vom Arbeitsamt für eine Weiterbildungsmaßnahme anerkannt, wenn die Maßnahme mit einem **Zeugnis** abschließt, das **Auskunft über den vermittelten Lehrstoff** gibt (§ 86 Abs. 1 Nr. 6 SGB III). Nach § 93 Abs. 1 Satz 2 Nr. 1 SGB III kann das Arbeitsamt von dem Träger der Maßnahme und den Teilnehmern Auskunft über den Verlauf der Maßnahme und den Eingliederungserfolg verlangen,
- bei den berufsvorbereitenden Bildungsmaßnahmen nach §§ 61 ff. SGB III, die sich an Jugendliche und junge Erwachsene ohne berufliche Erstqualifikation richten, fehlt es völlig an gesetzlichen Regelungen für

die Beurteilung der betroffenen Kunden des Arbeitsamtes.

Lediglich aus den die Maßnahmen betreffenden Runderlassen der BA sind an verschiedenen Stellen Hinweise zu entnehmen, dass die Beurteilung der Teilnehmer ein wesentlicher Bestandteil der jeweiligen Maßnahme ist. Bei der Beurteilung der Arbeitslosen durch die Maßnahmeträger, die sich auch auf deren Sozialverhalten bezieht, sind die entsprechenden Runderlasse nicht durch gesetzliche Vorschriften gedeckt.

Da durch die Beurteilung tief in das Persönlichkeitsrecht des betroffenen Arbeits- bzw. Ausbildungssuchenden eingegriffen wird, halte ich eine gesetzliche Regelung für unerlässlich. Das derzeitige Vorgehen der Arbeitsämter kann daher nur deshalb vorübergehend hingenommen werden,

- weil der Arbeitslose im Rahmen eines Erklärungsbogens, der vor der Teilnahme an einer Maßnahme auszufüllen ist, unterschreibt, dass ihm bekannt ist, dass Zeugnisse/Beurteilungen und für die Arbeitsvermittlung oder die Gewährung von Leistungen notwendige Mitteilungen vom Träger der Trainingsmaßnahme im erforderlichen Umfang an das Arbeitsamt weitergeleitet werden,

und

- dem Arbeitsuchenden ein Merkblatt aushändigt wird, in dem u. a. auf die Möglichkeit der Beurteilung hingewiesen wird. Die Übergabe des Merkblattes ist vom Arbeitsuchenden zu quittieren.

Diese Einwilligungsregelung kann jedoch nur als Übergangslösung bis zu einer gesetzlichen Regelung angesehen werden. Lehnt ein Arbeitsloser die Maßnahme ab, weil er nicht bereit ist, seine Einwilligung zur Erstellung und Übermittlung einer Beurteilung zu geben, kann dies leistungsrechtliche Folgen für ihn haben. Da dies die Freiwilligkeit seiner Einwilligung in Frage stellt, habe ich mit der BA vereinbart, dass ein Arbeitsuchender derzeit die Beurteilung folgenlos ablehnen kann.

Die notwendige gesetzliche Regelung habe ich gegenüber dem BMA angeregt. Eine Stellungnahme hierzu steht noch aus.

20.5 Löschungs- und Berichtigungsrechte eingeschränkt?

In vielen Fällen wenden sich Petenten an mich, weil sie der Meinung sind, ihr zuständiges Arbeitsamt speichere falsche oder aber für dessen rechtmäßige Aufgabenerfüllung nicht (mehr) relevante Daten über sie. Stellt sich im Rahmen der datenschutzrechtlichen Prüfung heraus, dass die – insbesondere in den computergestützten Beratungsvermerken – gespeicherten Daten tatsächlich unzutreffend oder für die Aufgabenerledigung nicht bzw. nicht mehr erforderlich sind, hat der Kunde nach § 84 SGB X einen Anspruch auf Berichtigung bzw. Löschung dieser Daten.

Auf diesen Rechtsanspruch ihrer Kunden hingewiesen, teilte mir die BA mit, dass es nicht möglich sei, *einzelne Daten* aus den Beratungsvermerken zu entfernen oder diese zu berichtigen. Sei der Inhalt eines Beratungsvermerks zu ändern, müsse der *gesamte Datensatz* gelöscht und anschließend in berichtigter Form neu eingegeben werden. Diese Regelung sei bewusst getroffen worden, um sicherzustellen, dass im nachhinein keine manipulierenden Veränderungen vorgenommen werden könnten.

Da die Beratungsvermerke grundsätzlich solange gespeichert werden, wie das Arbeitsamt das Bewerberangebot führt, kann der Datensatz – gerade bei Langzeitarbeitslosen – unter Umständen sehr umfangreich sein. Entsprechend arbeitsaufwendig kann sich die Neueingabe eines kompletten Datensatzes in berichtigter Form gestalten. Aus diesem Grund haben sich die Arbeitsämter bisher häufig geweigert, datenschutzrechtlich zu beanstandende Beratungsvermerke zu berichtigen.

Ich habe die BA darauf hingewiesen, dass ich diesen von ihr selbst zu verantwortenden hohen Verwaltungsaufwand nicht als Rechtfertigungsgrund für die Verletzung des Datenschutzrechts akzeptieren kann. Inzwischen hat die BA mir zugesagt, berechtigten Löschungs- und Berichtigungsansprüchen künftig – unabhängig von dem damit verbundenen Aufwand – nachzukommen. In diesem Zusammenhang habe ich angeregt, im Rahmen der ohnehin anstehenden technischen Neugestaltung der computerunterstützten Arbeitsvermittlung (coArb) auch über Möglichkeiten nachzudenken, die die Berichtigung und selektive Löschung einzelner Daten in den Beratungsvermerken vereinfachen würden. Um Manipulationen auszuschließen, müsste dabei gewährleistet sein, dass Änderungen mit Hilfe geeigneter Protokollierungsmaßnahmen zugeordnet werden können.

20.6 Ein folgenschwerer Brief an die Schule

Die Gründe vieler Eingaben, die die BA betreffen, liegen im gespannten Verhältnis vieler Bürger, die in Kontakt mit dem Arbeitsamt kommen, zu den Mitarbeitern des Arbeitsamtes. Dass dies nicht nur Arbeitsuchende betrifft, die persönliche Frustrationen manchmal auf dem Rücken ihres Arbeitsamtsberaters abladen, zeigte eine Eingabe, die mich im Berichtszeitraum erreichte.

Die Mutter eines Schülers der Abschlussklasse einer Hauptschule wandte sich an das örtlich zuständige Arbeitsamt, um die Chancen ihres Sohnes auf einen Ausbildungsplatz zu verbessern. Von dem für ihren Sohn zuständigen Berater des Arbeitsamtes fühlte sie sich jedoch nicht ausreichend unterstützt. Dies gelang erst mit Hilfe eines anderen Beraters. Damit hätte die Geschichte einen guten Abschluss finden können. Datenschutzrechtlich fing sie jedoch erst an.

Über ihre Erfahrungen mit dem Arbeitsamt führte die Mutter ein Gespräch mit dem Klassenlehrer ihres Sohnes und erwähnte dabei auch das ihrer Ansicht nach wenig überzeugende Verhalten des ersten Arbeitsamtsberaters. Über das Gespräch unterrichtete der Klassenlehrer den Arbeitsamtsberater, der sich über das Verhalten der Mut-

ter ärgerte und sich darauf hin in einem Schreiben an den Rektor der Hauptschule und an den Klassenlehrer über das Verhalten der Mutter und die seiner Ansicht nach ungeeignete geistige Leistungsfähigkeit des Schülers äußerte. Hinsichtlich des Verhaltens der Mutter im Arbeitsamt übersandte er der Schule Hardcopies aus dem arbeitsamtsinternen System **COMPAS** (**comp**uterunterstütztes **A**usbildungsvermittlungs**s**ystem), in dem er Gesprächsvermerke mit der Mutter und dem Sohn festgehalten hatte. Wegen der mangelnden Leistungsfähigkeit verwies er auf ein dem Arbeitsamt vorliegendes psychologisches Gutachten. Eine Kopie des Schreibens ließ er der Mutter des Schülers zukommen.

Die Eintragungen im System COMPAS verstießen gegen einen bundesweit geltenden Runderlass der BA, der den zulässigen Inhalt von Beratungsvermerken regelt und über den ich bereits mehrfach berichtet habe (vgl. 15. TB Nr. 11.2; 14. TB S. 85 f., 13. TB S. 63 ff.). Sie waren z.T. unsachlich sowie für die Vermittlung eines Ausbildungsplatzes für den Sohn nicht relevant und wurden mittlerweile im System gelöscht. Das Schreiben an den Rektor und den Klassenlehrer habe ich als gravierenden Verstoß gegen die Wahrung des Sozialgeheimnisses (§ 35 SGB I) und die Übermittlungsregelungen im Sozialgesetzbuch (§§ 67b, 67d, 68 bis 77 SGB X, § 298 SGB III) gewertet.

Auf eine förmliche Beanstandung habe ich jedoch verzichtet, weil es sich um einen inzwischen beseitigten Mangel im Sinne des § 25 Abs. 2 BDSG handelte. Die Vorgesetzten des im übrigen sehr engagierten Arbeitsamtsberaters haben diesen in einem Personalführungsgespräch eindringlich auf den Verstoß gegen das Sozialgeheimnis und die Unzulässigkeit seines Handelns hingewiesen und auch den Fall in anonymisierter Form nochmals zum Anlass genommen, alle Mitarbeiter der Arbeitsverwaltung auf die Einhaltung datenschutzrechtlicher Bestimmungen hinzuweisen.

20.7 Die Arbeitsvermittlung im Internet

Bereits in meinem 16. Tätigkeitsbericht (Nr. 20.2) hatte ich über die Erprobung neuer Wege der Selbstinformation bei der BA berichtet. Seit der Einführung des Arbeitgeber-Informations-Service (AIS), des Stellen-Informations-Service (SIS) und des Ausbildungs-Stellen-Informations-Service (ASIS) hat die BA ihre Online-Vermittlungsangebote, die inzwischen auch im Internet zur Verfügung stehen, kontinuierlich erweitert. So gibt es heute neben einem internationalen Vermittlungsservice auch Angebote für bestimmte Berufsgruppen wie z. B. Hotel- und Gaststättenpersonal oder Künstlerdienste. Darüber hinaus wurde damit begonnen, sog. Vermittlungs**börsen** – wie etwa für IT-Fachkräfte (s. u. Nr. 20.7.2) – einzurichten, bei denen die Nutzer ihre Bewerberangebote selbst auf einer von der BA zur Verfügung gestellten Kommunikationsplattform in das Internet einstellen können.

Die für diese Informationssysteme geltenden datenschutzrechtlichen Vorgaben konkretisiert § 41 Abs. 3 SGB III. So dürfen in die Selbstinformationseinrichtungen nur diejenigen Daten über Ausbildungsuchende, Arbeitsuchende und Arbeitgeber aufgenommen werden, die für die Vermittlung erforderlich sind. Daten, die eine Identifizierung des Betroffenen ermöglichen, dürfen nur mit seiner Einwilligung aufgenommen werden.

20.7.1 Anonymisierung nicht immer erfolgreich!

Die vom Arbeitsamt in den Selbstinformationssystemen vorgenommene Anonymisierung führt offenbar nicht immer zu dem gewünschten Erfolg. So hat sich ein Petent an mich gewandt, weil er – obwohl sein Name nicht genannt und das Angebot aus Sicht des Arbeitsamtes somit anonymisiert war – aufgrund der ansonsten sehr detaillierten Darstellung seiner Bewerberdaten im AIS (Alter, Geschlecht, Wohnort, Berufsausbildung, Weiterbildung, Berufpraxis usw.) entgegen seinem Willen von Dritten identifiziert werden konnte. Dies lag insbesondere daran, dass er in einem kleineren Ort wohnte.

Die BA hat mir hierzu mitgeteilt, dass die im AIS veröffentlichten Daten automatisch aus den für die Vermittlung gespeicherten Bewerberdaten abgerufen werden. Welche Daten zur Veröffentlichung herangezogen werden, ist bei diesem Verfahren einheitlich vorgegeben. Systembedingt ist es daher nicht möglich, auf die Veröffentlichung des Teils der Daten zu verzichten, der in Einzelfällen eine Identifizierung ermöglichen könnte.

In dem mir bekannt gewordenen Fall hat das Arbeitsamt das Bewerberangebot daher vollkommen aus dem AIS herausgenommen. Gleichzeitig hat die BA eine Regelung angekündigt, wonach künftig auch dann, wenn allein durch Weglassen des Namens die Anonymisierung nicht sichergestellt ist, Bewerberangebote datenschutzgerecht in die Selbstinformationseinrichtungen eingestellt werden können. Ich werde die weitere Entwicklung in dieser Angelegenheit verfolgen.

20.7.2 Green Card und andere Vermittlungsbörsen im Internet

Aufgrund einer Absprache der Bundesregierung mit Unternehmensvertretern der Informations- und Kommunikationstechnologie (IuK) bietet die BA seit Mitte 2000 im Internet eine neue Form der Arbeitsvermittlung an: die **„Vermittlungsbörse für in- und ausländische IT-Fachkräfte“**. Die über diesen Weg erreichbare Arbeitserlaubnis ist auch als Green Card bekannt, die zu einer zeitlich befristeten Aufenthalts- und Arbeitserlaubnis für ausländische IT-Fachkräfte führt. Bei dem „Green-Card-Verfahren“ handelt es sich um ein kurzfristig ins Leben gerufenes Verfahren, um den Fachkräftemangel im IuK-Bereich zu beheben.

Hierzu werden bei der Vermittlungsbörse für IT-Fachkräfte im Internet neue Wege beschritten. Der Arbeitsuchende gibt hier selbst die vermittlungsrelevanten Daten (Ausbildung, Arbeitsschwerpunkte, Gehaltsvorstellung usw.) und zusätzlich seine Namen, seine postalische und seine E-Mail-Adresse ein, damit der potenzielle Arbeitgeber direkt ohne Einschaltung der Arbeitsverwaltung Kon-

takt zu ihm aufnehmen kann. Nicht nur ein potenzieller Arbeitgeber, sondern jeder kann – weltweit – anschließend die Bewerberangebote im Internet nachlesen. Auch die Betriebe können ihre Stellengesuche direkt im Internet eingeben. Schließlich gibt es die Option, sich an die Zentralstelle für Arbeitsvermittlung (ZAV) in Bonn zu wenden, die zentral für die Arbeitsvermittlung mit internationalem Bezug zuständig ist. Bei den herkömmlichen Internetangeboten der BA werden dagegen die Eintragungen vom Arbeitsamt vorgenommen. Dies gilt auch für die **„Künstlerdienste“** und die **„Zentrale Bühnen-, Fernseh- und Filmvermittlung (ZBF)“**, in denen die zu vermittelnden Künstler – im Gegensatz zu den übrigen anonymisierten Internetangeboten der BA – mit Namen und Foto abrufbar sind.

Grundsätzliche Bedenken habe ich gegen das von der BA praktizierte Verfahren nicht. Wesentlich für die datenschutzrechtliche Bewertung dieser Vermittlungsbörse ist, dass sie sich an IT-Fachkräfte richtet, bei denen in der Regel davon auszugehen ist, dass sie ihr Recht auf informationelle Selbstbestimmung bewusst ausüben. Allerdings habe ich die BA auf einige datenschutzrechtliche Schwachpunkte hingewiesen, worauf sie in der Folgezeit Verbesserungen vorgenommen hat. So wird den Bewerbern nunmehr die Möglichkeit geboten, sich zunächst anonym um eine Arbeitsstelle in der IT-Branche zu bewerben. Missbrauchsmöglichkeiten begegnet die BA mittlerweile dadurch, dass sie die ZAV damit beauftragt hat, den Datenbestand zu pflegen und offensichtlich unseriöse Angebote aus dem Angebot zu löschen.

Auch bei der **„Vermittlungsbörse für Firmennachfolgen, Kooperationen und Existenzgründungen“** können künftige Arbeitgeber, aber auch potentielle Bewerber eigenständig Angebote in das Internet-Angebot der BA einstellen. Im Gegensatz zur Vermittlungsbörse für IT-Fachkräfte erfolgen die Angebote hier zu einem großen Teil anonym.

Die Entwicklung des Internet-Angebotes der BA werde ich mit Interesse weiterverfolgen, da die BA beabsichtigt, ihre Vermittlungsbörsen in Zukunft auszubauen. So ist u. a. geplant, die bisherigen Verfahren (AIS, SIS, ASIS usw.) dem technischen Fortschritt anzupassen und neu zu gestalten. In diesem Zusammenhang wird beispielsweise daran gedacht, dass künftige Börsen von ihren Nutzern frei gestaltet werden können.

Die BA hat mir zugesagt, mich hinsichtlich der datenschutzgerechten Umsetzung ihrer Planungen zu beteiligen.

20.8 Unzulässiger Datenabgleich zwischen der BA, der IHK und den Handwerkskammern

Weit verbreitet ist die Ansicht, Jugendliche würden Ausbildungsplätze dadurch blockieren, dass sie – obwohl sie bereits einen Ausbildungsvertrag mit einem Ausbildungsbetrieb abgeschlossen haben – weiterhin auf Ausbildungsplatzsuche bleiben, um möglicherweise doch in ihrem Traumjob ausgebildet zu werden. Fänden sie einen „besseren“ Ausbildungsplatz würden viele dieser Jugendlichen erneut einen Ausbildungsvertrag abschließen, ohne den zunächst abgeschlossenen Ausbildungsvertrag zu kündigen oder auch nur dem Arbeitsamt vom Abschluss der Ausbildungsverträge Kenntnis zu geben, so dass sie in der entsprechenden Statistik der Arbeitsverwaltung weiterhin als ausbildungssuchend geführt würden.

Um herauszufinden, ob diese Ansicht richtig ist, war 1997 zwischen dem Deutschen Industrie- und Handelstag (DIHT) und der BA eine Vereinbarung getroffen worden, wonach ab März 1998 regelmäßig Daten über noch nicht vermittelte Bewerber und unbesetzte Ausbildungsstellen bei den Arbeitsämtern mit den eingetragenen Ausbildungsverhältnissen bei den Industrie- und Handelskammern (IHK) abgeglichen werden sollten. Anfang 1998 folgte eine entsprechende Vereinbarung zwischen dem Deutschen Handwerkskammertag und der BA. Darüber hinaus wurden eine Reihe von ähnlichen Vereinbarungen auf regionaler Ebene zwischen einzelnen Landesarbeitsämtern und IHK bzw. Handwerkskammern abgeschlossen. Der Bundesverband der Freien Berufe, der an den vorbereiteten Gesprächen ebenfalls beteiligt war, hatte im Mai 1998 u. a. wegen des hohen Verwaltungsaufwandes und wegen „Datenschutzproblemen“ eine Teilnahme an dem Datenabgleich abgelehnt. In den Monaten März bis September 1998 wurden der Arbeitsverwaltung von den meisten IHK und Handwerkskammern Daten über die bei ihnen eingetragenen Ausbildungsverhältnisse übermittelt und im Zentralamt der BA abgeglichen.

Auf dieses Datenabgleichverfahrens wurde ich durch mehrere LfD aufmerksam gemacht, an die sich einige Kammern gewandt hatten, die datenschutzrechtliche Bedenken wegen der Übermittlung der von ihnen erbetenen Daten über abgeschlossene Ausbildungsverhältnisse an die Arbeitsverwaltung hatten. Rückfragen bei den Kammern, worin diese denn eine Rechtsgrundlage für die Datenübermittlung an die Arbeitsverwaltung zum Zwecke des Datenabgleichs sähen, führten zur Nennung einer Vielzahl von gesetzlichen Bestimmungen, die ebenso wenig wie die oben erwähnten Vereinbarungen zwischen der BA und den Spitzenorganisationen der Kammern geeignet waren, das Datenabgleichverfahren zwischen den Kammern und der Arbeitsverwaltung zu rechtfertigen. Als sich dann noch herausstellte, dass der Verwaltungsaufwand für das Verfahren bei den Kammern unverhältnismäßig groß war und die Ergebnisse des Abgleichsverfahrens die eingangs genannte Ansicht nicht stützten, stellten die Handwerkskammern die Datenübermittlung an die Arbeitsverwaltung ein.

Tatsächlich stellte sich anlässlich eines Gesprächs mit der BA und dem DIHT für die IHK heraus, dass die Trefferquote, also die Anzahl der Jugendlichen, die einen weiteren Ausbildungsvertrag abgeschlossen hatten, ohne dies dem Arbeitsamt zu melden, bei dem Datenabgleich zwischen den Daten der IHK´n und der Daten der Arbeitsämter zwischen 1,4 % im März und 0,2 % im September 1998 lag. Ich habe das Gespräch mit der BA und dem

DIHT zum Anlass genommen, nicht nur auf die fehlende Rechtsgrundlage für die 1998 gemachten Datenabgleiche hinzuweisen, sondern auch darauf, dass der Deutsche Bundestag die Bundesregierung anlässlich der Beratungen zu meinem 14. TB mit Beschluss vom 22. Juni 1995 aufgefordert hat, „vor Einrichtung von Datenabgleichverfahren jeweils zu prüfen, ob sie im Interesse des Gemeinwohls zur Erreichung eines konkreten Zieles erforderlich und verhältnismäßig sind“ (BT-Plenarprotokoll 13/44, S. 3630, i. V. m. der Beschlussempfehlung des Innenausschusses, BT-Drs. 13/1636, S. 3 Nr. 1 Satz 1).

Die von mir wegen des Ergebnisses erbetene erneute Bewertung durch die Beteiligten führte dazu, dass die BA mit Erlass vom 10. Mai 1999 die Arbeitsämter anwies, das Datenabgleichverfahren mit den Kammern nicht mehr durchzuführen. Auch die IHK haben das Datenabgleichverfahren aufgegeben.

20.9 Datenabgleich zwischen Arbeitsamt und Bundesamt für Finanzen

In meinem 17. TB (Nr. 20.2) hatte ich mich mit der Zulässigkeit des Datenabgleichs der von den Arbeitsämtern im Rahmen der Bedürftigkeitsprüfung bei Arbeitslosenhilfeempfängern erhobenen Angaben über die Anzahl ihrer Freistellungsaufträge mit der Anzahl ihrer beim BfF tatsächlich gespeicherten Freistellungsaufträge befasst. Damals habe ich wegen der von den Arbeitsämtern erwirkten beträchtlichen Einsparungen und im Hinblick auf die erwartete Präventivwirkung des Abgleichverfahrens ein überwiegendes Allgemeininteresse an dem Datenabgleich als gegeben angesehen und diesen als zulässig beurteilt. Die mir im Berichtszeitraum auf meine Bitte vom BMA erneut zur Verfügung gestellten Zahlen bestätigen meine Bewertung.

Nach Mitteilung des BMA wurden von den Arbeitsämtern im Bundesgebiet in der Zeit vom 1. Januar bis zum 30. Juni 2000 insgesamt 59.218 Zahlungsnachweise mit Angaben aus dem Datenabgleich mit dem BfF ausgewertet. In 19.688 Fällen, d. h. bei einem Anteil von rund 33 %, waren vorhandene Vermögen nicht angegeben worden.

In 4.487 Fällen wurden Bewilligungsbescheide wegen nachträglicher Berücksichtigung von Vermögen oder Einkommen (Kapitalerträgen) nach § 45 SGB X aufgehoben. Hieraus ergab sich an eingesparten Leistungen und Sozialversicherungsbeiträgen ein Gesamtbetrag von 39,17 Mio. DM. Weitere Einsparungen ergaben sich daraus, dass in dieser Zeit aufgrund der Nachfragen der Arbeitsämter bundesweit 187 Anträge auf Arbeitslosenhilfe zurückgezogen wurden.

Die mir vom BMA diesmal mitgeteilten Einsparung durch Aufhebung von Bewilligungsbescheiden liegt zwar unter derjenigen, über die ich in meinem 17. TB berichtet habe (84,7 Mio. DM), auch wenn man berücksichtigt, dass sie sich diesmal auf ein halbes und nicht auf ein dreiviertel Jahr bezieht. Der Rückgang der Einsparung dürfte zu einem großen Teil darauf zurückzuführen sein, dass das von der BA herausgegebene Merkblatt für Bezieher von Arbeitslosenhilfe ausführlich auf den Datenabgleich mit den dem BfF zu Freistellungsaufträgen vorliegenden Daten hinweist. Dennoch ist die im ersten Halbjahr 2000 aufgrund des Datenabgleichs erzielte Einsparung immer noch durchaus beträchtlich. Auch im Hinblick darauf, dass bei rund einem Drittel der ausgewerteten Zahlungsnachweise vom Arbeitslosenhilfeempfänger zunächst nicht angegebene Vermögen festgestellt wurden, sehe ich nach wie vor ein überwiegendes Allgemeininteresse an dem Datenabgleich als gegeben an, hinter dem das Interesse des Einzelnen zurücktreten muss, dass das BfF dort zu seinen Freistellungsaufträgen gespeicherte Daten nicht übermittelt.

Im Berichtszeitraum ist § 45d EStG, der dem Datenabgleich zwischen den Arbeitsämtern und dem BfF zugrunde liegt, geändert worden. Nunmehr darf das BfF nicht nur der BA (für die Arbeitsämter), sondern allen Sozialleistungsträgern die bei ihm über die Freistellungsaufträge der jeweils Betroffenen gespeicherten Daten mitteilen, soweit dies zur Überprüfung des bei der Sozialleistung zu berücksichtigenden Einkommens oder Vermögens erforderlich ist oder der Betroffene zustimmt. Vor dem Hintergrund meiner Bewertung der Mitteilungen des BfF an die Arbeitsämter konnte ich mich der Notwendigkeit nicht verschließen, die anderen Sozialleistungsträger in die bisherige Regelung mit einzubeziehen, soweit es um gleichgelagerte Prüfungen der Einkommens- oder Vermögensverhältnisse der Betroffenen geht. Auch die nunmehr zusätzliche Angabe der freigestellten Kapitalerträge und der Kreditinstitute und sonstigen Stellen, denen die Freistellungsaufträge erteilt worden sind, halte ich im Hinblick auf die Erfordernisse der Praxis für vertretbar.

Soweit ich in meinem 17. TB (Nr. 20.2) auf die Notwendigkeit hingewiesen hatte, den für die Mitteilungen des BfF an die BA erforderlichen Datenabgleich gesetzlich zu regeln, ist dies – bezogen auf alle Sozialleistungsträger – mit der Neufassung des § 45d EStG erfolgt.

21 Krankenversicherung

21.1 Gesundheitsreform

In den Jahren 1999 und 2000 habe ich mich in besonderem Maße mit Gesetzgebungsvorhaben im Bereich der Gesundheitsreform befasst. Bundesregierung und die Fraktionen der Regierungsparteien haben im Sommer 1999 inhaltsgleiche Entwürfe eines Gesetzes zur Reform der Gesetzlichen Krankenversicherung ab dem Jahr 2000 (GKV–Gesundheitsreform 2000) vorgelegt (vgl. BT–Drs. 14/1245 und 14/1721). Vorrangiges Ziel dieser Entwürfe war, die Kosten im Gesundheitswesen zu begrenzen und gleichzeitig – weiterhin – eine gute Versorgung der Patienten sicherzustellen. In den Gesetzentwürfen waren Regelungen enthalten, die in das Recht der Versicherten auf informationelle Selbstbestimmung stark eingegriffen hätten, ohne die Prinzipien der Erforderlichkeit und der Verhältnismäßigkeit zu wahren. Falls das Gesetz in der

Entwurfsfassung in Kraft getreten wäre, hätten die Krankenkassen über umfangreiche medizinische, versichertenbezogene Patientendatenbestände (Patientenprofile) verfügt. Bei den Krankenkassen wäre der „gläserne Patient“ entstanden.

Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb an den ursprünglichen Entwürfen des Gesetzes massive Kritik geübt. Auch auf Grund dieser geschlossen vorgetragenen Position ist es gelungen, in den parlamentarischen Beratungen die gegen die Entwürfe erhobenen erheblichen datenschutzrechtlichen Einwendungen auszuräumen; die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in einer Entschließung zu der gefundenen Lösung zustimmend geäußert (s. **Anlage 17**). Mit der vom Deutschen Bundestag verabschiedeten Fassung wäre der Datenschutz in der Gesetzlichen Krankenversicherung zugunsten der Versicherten weiterentwickelt worden, ohne dass hierdurch die Zielsetzung der ursprünglichen Gesetzentwürfe beeinträchtigt worden wäre. Einerseits sollten dadurch die Krankenkassen künftig über die vollständigen Abrechnungsdaten **aller** Leistungserbringer, also auch die der Ärzte und der Zahnärzte, für alle Versicherten verfügen können, womit einem Anliegen der Bundesregierung – stärkere Verantwortung der Krankenkassen bei der Kostendämpfung – Rechnung getragen worden wäre. Andererseits hätte jedoch zugleich vermieden werden können, dass die Krankenkassen die Leistungsdaten versichertenbezogen speichern. Denn es war vorgesehen, alle Leistungsabrechnungsdaten von den Leistungserbringern den neu einzurichtenden Datenannahmestellen zu übermitteln. Die Datenannahmestellen sollten die Leistungsabrechnungen vor der Übermittlung an die jeweilige Krankenkasse pseudonymisieren. Diese hätte dann zwar alle Leistungen, z. B. auch die verschiedener Ärzte für einen Versicherten, zusammenführen können; der Bezug zum Namen oder zur Versichertennummer wäre ihr jedoch grundsätzlich nicht – nur bis auf wenige ausdrücklich gesetzlich geregelte Ausnahmen – möglich gewesen. Diese Reidentifikation hätte nur von einem Trust-Center vorgenommen werden können, das räumlich und organisatorisch von der Datenannahmestelle getrennt war. Die Reidentifikation hätte unter Angabe des Grundes protokolliert werden müssen und wäre damit jeweils nachvollzieh- und kontrollierbar gewesen. Dies hätte zur Transparenz des Verfahrens erheblich beigetragen. Eine Reidentifikation durch die Krankenkassen wäre in keinem Fall möglich gewesen.

In dem am 1. Januar 2000 in Kraft getretenen GKV-Gesundheitsreformgesetz 2000 (BGBl. I S. 2626), das das Ergebnis eines Vermittlungsverfahrens ist, sind die Vorschriften über Datenannahmestellen und über die Pseudonymisierung nicht mehr enthalten; insoweit ist der Gesetzentwurf, der zur Verbesserung des Datenschutzes im Bereich der GKV erheblich beigetragen hätte, gescheitert. Ich habe deshalb das BMG bestärkt, die im Jahre 1999 gemeinsam erarbeiteten sehr datenschutzfreundlichen Regelungen im Umgang mit den Daten der Versicherten im Sozialgesetzbuch zu verankern.

Das BMG bereitet zur Zeit den Entwurf eines Gesetzes über Datentransparenz und Datenschutz in der GKV (Transparenzgesetz) vor. Soweit mir bekannt ist, sieht auch dieser Entwurf datenschutzrechtliche Verbesserungen gegenüber dem derzeitigen Rechtszustand vor. So soll eine Pseudonymisierung der Abrechnungsdaten erfolgen, allerdings erst nach der Leistungsabrechnung. Auch sollen die Krankenkassen die Leistungsabrechnungen auf Dauer nur pseudonymisiert speichern dürfen, so dass nach dem neuen Entwurf der „gläserne Versicherte“ nicht entstehen kann.

Wie bei der Beratung des Gesetzentwurfs im Jahre 1999 werde ich mich intensiv in die Vorbereitung des Entwurfs und in die parlamentarischen Beratungen einschalten, um datenschutzrechtliche Verbesserungen im Bereich der Gesetzlichen Krankenversicherung sicherzustellen.

21.2 ICD-10

Mit der Automatisierung der Datenübermittlung zu Abrechnungszwecken ist es erforderlich, dass Ärzte und Krankenhäuser zur Codierung der zu übermittelnden leistungsbegründenden Diagnosen einen Schlüssel als Ersatz des bisher üblichen Klarschrifteintrags der Diagnose verwenden. In der Vergangenheit habe ich mich bereits mehrfach mit der Einführung des hierfür vorgesehenen ICD-10 befasst (vgl. 16. TB Nr. 21.1.5, 17. TB Nr. 21.5). In diesen Tätigkeitsberichten hatte ich erhebliche Bedenken gegen die feine und tiefe Aufgliederung der Schlüssel vorgetragen, die so nicht immer zur Leistungsbegründung gegenüber den Krankenkassen erforderlich seien und in Einzelfällen sogar den Therapieerfolg gefährden könnten. Insbesondere im Hinblick auf diese Bedenken und nach heftigen Reaktionen der Öffentlichkeit war die Inkraftsetzung des ICD-10 vom BMG verschoben worden.

Der vom Deutschen Institut für medizinische Dokumentation und Information – DIMDI – im Auftrag des BMG herausgegebene ICD-10 ist inzwischen – mit für einzelne Fachgruppen erheblichen Zusammenfassungen – vom BMG durch Bekanntmachung vom 24. Juni 1999 (Bundesanzeiger vom 8. Juli 1999, Nr. 124, S. 10985) mit Wirkung vom 1. Januar 2000 in Kraft gesetzt worden. Der jetzt zu verwendende Schlüssel ist durch § 295 Abs. 1 bzw. § 301 Abs. 2 SGB V in der Fassung des GKV-Gesundheitsreformgesetzes 2000, die die Ärzte bzw. Krankenhäuser verpflichten, bei der Abrechnung der Leistungen die Diagnosen nach dem ICD–10 zu verwenden, seit 1. Januar 2000 abgedeckt. Dieser abrechnungsorientierte ICD-10 entspricht meinen Erwartungen.

Im Hinblick auf die in § 17b Krankenhausfinanzierungsgesetz vorgesehene Einführung eines pauschalisierenden Entgeltsystems für die Abrechnung der allgemeinen Krankenhausleistungen ist eine Erweiterung des ICD-10 erforderlich. Gegen die ursprünglich vom BMG vorgesehene Fassung habe ich gemeinsam mit den Landesbeauftragten für den Datenschutz Bedenken vorgetragen. Ich habe insbesondere darauf hingewiesen, dass der ICD-10 im Hinblick auf § 17b Krankenhausfinanzierungsgesetz nur insoweit erweitert werden darf, als die einzelnen

Schlüssel zur Erfüllung der Aufgaben nach dieser Vorschrift erforderlich sind und nicht unverhältnismäßig – insbesondere durch zu tiefgehende Spezifizierung – in die Privatsphäre des jeweils Betroffenen eingreifen. Außerdem habe ich darauf aufmerksam gemacht, dass die Erweiterung nur für die Abrechnung der Leistungen der Krankenhäuser nach § 301 SGB V vorgenommen werden kann, nicht dagegen für die Abrechnungen ärztlicher Leistungen nach § 295 SGB V. Das BMG und das DIMDI sind meinen Vorschlägen gefolgt. Die Erweiterung des ICD-10 ist durch § 301 Abs. 2 SGB V i. V. m. § 17 b Krankenhausfinanzierungsgesetz gedeckt; gegen die jetzt ergänzte Fassung des ICD-10 habe ich keine Bedenken mehr.

21.3 Anforderung von Krankenhausentlassungsberichten durch Krankenkassen

Wegen vieler Eingaben zur Anforderung von Krankenhausberichten durch gesetzliche Krankenkassen stelle ich nachfolgend meine Auffassung hierzu dar:

- Die Krankenkassen dürfen Daten nur erheben, wenn sie hierfür eine Befugnis haben. Diese Erhebungsbefugnis hat allerdings ihre Grenzen in für die gesetzliche Krankenversicherung abschließend im SGB geregelten Übermittlungsbefugnissen der Leistungserbringer.
- Eine Verpflichtung der Krankenhäuser zur Übermittlung von Krankenhausentlassungsberichten, Arztbriefen, Befundberichten, ärztlichen Gutachten, Röntgenaufnahmen usw. besteht nicht. Der Datenkatalog der Vorschrift des § 301 SGB V ist nicht nur eine Regelung für die Fälle der maschinenlesbaren Übermittlung von Leistungsdaten, sondern grundsätzlich eine abschließende Regelung zulässiger Datenübermittlungen zu Abrechnungszwecken zwischen Krankenhaus und Krankenkasse.
- § 301 Abs. 1 Satz 1 Nr. 3 SGB V sieht lediglich vor, dass auf Verlangen der Krankenkassen die medizinische Begründung für die Überschreitung der Dauer der Krankenhausbehandlung zu übermitteln ist. Diese Vorschrift eröffnet nicht die Befugnis zur Erhebung von Krankenhausentlassungsberichten, Arztbriefen, Befundberichten, ärztlichen Gutachten, Röntgenaufnahmen usw., sondern vielmehr zur Übermittlung von Antworten auf bestimmte Fragen im erforderlichen Umfang.
- Auch aus § 73 Abs. 2 Nr. 9 SGB V lässt sich keine Verpflichtung von Ärzten zur Übermittlung der vorgenannten Unterlagen an die Krankenkassen herleiten.
- Auf Grund der spezialgesetzlichen Regelungen im SGB V sehe ich für die Anwendung des § 100 SGB X – soweit es die Übermittlung von Krankenhausentlassungsberichten angeht – keinen Raum; dies gilt auch für die zweite Alternative in § 100 Abs. 1 Satz 1 SGB X, nach der eine Übermittlung durch den Arzt dann zulässig ist, wenn der Betroffene im Einzelfall eingewilligt hat.
- Die Einholung einer Einwilligungserklärung des Versicherten zur Übermittlung der vorgenannten Unterlagen an die Krankenkasse wäre eine Umgehung der gesetzlichen Regelung zur Prüfung der medizinischen Sachverhalte durch den Medizinischen Dienst der Krankenversicherung (MDK). Aus diesem Grunde halte ich die Forderungen der Krankenkassen an Krankenhäuser und Ärzte, bei Vorliegen einer Einwilligungserklärung des Versicherten die vorgenannten Unterlagen an die Krankenkassen zu übermitteln, für rechtlich nicht gedeckt und damit unzulässig.
- Der Gesetzgeber hat die Prüfung medizinischer Sachverhalte ausdrücklich dem MDK übertragen. In § 275 SGB V ist eindeutig geregelt, dass die Krankenkassen beim MDK in folgenden Fällen unter den in dieser Vorschrift genannten Voraussetzungen eine gutachtliche Stellungnahme einholen müssen:
  - bei der Erbringung von Leistungen, insbesondere zur Prüfung von Voraussetzung, Art und Umfang der Leistung,
  - zur Einleitung von Rehabilitationsleistungen,
  - in bestimmten Fällen bei Arbeitsunfähigkeit.
- Zum Verfahren hinsichtlich der Einschaltung des MDK bemerke ich:

  Nach § 276 Abs. 1 Satz 1 SGB V sind die Krankenkassen verpflichtet, dem Medizinischen Dienst die für die Beratung und Begutachtung erforderlichen Unterlagen vorzulegen und Auskünfte zu erteilen.

  Nach § 276 Abs. 1 Satz 2 SGB V dürfen Unterlagen, die der Versicherte freiwillig der Krankenkasse übermittelt hat, dem MDK nur mit Einwilligung des Versicherten weitergegeben werden.

  § 276 Abs. 2 Satz 1 SGB V regelt die Befugnis des MDK, Sozialdaten zu erheben, soweit dies für die Prüfungen, Beratungen und gutachtlichen Stellungnahmen nach § 275 SGB V erforderlich ist. Die Leistungserbringer sind nach § 276 Abs. 2 Satz 1 2. Halbsatz SGB V verpflichtet, Sozialdaten – gemeint sind personenbezogene Daten, Unterlagen einschließlich Befundunterlagen, auch von anderen Leistungserbringern – dem MDK zu übermitteln. Die Versendung sollte unmittelbar an den MDK erfolgen. Falls die Anforderung nicht durch den MDK, sondern durch die Krankenkasse zur Weiterleitung an den MDK erfolgt, ist die Versendung auch an die Krankenkasse hinnehmbar, wenn die medizinischen Unterlagen in einem gesonderten, verschlossenen Umschlag übersandt werden, der mit der Anschrift des MDK sowie einem Vermerk „ärztliche Unterlagen – nur vom MDK zu öffnen“ versehen ist. Damit wird sichergestellt, dass eine unzulässige Einsichtnahme in die Krankenhausentlassungsberichte durch die Krankenkasse dabei nicht erfolgt.

Diese Auffassung werde ich bei der Bearbeitung von Eingaben nach § 81 Abs. 1 Nr. 1 SGB X, bei Anfragen von Krankenhäusern und Ärzten sowie bei der Beratung und der Kontrolle nach § 81 Abs. 2 Satz 1 SGB X i.V.m. §§ 24 bis 26 BDSG zu Grunde legen. Ich habe sie den Spitzenverbänden der Krankenkassen mitgeteilt und diese gebeten, ihre Mitgliedskrankenkassen entsprechend zu unterrichten.

21.4 Private Versicherungsagentur erhält unzulässiger Weise Sozialdaten

Die hauptamtlich besetzten Geschäftsstellen einer Ersatzkasse haben die Möglichkeit, an Orten ihres Geschäftsstellenbereiches, in denen die Kasse bisher noch nicht hauptamtlich vertreten ist, sog. nebenamtliche Außenstellen einzurichten. Diese Außenstellen bekommen allerdings keine Versichertendaten zur Verfügung gestellt.

Neben einer Datenschutzverpflichtung des Außenstellenleiters sind auch die Aufgaben der Außenstellen in einer schriftlichen Vereinbarung geregelt. Danach beschränkt sich der Aufgabenbereich auf die Vermittlung neuer Mitglieder, Aushändigung von Broschürenmaterial oder Entgegennahme von Unterlagen zur Weiterleitung an die hauptamtliche Geschäftsstelle.

Mit der Errichtung solcher „nebenamtlicher Außenstellen“ dieser Kasse hatte ich mich bereits vor 10 Jahren auseinandergesetzt und dies damals im Rahmen einer Kontrolle mit Vertretern der Kasse umfassend erörtert. Unter Berücksichtigung des Ergebnisses hatte ich hiergegen keine grundsätzlichen Bedenken erhoben.

Im Berichtszeitraum wurde ich jedoch im Rahmen zweier Petitionen darüber informiert, dass von dieser Krankenkasse Sozialdaten ihrer Versicherten an eine private Versicherungsagentur übermittelt worden sind. Diese hatte die Agentur ihrerseits dann für eigene Werbezwecke verwendet und den Petenten u. a. Versicherungsangebote unterbreitet.

Die Hauptverwaltung der Kasse hat mir bestätigt, dass vorliegend seitens ihrer zuständigen Geschäftsstelle unzulässigerweise und entgegen den klaren Anweisungen einer privaten Versicherungsagentur, die gleichzeitig als „nebenamtliche Außenstelle“ der Krankenkasse fungierte, eine Mitgliederliste zur Verfügung gestellt wurde. Der Außenstellenleiter habe diese dann eigenmächtig – und entgegen seiner schriftlichen Verpflichtung zur Einhaltung datenschutzrechtlicher Bestimmungen – für eine Werbeaktion als Versicherungsagentur verwandt.

Die Kasse hat diesen konkreten, regional begrenzten Vorfall bedauert und die Außenstellenvereinbarung aufgelöst.

Ich habe daraufhin die bei der Kasse bestehenden grundsätzlichen Anweisungen und datenschutzrechtlichen Sicherheitsmaßnahmen im Umgang mit nebenamtlichen Außenstellen geprüft. Sie entsprechen den datenschutzrechtlichen Anforderungen und stellen organisatorische Maßnahmen dar, um einem Verstoß gegen datenschutzrechtliche Vorschriften vorzubeugen, so dass ich gemäß § 81 Abs. 2 SGB X i.V.m. § 25 Abs. 2 BDSG darauf verzichten konnte, den vorliegenden Datenschutzverstoß förmlich zu beanstanden. Hierbei habe ich auch berücksichtigt, dass es sich um einen auf eine Außenstelle der Krankenkasse begrenzten Fall gehandelt hat, den die Hauptverwaltung zum Anlass genommen hat, für die Zukunft weitere datenschutzgerechte Veranlassungen zu treffen.

21.5 Werbung durch Krankenkassen

Mit der Werbung durch öffentlich-rechtliche Krankenkassen habe ich mich schon in meinen letzten Tätigkeitsberichten befasst (vgl. 16. TB Nr. 21.3, 17. TB Nr. 34.12.). Dabei habe ich die Auffassung vertreten, dass den Krankenkassen die Möglichkeit eröffnet werden sollte, potentielle neue Mitglieder auch direkt zu werben. Hierfür ist aber eine entsprechende gesetzliche Klärung zur Zulässigkeit personenbezogener Werbemaßnahmen erforderlich. Das BMG hat in den Entwurf eines Gesetzes zur Reform der gesetzlichen Krankenversicherung ab dem Jahr 2000 (GKV-Gesundheitsreformgesetz 2000) eine entsprechende Regelung (§ 284 Abs. 3 SGB V) aufgenommen (vgl. BT–Drs. 14/1245). In dem am 1. Januar 2000 in Kraft getretenen Gesetz, das Ergebnis eines Vermittlungsverfahrens ist, ist aber die Änderung des § 284 SGB V nicht mehr enthalten.

Um den Kassen die gewünschten Möglichkeiten der Werbung doch endlich zu eröffnen, sollte in den bei Redaktionsschluss in Vorbereitung befindlichen Entwurf eines Gesetzes über Datentransparenz und Datenschutz in der GKV (Transparenzgesetz) der gekippte § 284 Abs. 3 SGB V wieder aufgenommen werden. Auch sollte im Rahmen der Beratungen des Transparenzgesetzes geprüft werden, ob eine Regelung aufzunehmen ist, nach der der Betroffene in die Erhebung seiner Daten einwilligen muss und dass ausgeschiedene Mitglieder einer Krankenkasse in die Werbung einbezogen werden können. Das BMG habe ich entsprechend beraten.

21.6 Geschäftsstellenübergreifender Zugriff auf Versichertendaten

Bei einigen überregional tätigen Krankenkassen ist es möglich, dass alle Geschäftsstellen auf die medizinischen Daten ihrer Versicherten zugreifen können. Dies ist durch die bestehende Rechtslage nicht abgedeckt. Nach § 35 Abs. 1 SGB I hat jeder Versicherte Anspruch auf Wahrung des Sozialgeheimnisses. Dies umfasst auch die Verpflichtung der Krankenkassen, intern sicherzustellen, dass die Sozialdaten der Versicherten nur Befugten zugänglich sind. § 78 a SGB X verpflichtet die Krankenkassen, die technischen und organisatorischen Maßnahmen – einschließlich der Dienstanweisungen – zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des SGB zu gewährleisten. Dies erfordert es, grundsätzlich festzulegen, dass jeweils nur einer Geschäftsstelle einer Krankenkasse der Zugriff auf die medizinischen Daten des Versicherten ermöglicht wird.

Auf meine Initiative hin ist § 284 SGB V während der parlamentarischen Beratungen des Entwurfs eines Gesetzes zur Reform der gesetzlichen Krankenversicherung ab dem Jahr 2000 (GKV-Gesundheitsreformgesetz 2000) entsprechend geändert worden (vgl. BT-Drs. 14/1977). Nach der vorgesehenen Fassung des § 284 Abs. 4 SGB V sollte einer Krankenkasse für ihren gesamten Bereich ein geschäftsstellenübergreifender Zugriff ohne schriftliche Einwilligung nur noch auf diejenigen Daten möglich sein, die zur Feststellung des Versicherungsverhältnisses und der Mitgliedschaft erforderlich sind. Zugriffe auf weitere Daten eines Versicherten sollten nur noch für die Geschäftsstelle zugelassen werden, die für den Versicherten örtlich zuständig ist. Der Zugriff durch andere Geschäftsstellen sollte nur mit schriftlicher Einwilligung des Versicherten ermöglicht werden.

In dem am 1. Januar 2000 in Kraft getretenen Gesetz, das das Ergebnis eines Vermittlungsverfahrens ist, ist die Änderung des § 284 SGB V nicht mehr enthalten. Ich habe das BMG aufgefordert, die im Jahre 1999 beschlossene Fassung des § 284 Abs. 4 SGB V in den in Vorbereitung befindlichen Entwurf eines Gesetzes über Datentransparenz und Datenschutz in der GKV – Transparenzgesetz – (s. o. Nr. 21.1) aufzunehmen. Auch sollte im Rahmen der Beratungen des Transparenzgesetzes die Aufnahme einer Regelung geprüft werden, nach der die schriftliche Einwilligung auch durch Vorlage der Krankenversichertenkarte und deren Protokollierung erfolgen kann.

21.7 Mitteilung von Krankheitsursachen und drittverursachten Gesundheitsschäden (Regressfälle)

Zur Feststellung anderer Kostenträger und um Schadensersatzansprüche nach § 116 SGB X geltend machen zu können, ist die Übermittlung von Leistungsdaten an die Krankenkassen erforderlich. Hierfür fehlt zur Zeit eine entsprechende gesetzliche Regelung. Durch Eingaben habe ich Kenntnis bekommen, dass Krankenkassen zum Teil dennoch Unterlagen zur Erfüllung dieser Aufgaben anfordern. Da nicht von der Hand zu weisen ist, dass die Krankenkassen diese Unterlagen zur Klärung von Regressfällen benötigen, muss eine Rechtsgrundlage geschaffen werden.

In den Entwurf eines Gesetzes zur Reform der gesetzlichen Krankenversicherung ab dem Jahr 2000 (GKV-Gesundheitsreform 2000) war eine entsprechende Regelung (§ 294a SGB V) aufgenommen worden (vgl. BT–Drs. 14/1977). In dem am 1. Januar 2000 in Kraft getretenen Gesetz (BGBl. I S. 2626), das das Ergebnis eines Vermittlungsverfahrens ist, ist diese Vorschrift nicht mehr enthalten. Ich habe daher das BMG gebeten, die ursprüngliche Fassung des § 294a SGB V in den in Vorbereitung befindlichen Entwurf eines Gesetzes über Datentransparenz und Datenschutz in der GKV (Transparenzgesetz) aufzunehmen.

21.8 Krankenkassen lassen ihre Leistungspflicht durch ärztliche Gutachter ihres Vertrauens prüfen

Durch Eingaben bin ich darauf hingewiesen worden, dass einzelne Krankenkassen Gutachtenaufträge an externe Ärzte vergeben, obwohl sie in den jeweiligen Einzelfällen zur Klärung medizinischer Sachverhalte beim Medizinischen Dienst der Krankenversicherung (MDK) eine gutachtliche Stellungnahme einholen müssten. Dies wird zum Teil damit begründet, dass der MDK Gutachten nicht immer in dem von der Krankenkasse erwarteten Zeitrahmen erstellt bzw. dass die Krankenkassen in Erfüllung ihrer Aufgaben ggf. auch die Gutachten des MDK prüfen wollen.

Gegen diese Praxis bestehen erhebliche datenschutzrechtliche Bedenken. Durch das von einigen Krankenkassen durchgeführte Verfahren erhalten diese Krankenkassen Kenntnis von medizinischen Daten von Versicherten, die sie zur Erfüllung ihrer gesetzlich festgelegten Aufgaben nicht benötigen und daher auch nicht erheben dürfen (vgl. § 284 SGB V, s. o. Nr. 21.3).

Die Prüfung medizinischer Sachverhalte für die Erfüllung der gesetzlichen Aufgaben der Krankenkassen, beispielsweise zur Prüfung ihrer Leistungsverpflichtung, von Arbeitsunfähigkeiten sowie zur Einleitung von Rehabilitationsmaßnahmen ist ausschließlich dem MDK übertragen (§ 275 SGB V). Das schließt ein, dass auch nur der MDK einen externen Gutachter beauftragen darf (§ 279 Abs. 5 SGB V).

Die bestehende Rechtslage lässt nicht zu, dass die medizinische Begutachtung von Versicherten durch eigene Ärzte der Krankenkassen oder durch von den Krankenkassen unmittelbar beauftragten externen Gutachtern durchgeführt werden.

22 Rentenversicherung

22.1 Kontrolle einer Auskunfts- und Beratungsstelle der BfA

Im Berichtszeitraum habe ich eine Auskunfts- und Beratungsstelle (A- und B-Stelle) der BfA datenschutzrechtlich beraten und kontrolliert. In solchen Außenstellen der BfA können Versicherte sich persönlich und Orts nah in Rentenangelegenheiten beraten lassen und Auskünfte erhalten.

Da in einer solchen Stelle in erheblichem Umfang Publikumsverkehr stattfindet, kommt einer effizienten Zugangskontrolle besondere Bedeutung zu. In der A- und B-Stelle habe ich kontrolliert, wie die Identität der Besucher geprüft wird und wie die Beratung der Versicherten in der zentralen Anmeldestelle organisiert ist. Die Versicherten werden von den Beratern in Einzelräumen bedient. Damit sich die Besucher nicht frei im Dienstge-

bäude bewegen, werden sie von den Beratern persönlich im Warteraum geholt und auch wieder dorthin zurück begleitet. Dieses Vorgehen trägt zum Schutz der Sozialdaten der Versicherten vor einer Kenntnisnahme durch Unbefugte bei und stellt die Wahrung des Sozialgeheimnisses gemäß § 35 SGB I sicher. Das praktizierte Verfahren entspricht den gesetzlichen Vorgaben des § 78a SGB X.

Ich begrüße es besonders, dass neben den von der Hauptstelle der BfA vorgegebenen bundesweit geltenden datenschutzrechtlichen Regelungen in der geprüften A– und B-Stelle spezielle Weisungen existieren und die Mitarbeiter laufend durch entsprechende Rundschreiben, Informationen und Schulungen zu datenschutzrechtlichen Fragen informiert und sensibilisiert werden. Die Einhaltung der datenschutzrechtlichen Vorgaben wird durch den Leiter der Dienststelle angemessen kontrolliert.

Bei der stichprobenartigen Kontrolle der vorhandenen Versichertenunterlagen habe ich in Einzelfällen festgestellt, dass diese oftmals für die Aufgabenerfüllung der Auskunfts- und Beratungsstelle nicht mehr erforderliche personenbezogene Daten, etwa Kopien vollständiger Schulzeugnisse, enthielten. Es bestand mit der BfA Einvernehmen darüber, dass zwar die Vorlage solcher Unterlagen zur Bearbeitung der Versicherungsangelegenheiten grundsätzlich erforderlich ist, hierbei jedoch sichergestellt sein muss, dass der Betroffene vorher bestimmte, von der BfA nicht benötigte Angaben unkenntlich machen kann. Die nicht erforderlichen Daten wurden umgehend gelöscht.

Weiterhin fand ich Unterlagen mit Sozialdaten der Versicherten, die zu lange aufbewahrt wurden. Nach § 84 Abs. 2 Satz 2 SGB X sind Sozialdaten zu löschen, wenn ihre Kenntnis für die A- und B-Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Die BfA hat die nicht mehr erforderlichen Unterlagen, etwa länger zurückliegende und bereits abgeschlossene Beschwerdevorgänge, sofort gelöscht und meine diesbezüglichen Kontrollfeststellungen zum Anlass genommen, dieses Thema mit den Leitern sämtlicher Auskunfts- und Beratungsstellen im Rahmen einer Schulung zu erörtern.

Die Ergebnisse meines Besuchs haben einmal mehr belegt, dass dem Datenschutz im Bereich der BfA ein hoher Stellenwert beigemessen wird.

22.2 Kontrolle einer Rehabilitationsklinik der BfA

In einer Rehabilitationsklinik in der Trägerschaft der BfA habe ich die Verarbeitung der Sozialdaten in verschiedenen Bereichen der Klinik – insbesondere Rezeption, Patientenaufnahme, Stationen, Sekretariate, Archive – kontrolliert.

Ein besonderes Augenmerk habe ich dort auf die sog. Patientenaufnahme gerichtet, da dort mehr Sozialdaten verarbeitet werden, als dies erfahrungsgemäß in sonstigen Krankenhäusern der Fall ist. Vorgefunden habe ich für Zwecke der Patientenaufnahme und -betreuung insbesondere umfassende dem Arztgeheimnis unterliegende personenbezogene Daten, etwa ärztliche Befundberichte und Anträge auf medizinische Leistungen zur Rehabilitation. Diese Unterlagen sind insgesamt für die Aufgabenerfüllung dieses Bereiches zu umfangreich und nicht genügend vor der Einsichtnahme des Publikums gesichert. Ich habe gegenüber der Klinikleitung entsprechende Verbesserungen angeregt und empfohlen, ergänzend schriftliche organisatorische und datenschutzrechtliche Regelungen für diesen Klinikbereich zu treffen. Dies wurde erfreulicherweise kurzfristig umgesetzt.

Weitere Einzelfeststellungen in den anderen Bereichen der Klinik, etwa bezüglich dortiger Löschungen und Datensicherungsmaßnahmen, wurden ebenfalls unmittelbar mit der Klinikleitung besprochen. Die BfA bzw. die Klinik ist auch hierzu meinen Empfehlungen zeitnah nachgekommen.

Auch diese Kontrolle hat – nicht zuletzt wegen der großen Aufgeschlossenheit der Klinikleitung dem Datenschutz gegenüber – meinen positiven Gesamteindruck für den Bereich der BfA bestätigt.

23 Unfallversicherung

23.1 Gutachtertätigkeit in der gesetzlichen Unfallversicherung

In meinem 17. TB habe ich ausführlich über die Schwierigkeiten berichtet, die im Zusammenhang mit dem Gutachterauswahlrecht für Versicherte entstanden sind (vgl. 17. TB Nr. 23.4). Mit dem Inkrafttreten des § 200 Abs. 2 SGB VII zum 1.1.2000 wurde mit dem Recht für die Versicherten, einen Gutachter auszuwählen oder selbst vorzuschlagen, erstmals eine Regelung getroffen, die nicht nur die Transparenz des Verfahren verbessert, sondern den Versicherten Mitwirkungsrechte in Anerkennungs- und Feststellungsverfahren einräumt.

Auch im Berichtszeitraum hat sich trotz konstruktiver Ansätze gezeigt, dass die Abkehr von einer jahrzehntelang geübten Praxis nur schleppend vorangeht, insbesondere bei der Einschaltung eines beratenden Arztes. In fünf Eingabefällen habe ich einen Verstoß gegen § 200 Abs. 2 SGB VII beanstandet, weil ein beratender Arzt eine Stellungnahme abgegeben hatte, die als Gutachten i. S. dieser Vorschrift zu werten war. In diesen Fällen hatten die jeweiligen Berufsgenossenschaften ihre beratenden Ärzte mit umfassenden Gutachten zur Zusammenhangsfrage beauftragt. Mit nur wenig differierenden Begründungen hatten die Berufsgenossenschaften § 200 Abs. 2 SGB VII nicht für anwendbar gehalten, da es sich bei den Anfragen an den beratenden Arzt nach ihrer Meinung um eine interne Beratung gehandelt habe. Dies hat mich in Anbe-

tracht der jeweiligen Beauftragung mit einer umfassenden Bewertung zur haftungsbegründenden und haftungsausfüllenden Kausalität und/oder der Höhe der MdE (Minderung der Erwerbstätigkeit) nicht überzeugt, zumal von keiner Berufsgenossenschaft bestritten wird, dass der beratende Arzt auch ein Gutachten erstellen kann. In drei Eingabefällen war die ablehnende Entscheidung sogar ausdrücklich auf die Stellungnahme des beratenden Arztes gestützt worden.

Die dargestellte Problematik bei der Anwendbarkeit des § 200 Abs. 2 SGB VII wird dadurch verschärft, dass das Bundesversicherungsamt (BVA) als Aufsichtsbehörde der Berufsgenossenschaften eine weitere, divergierende Auffassung vertritt. Denn das BVA geht nur dann von einem Gutachten i.S. der genannten Vorschrift aus, wenn die Stellungnahme des beratenden Arztes – wie in den drei letztgenannten Eingabefällen – ausdrücklich im Bescheid genannt wird. Wird die Stellungnahme dagegen im Bescheid nicht erwähnt, handele es sich dagegen lediglich um eine interne Beweiswürdigung.

Die rückblickende Beurteilung, ob der eingesetzte Arzt als Gutachter oder Berater gehandelt hat, ist zwar aus der Aufgabenstellung einer Aufsichtsbehörde verständlich, wird aber dem datenschutzrechtlichen Ansatz des § 200 Abs. 2 SGB VII nicht gerecht. Vielmehr ist von der Situation vor der Gutachterbeauftragung auszugehen, denn nur vor der Beauftragung des Gutachters können dem Versicherten die Rechte nach § 200 Abs. 2 SGB VII überhaupt gewährt werden. Es trägt auch nicht zur Transparenz des Verfahrens bei, die Entscheidung, ob eine Stellungnahme als Gutachten oder als interne Beratung gewertet wird, bis zur Erteilung des Bescheides offen zu lassen.

Um noch vor einer einvernehmlichen Lösung mit dem BVA eine datenschutzfreundliche Handhabung des § 200 Abs. 2 SGB VII sicherzustellen, habe ich zugleich mit dem Hauptverband der gewerblichen Berufsgenossenschaften (HVBG) im Rahmen einer Fortschreibung der Musterdienstanweisung Gespräche über mögliche Abgrenzungskriterien zwischen der beratungsärztlichen Tätigkeit und der Einschaltung eines Gutachters geführt. Die Schwierigkeiten bei der Aufstellung dieser Kriterien besteht darin, dass eine Beratung im Sinne einer Erläuterung oder Vermittlung allgemeiner medizinischer Sachverhalte durch den beratenden Arzt zwar möglich sein soll, vor der Beauftragung des beratenden Arztes mit einem Gutachten aber dem Versicherten die Rechte des § 200 Abs. 2 SGB VII zu gewähren sind.

Vor diesem Hintergrund wurden folgende Fallkonstellationen gebildet, in denen eine beratungsärztliche Tätigkeit angenommen werden kann:

- Fälle, in denen die Verwaltung des Unfallversicherungsträgers aufgrund eigener Erkenntnis in der Lage ist, selbst einen Entscheidungsvorschlag zu erarbeiten, den der beratende Arzt hinsichtlich evtl. Fallbesonderheiten prüfen soll. Weicht die Stellungnahme des beratenden Arztes vom Entscheidungsvorschlag ab oder weist sie auf klärungsbedürftige Sachverhalte hin, ist über die Notwendigkeit weiterer Ermittlungen, insbesondere der Einholung eines Gutachtens, zu entscheiden.
- Medizinisch klar gelagerte Fälle, in denen es dem beratenden Arzt möglich ist, schon aufgrund des Akteninhalts eine Stellungnahme abzugeben, die zur abschließenden Entscheidung der Sachbearbeitung oder zur Auftragsvergabe an einen Gutachter führt.
- Fälle, in denen ein Gutachten vorliegt und der beratende Arzt gebeten wird, zur Schlüssigkeit des Gutachtens Stellung zu nehmen. Bei fehlender Schlüssigkeit hat sich der beratende Arzt im Regelfall darauf zu beschränken, die Rückgabe des Gutachtens an den Gutachter mit konkreten Fragestellungen oder die Einholung eines weiteren Gutachtens vorzuschlagen. Ausnahmsweise kann der beratende Arzt bei fehlender Schlüssigkeit des Gutachtens und eindeutiger Befundlage einen begründeten Vorschlag zur Entscheidung in einzelnen Sachfragen machen. Bevor die Berufsgenossenschaft eine von den Aussagen des Gutachtens abweichende Entscheidung trifft, hat sie dem Gutachter Gelegenheit zur Gegenäußerung zu geben.

Umgekehrt ist bei einer ärztlichen Beurteilung nach körperlicher Untersuchung von einer gutachtlichen Tätigkeit auszugehen und damit § 200 Abs. 2 SGB VII zu beachten, d. h. dem Betroffenen sind mehrere geeignete Gutachter zur Auswahl zu benennen. Das gilt auch für Fälle zur Diagnosesicherung. Ist der beratende Arzt in dem Verwaltungsvorgang bereits tätig geworden, so kann er in derselben Sache nicht als Gutachter beauftragt werden.

Diese Kriterien geben Anhaltspunkte für die Entscheidung der Unfallversicherungsträger in Fällen, die in der Vergangenheit oftmals zu Schwierigkeiten geführt haben. Die Berufsgenossenschaften haben grundsätzlich ein positives Signal gegeben, künftig im wesentlichen diese Kriterien bei der Einschaltung eines beratenden Arztes zugrunde zulegen. In den nächsten Jahren werde ich verstärkt kontrollieren, ob dies im Hinblick auf § 200 Abs. 2 SGB VII zu einer Verbesserung der datenschutzrechtlichen Positionen der Versicherten führt.

23.1.1 BK-Report des HVBG zu der neuen Berufskrankheit Nr. 1317

Die Berufskrankheit Nr. 1317 (Polyneuropathie oder Enzephalopathie durch organische Lösungsmittel oder deren Gemische) ist seit dem 1.12.1997 in die Berufskrankheiten-Verordnung aufgenommen worden. Im Frühjahr 1999 gab der HVBG in einem BK-Report zu dieser Berufskrankheit auch Empfehlungen zur Sachbearbeitung. Gegen diese Bearbeitungshinweise habe ich im Hinblick auf die §§ 199 Abs. 3 und 200 Abs. 2 SGB VII datenschutzrechtliche Bedenken.

Nach den Empfehlungen des BK-Reports wird zum einen das in § 199 Abs. 3 SGB VII geregelte abgestufte Feststellungsverfahren unterlaufen, da Auskünfte zu den Gesundheitsdaten des Betroffenen von Ärzten, Krankenkas-

sen und anderen Stellen bereits nach den Ersterhebungen bei dem Versicherten möglich sein sollen. Demgegenüber setzt die Erhebung medizinischer Daten in § 199 Abs. 3 SGB VII voraus, dass zuvor hinreichende Anhaltspunkte für den ursächlichen Zusammenhang zwischen der versicherten Tätigkeit und der schädigenden Einwirkung festgestellt sein sollen. Von dieser Reihenfolge kann nur abgewichen werden, wenn die Expositionsermittlung in besonders gelagerten Einzelfällen zu einem unverhältnismäßigen Aufwand führen würde.

Zum anderen ist die Empfehlung des BK-Reports zur arbeitsmedizinischen Beratung weder mit § 200 Abs. 2 SGB VII noch mit den Verhandlungsergebnissen über Abgrenzungskriterien von Gutachter und beratendem Arzt (s. o. Nr. 23.1) vereinbar. Der beratende Arzt soll mit einer Beurteilung nach Aktenlage oder mit einer Untersuchung beauftragt werden können, ohne dem Betroffenen das in § 200 Abs. 2 SGB VII enthaltene Gutachterauswahlrecht einzuräumen. Demgegenüber argumentiert der HVBG, die ärztlichen Feststellungen seien eine „Anknüpfungstatsache“, um überhaupt in eine Kausalitätsprüfung zwischen Einwirkung und Erkrankung eintreten zu können. Dagegen beginnt das unfallversicherungsrechtliche Anerkennungs- und Feststellungsverfahren bereits mit der BK-Verdachtsanzeige, in dem § 200 Abs. 2 SGB VII anzuwenden ist. In den gesetzlichen Regelungen findet die Konstruktion eines „Vorfelds einer Begutachtung“ keine Grundlage.

Inzwischen hat der HVBG erklärt, dass in der demnächst erscheinenden Neuauflage des BK–Reports keine Verfahrensempfehlungen mehr enthalten sind.

23.1.2 Vorschlagsrecht des Versicherten

Das Recht des Versicherten, vor einem Gutachtenauftrag i. S. des § 200 Abs. 2 SGB VII selbst einen oder mehrere Gutachter vorzuschlagen, war schon in der Gesetzesbegründung zu § 200 Abs. 2 SGB VII genannt und ist zwischenzeitlich mehrfach vom BMA bestätigt worden. Dieses hat klargestellt, dass die von den Versicherten vorgeschlagenen Gutachter von den Unfallversicherungsträgern grundsätzlich beauftragt würden, wenn diese geeignet sind. Sollte dem Vorschlag eines Versicherten nicht gefolgt werden, sei die Ablehnung nachvollziehbar zu begründen.

Demgegenüber war das Gutachtervorschlagsrecht von Berufsgenossenschaften in verschiedenen Eingabefällen zunächst abgelehnt und erst auf meine Intervention eingeräumt worden. In anderen Fällen waren die vorgeschlagenen Gutachter ohne oder mit kaum nachvollziehbaren Begründungen als nicht geeignet abgelehnt worden. So hatte eine Berufsgenossenschaft ausgeführt, geeignet seien nur Gutachter, die der Berufsgenossenschaft bereits bekannt seien. Eine andere Berufsgenossenschaft hatte den Chefarzt eines Krankenhauses als Gutachter u. a. abgelehnt, weil die Versicherte sich bereits drei Wochen in seiner stationären Behandlung befunden hatte, und es somit an der Unvoreingenommenheit fehle.

In meinem 17. TB habe ich noch berichtet, dass Versicherte von keiner Berufsgenossenschaft auf ihr Vorschlagsrecht hingewiesen wurden und deshalb in den Verhandlungen über die Musterdienstanweisung – Datenschutz mit dem HVBG ein „Pilotprojekt“ vereinbart wurde (vgl. 17. TB Nr. 23.4.1). Dieses Projekt ist zwischenzeitlich von einer Berufsgenossenschaft mit sehr positiven Erfahrungen umgesetzt worden: Mit dem Schreiben zum Gutachtervorschlag wurde der Versicherte auf sein Recht hingewiesen, selbst einen Gutachter vorzuschlagen. Zugleich wurde er darüber informiert, ob und ggf. welcher Gutachter für die Berufsgenossenschaft auch als beratender Arzt tätig ist. Die Auswertung wurde für Unfallverfahren und BK–Verfahren getrennt vorgenommen. In den Unfallverfahren wurde von den Versicherten in keinem Fall von dem eigenen Gutachtervorschlagsrecht Gebrauch gemacht, da die Berufsgenossenschaften im Regelfall den behandelnden Arzt für ein Gutachten vorschlugen, der den Versicherten am besten kennt und zu dem bereits ein Vertrauensverhältnis besteht. In den BK-Verfahren waren fast 70 % der Versicherten mit dem von der Berufsgenossenschaft an erster Stelle genannten Gutachter einverstanden. In etwa 10 % der Fälle haben die Versicherten eigene Gutachter vorgeschlagen, die überwiegend beauftragt werden konnten und deren Gutachten nur zu einem äußerst geringen Prozentsatz nicht hinreichend begründet waren oder Abweichungen zu allgemeinen Erfahrungssätzen aufwiesen.

Die ursprünglichen Befürchtungen, dass die Versicherten ungeeignete Gutachtervorschläge unterbreiten und sich die Verfahren dadurch wesentlich verzögern würden, haben sich insgesamt nicht bestätigt. Die Erfahrungen waren im Gegenteil so überzeugend, dass die Berufsgenossenschaft, die das Pilotverfahren durchgeführt hat, künftig in allen Bezirksverwaltungen entsprechende Hinweise an die Versicherten geben wird. Angesichts vieler Vorbehalte anderer Berufsgenossenschaften gegen ein ausdrückliches Vorschlagsrecht des Versicherten findet das Vorgehen dieser Berufsgenossenschaft meine volle Anerkennung.

Um die Auswirkungen der Hinweise auf das Gutachtervorschlagsrecht besser einschätzen zu können, ist nunmehr vor einer Empfehlung des HVBG, dieses Verfahren allgemein umzusetzen, vorgesehen, dass zwei weitere Berufsgenossenschaften das Pilotverfahren durchführen.

23.1.3 Gutachtenauftrag unter Ausschluss der Betroffenen

Immer noch höre ich von vielen Versicherten der gesetzlichen Unfallversicherung, dass ihr Recht nach § 200 Abs. 2 SGB VII, vor Erteilung eines Gutachtenauftrages aus mehreren vorgeschlagenen einen Gutachter auswählen zu können und auch selbst Gutachter vorzuschlagen, eingeschränkt wird. Ich habe dabei die Erfahrung gemacht, dass Berufsgenossenschaften insbesondere in schwierigen oder von der Routine abweichenden Fallkonstellationen dazu neigen, die Rechte nach § 200 Abs. 2 SGB VII restriktiv auszulegen. Begründet wird diese Haltung damit, dass die Inanspruchnahme von Selbstbestim-

mungsrechten das Verfahren komplizieren und zu zeitlichen Verzögerungen führen könnte.

Ich halte solche Befürchtungen und Vorbehalte für grundlos. Sachgerechte Lösungen können – gerade in schwierigen Einzelfällen – nur dann gefunden werden, wenn der Versicherte in das Verfahren als Rechtssubjekt miteinbezogen wird. Mit dem Gutachterauswahl- und -vorschlagsrecht nach § 200 Abs. 2 SGB VII hat der Gesetzgeber hierzu einen wichtigen Schritt getan und dem Versicherten Rechte auf Mitwirkung und Transparenz im Verfahren eingeräumt.

Zwischen diesen Rechten und der angestrebten Beschleunigung von Verfahren besteht kein notwendiger Gegensatz. Nach aller Lebenserfahrung wird es im Gegenteil zur Verfahrensbeschleunigung beitragen, wenn der Versicherte die Entscheidung des Unfallversicherungsträgers akzeptieren kann. Dies wird selbst bei Ablehnung des Antrags dann eher der Fall sein, wenn der Versicherte das ihn betreffende Verfahren durchschauen kann und er nicht den Eindruck gewinnt, dass etwas hinter seinem Rücken geschieht. Dieses wird auch – zumindest hinsichtlich des Vorschlagsrechtes – durch das vorstehend unter Nr. 23.1.2 erwähnte erfolgreich durchgeführte Pilotverfahren bestätigt.

23.1.3.1 Gutachten aufgrund „anonymisierter" Daten

Um den Versicherten nicht mehrere Gutachter zur Auswahl vorschlagen oder den Gutachtenvorschlägen der Versicherten folgen zu müssen, übermittelt eine Berufsgenossenschaft Daten der Versicherten ohne Nennung von Namen an einen Gutachter zur Stellungnahme. Nach Auffassung der Berufsgenossenschaft ist in diesem Fall keine datenschutzrechtliche Frage berührt, da es sich nicht um die Bekanntgabe personenbezogener Daten an einen Dritten handele. Eventuelle Bedenken im Hinblick auf § 200 Abs. 2 SGB VII beträfen nicht den Datenschutz, sondern seien ausschließlich Verfahrensfragen, die nicht meiner Zuständigkeit unterlägen.

Diese Argumentation vermag nur unzureichend den Eindruck zu verschleiern, dass auf diese Weise durchgeführte Gutachterbeauftragungen einer datenschutzrechtlichen Kontrolle entzogen werden sollen. Sie hält aber auch rechtlichen Anforderungen nicht Stand. Durch die Rechte des § 200 Abs. 2 SGB VII soll der Sozialdatenschutz in bestimmten Verfahrenssituationen gestärkt werden. Diese Vorschrift trifft zwar auch eine Regelung, auf welche Art und Weise ein Beweismittel einzuholen ist, gibt dem Betroffenen aber zugleich ein Recht auf Mitwirkung in dem Verfahren. Das Mitwirkungsrecht beruht unmittelbar auf dem Recht auf informationelle Selbstbestimmung und betrifft damit den Kernbereich des Datenschutzes. Dass auch der Gesetzgeber dies so gesehen hat, zeigt die Einordnung der Vorschrift unter das 8. Kapitel des SGB VII, das mit „Datenschutz" überschrieben ist. Zudem ist durch die beschriebene Verfahrensweise die Transparenz des Verfahrens nicht mehr gegeben. Diese zählt als grundlegendes Element des Datenschutzes – neben dem Mitwirkungsrecht des Betroffenen – ebenfalls zum datenschutzrechtlichen Inhalt der Vorschrift.

Unabhängig von dieser Beurteilung stellt sich insbesondere vor dem Hintergrund der Novellierung des BDSG die Frage, ob eine Anonymisierung von Versichertendaten bei der Übersendung an einen Gutachter mit der Bitte um Stellungnahme überhaupt möglich ist. Dem Gutachter soll zwar der Name des Versicherten nicht genannt werden. Es ist aber beabsichtigt, das auf den Daten des Versicherten basierende Gutachten in seinem Verfahren zu verwenden. Damit muss das Gutachten dem Versicherten wieder zugeordnet werden können. Für die Bewertung, ob ein Personenbezug vorliegt, sind die strengeren Maßstäbe der Anonymisierung nach dem BDSG-Entwurf heranzuziehen: Danach müssen nicht nur die personenbezogenen Daten des Versicherten, sondern auch alle Angaben, die Rückschlüsse auf dessen Identität möglich machen – wie beispielsweise Namen von Gutachtern, Ärzten und Arbeitgebern – unkenntlich gemacht werden. Schon bei außergewöhnlichen Erkrankungen oder Abläufen kann aber eine Zuordnung möglich sein. Zur Klärung dieser Frage führe ich mit der betroffenen Berufsgenossenschaft Gespräche. Ich hoffe, dass ich die Berufsgenossenschaft davon überzeugen kann, dass ein valides Gutachten einfacher und besser zu erhalten ist, wenn dem Versicherten mehrere Gutachter zur Auswahl vorgeschlagen werden oder ein von ihm vorgeschlagener Gutachter beauftragt wird, als durch eine mühevolle und sicherlich oft nicht erreichbare Anonymisierung.

23.1.3.2 Gutachten während eines Gerichtsverfahrens

An mich ist die Frage gerichtet worden, ob § 200 Abs. 2 SGB VII auch dann anzuwenden ist, wenn während eines anhängigen Sozialgerichtsverfahrens ein neues Gutachten zu der Frage in Auftrag gegeben wird, ob ein ursächlicher Zusammenhang zwischen Exposition am Arbeitsplatz und Erkrankung des Versicherten besteht. In mehreren Eingabefällen hatte ein vom Sozialgericht beauftragter Gutachter eine von der Entscheidung der jeweiligen Berufsgenossenschaft abweichende Auffassung vertreten, und die Berufsgenossenschaften wollten nun vor dem Sozialgericht anhand eines neuen Gutachtens eine medizinisch fundierte Stellungnahme dazu abgeben.

Nach dem Wortlaut des § 200 Abs. 2 SGB VII, wonach der Unfallversicherungsträger dem Versicherten vor Erteilung eines Gutachtenauftrages mehrere Gutachter zur Auswahl benennen soll, ist die Vorschrift auch in diesem Fall anzuwenden. Die Geltung der Vorschrift erstreckt sich auf das unfallversicherungsrechtliche Verfahren bis zur Bestandskraft bzw. Rechtskraft des Bescheides. Eine Einschränkung auf das Verfahren bis zur Entscheidung über den Widerspruch besteht nicht. Zwar ist nicht von der Hand zu weisen, dass diese Fallkonstellation nicht dem Regelfall des § 200 Abs. 2 SGB VII entspricht. Auch kommt die mit der Vorschrift beabsichtige Stärkung der Mitwirkungsrechte des Versicherten gegenüber den Unfallversicherungsträgern hier nicht insoweit zum Tragen,

als die Entscheidung über den Antrag des Versicherten nicht von einer Berufsgenossenschaft, sondern von dem Sozialgericht getroffen wird. Da dieses Gutachten aber nicht allein für eine Stellungnahme gegenüber dem Sozialgericht Bedeutung haben kann, halte ich eine Einholung durch die Berufsgenossenschaft in den Fällen für bedenklich, wenn der ursprüngliche Bescheid von dem Unfallversicherungsträger oder dem Sozialgericht aufgehoben wird und das Gutachten weiterhin in den Akten des Versicherten verbleibt. Denn dieses Gutachten könnte als Grundlage einer neuen Entscheidung der Berufsgenossenschaft dienen oder in sonstiger Weise Einfluss auf die Entscheidung eines Sachbearbeiters oder gegebenenfalls eines neuen Gutachters haben, obwohl dem Versicherten bei der Beauftragung des Gutachters nicht die Rechte des § 200 Abs. 2 SGB VII gewährt wurden, weil das Gutachten lediglich im Prozessverfahren als Parteiäußerung oder Beweismittel zu verstehen ist. Ein solches Ergebnis wäre mit der Intention der Vorschrift nicht vereinbar.

Ich bemühe mich, mit einzelnen Berufsgenossenschaften und auch dem HVBG in dieser schwierigen Situation eine praktikable und datenschutzfreundliche Lösung zu finden. Ein abschließendes Ergebnis konnte bislang nicht erzielt werden.

23.2 Noch ungewisse Folgen, wenn § 200 Abs. 2 und § 199 Abs. 3 SGB VII nicht beachtet werden

Auch im Zusammenhang mit Verstößen gegen datenschutzrechtliche Vorschriften stellt sich die Frage nach den Rechtsfolgen. Nach § 84 Abs. 2 Satz 1 SGB X besteht ein einklagbarer Anspruch auf die Löschung von Sozialdaten, wenn die Speicherung dieser Daten unzulässig ist.

Probleme bereitet das datenschutzrechtliche Löschungsgebot in noch nicht abgeschlossenen Verwaltungsverfahren. Einschlägige Kommentierungen hierzu gehen überwiegend davon aus, dass Verstöße gegen datenschutzrechtliche Vorschriften im Regelfall als bloße Verfahrensfehler zu behandeln sind, die vom Betroffenen nicht gesondert, sondern nur im Zusammenhang mit einer Sachentscheidung angefochten werden können. Zuzugeben ist, dass ein gesondert durchzusetzendes Löschungsgebot nur dann verwaltungsökonomisch sinnvoll ist, wenn bei Beachtung der fraglichen datenschutzrechtlichen Vorschrift eine andere Entscheidung in der Sache möglich gewesen wäre. Insofern erscheint es sachgerecht, ausgehend von dem datenschutzrechtlichen Löschungsgebot die Rechtsfolgen im laufenden Verfahren nach den in §§ 40 ff. SGB X festgelegten Maßstäben für verwaltungsrechtliche Verfahrensvorschriften zu beurteilen. In diesen Vorschriften ist eine Wertung hinsichtlich der Möglichkeit einer anders lautenden Sachentscheidung und der Schwere der nichtbeachteten Vorschriften enthalten.

Fragen nach den Rechtsfolgen bei Nichtbeachtung datenschutzrechtlicher Vorschriften haben im Berichtszeitraum insbesondere bei der Verletzung des Gutachterauswahl– und -vorschlagsrechts nach § 200 Abs. 2 SGB VII eine große Rolle gespielt. Ihre Beantwortung ist deshalb von besonderer Wichtigkeit, da die Löschung eines unzulässigerweise eingeholten Gutachtens für die Entscheidung über den Antrag selbst unmittelbaren Einfluss haben kann.

Nach den Regelungen des Sozialgesetzbuchs muss ein Verstoß gegen das Gutachterauswahlrecht auch nach der Auffassung, die von einem bloßen Verfahrensfehler im Sinne des § 42 SGB X ausgeht, zu einer Löschung des Gutachtens führen. Denn wendet man diese Vorschrift auf das Gutachterauswahlrecht an, kann allenfalls noch eine Parallele zu einer unterbliebenen Anhörung nach § 42 Satz 2 SGB X gezogen werden, wonach die Unbeachtlichkeit von Verfahrensmängeln ausgeschlossen ist. Die Gleichwertigkeit des Anhörungsrechts und des Gutachterauswahl- und -vorschlagsrechts wird daran deutlich, dass beide Rechte auf einem Grundrecht bzw. einem diesem gleichgestellten Recht beruhen und dem Betroffenen Beteiligungsrechte im Verfahren einräumen. Dabei geht das Auswahlrecht des § 200 Abs. 2 SGB VII in seiner Rechtswirkung noch über die einer bloßen Anhörung hinaus. Denn während der Unfallversicherungsträger seine Entscheidung ungeachtet des Ergebnisses einer Anhörung treffen kann, ist er an die Gutachterauswahl des Versicherten gebunden. In Anbetracht der Stärke des Gutachterauswahlrechts ist es daher gerechtfertigt, die Löschung des Gutachtens unabhängig vom Verfahren durchzusetzen.

Anders verhält es sich dagegen bei einem Verstoß gegen die datenschutzrechtliche Vorschrift des § 199 Abs. 3 SGB VII. Danach dürfen Auskünfte zu Vorerkrankungen erst eingeholt werden, wenn Anhaltspunkte für die Exposition vorliegen. Bei Nichtbeachtung dieser Vorschrift wird zwar die vom Gesetzgeber vorgesehene Staffelung bei den Eingriffen in die Rechte des Betroffenen nicht eingehalten. Ein Beteiligungsrecht, das u. U. zu einer anderen Entscheidung in der Sache führen könnte, ist aber nicht betroffen. Da die Vorschrift in ihrem Regelungsgehalt dabei mit einer Verfahrensvorschrift vergleichbar ist, halte ich es für sachgerecht, in diesen Fällen die Regelung über die Unbeachtlichkeit von Verfahrensmängeln anzuwenden.

Ich habe Gespräche zu dieser Thematik mit den betroffenen Berufsgenossenschaften und dem HVBG aufgenommen. Ein Ergebnis konnte bis zum Redaktionsschluss nicht erzielt werden.

23.3 Verträge zur Durchführung der Heilbehandlung nach § 34 Abs. 3 SGB VII

Zur Durchführung der Heilbehandlung, der Vergütung der Ärzte und Zahnärzte sowie über die Art und Weise der Abrechnung schließen die Verbände der Unfallversicherungsträger mit der Kassenärztlichen und der Kassenzahnärztlichen Bundesvereinigung Verträge, deren we-

sentlicher Anwendungsfall das Durchgangsarztverfahren ist. Im Berichtszeitraum hat mir der Vertrag mit der Kassenärztlichen Bundesvereinigung zur Stellungnahme nach § 34 Abs. 3 Satz 2 SGB VII vorgelegen. Nach eingehender Überprüfung des Vertragsentwurfs habe ich meine im 17. TB (vgl. Nr. 23.1.2) zum Vertrag mit der Kassenzahnärztlichen Bundesvereinigung geäußerten Bedenken gegen die Datenerhebung zu „Unfallhergang und -zeitpunkt“ im Hinblick auf die besondere Interessenlage beim Durchgangsarztverfahren zurückgestellt.

In dem Durchgangsarztverfahren erfragt der Arzt von dem Versicherten die Angaben zu Unfallhergang und -zeitpunkt. Nach der gesetzlichen Regelung des § 193 SGB VII hat grundsätzlich der Arbeitgeber diese Angaben binnen drei Tagen mit einer Unfallanzeige mitzuteilen, wenn der Versicherte mehr als drei Tage arbeitsunfähig ist. Vor dem Hintergrund der vertraglichen Gestaltung des Durchgangsarztverfahrens ist eine zusätzliche Erhebung dieser Daten durch den Arzt aber nicht zwingend als unzulässige Mehrfacherhebung anzusehen. Nach dem Vertrag hat der Arzt sofort die Entscheidung zu treffen, ob bei dem Unfall des Verletzten die Voraussetzungen eines Versicherungsfalls vorliegen, für den ein Unfallversicherungsträger die Kosten zu übernehmen hat. Diese Entscheidung über die Leistungsverpflichtung ist für den Unfallversicherungsträger solange verbindlich, bis er nachträglich eine – möglicherweise auf weiteren Tatsachen oder rechtlichen Würdigungen beruhende – andere Entscheidung trifft. Rückwirkend findet aber keine Änderung der Kostentragung statt. Wegen der weitreichenden Auswirkungen der Entscheidung des Durchgangsarztes ist daher eine schnellstmögliche Überprüfung der Leistungspflicht durch den Unfallversicherungsträger unter Heranziehung aller relevanten Angaben erforderlich.

Die schnelle Klärung, ob ein Versicherungsfall vorliegt, liegt letztlich im Interesse des Versicherten. Im Einzelfall kann davon der Ablauf des Heilverfahrens abhängen, da für die Versicherten der Berufsgenossenschaften besondere Krankenhäuser bestehen und spezielle insbesondere kostenintensive Behandlungsformen übernommen werden, mit denen gegebenenfalls ein vorteilhaftes Heilverfahren eingeleitet werden kann.

In dem Durchgangsarztverfahren ist es aber unerlässlich, dass die Transparenz des Verfahrens sichergestellt ist und der Versicherte die Möglichkeit hat, seine Angaben beim Durchgangsarzt zu vervollständigen oder richtig zu stellen. Deshalb informiert der Durchgangsarzt den Versicherten über die Übermittlung des Arztberichts an die Berufsgenossenschaft und überreicht ihm auf Wunsch eine Kopie des Berichts. In den Fällen, in denen der Durchgangsarzt Bedenken gegen die Angaben des Versicherten bzw. gegen den Unfallhergang oder den Befund im Bericht äußert, wird dem Versicherten in jedem Fall eine Durchschrift des Arztberichts ausgehändigt.

Gegen diese Handhabung des Durchgangsarztverfahrens habe ich gegenwärtig keine datenschutzrechtlichen Bedenken. Durch stichprobenartige Überprüfungen in diesem Bereich der Unfallverfahren werde ich mich darüber vergewissern, ob man sich in der Praxis an die Vorgaben des Gesetzgebers hält.

23.4 Datenschutz in Formularen

23.4.1 Verbesserungswürdige Vordrucke für Eröffnungsschreiben

Die Umsetzung der bereichsspezifischen datenschutzrechtlichen Vorschriften des SGB VII lässt sich in den sog. Massenverfahren der Berufsgenossenschaften am wirkungsvollsten anhand der Formulargestaltung beobachten und überprüfen, weshalb ich in meinen Kontrollen einen Schwerpunkt auf die Prüfung der aktuell verwendeten Vordrucke in Feststellungsverfahren und bei einigen Berufsgenossenschaften auf aus datenschutzrechtlicher Sicht bedeutsame Formulare gelegt habe. Eine einheitliche Bilanz zur Formulargestaltung lässt sich nicht ziehen, da keine einheitlichen Vordrucke für alle Unfallversicherungsträger bestehen und die bestehenden kontinuierlich überarbeitet werden. An die Vordrucke, die ein Formularausschuss beim HVBG den Berufsgenossenschaften zur Verfügung stellt, sind die einzelnen Berufsgenossenschaften nicht gebunden. Deshalb und wegen vieler jeweils spezifischer Einzelfragen, in denen datenschutzfreundlichere Formulierungen und die Aufnahme gesetzlicher Hinweise wünschenswert sind, ist besonders hervorzuheben, dass die Berufsgenossenschaften überwiegend bereit sind, Verbesserungsvorschläge aufzugreifen und in der neuen Formulargestaltung umzusetzen.

Fast alle Berufsgenossenschaften übersenden den Versicherten zu Beginn des Feststellungsverfahrens ein sog. Eröffnungsschreiben, mit dem sie die Versicherten über den Verlauf des Verfahrens informieren und ihre Rechte und Pflichten umfassend erläutern. Bei einer Berufsgenossenschaft fiel mir auf, dass sie wegen der besseren Verständlichkeit vollständig auf die Nennung von gesetzlichen Vorschriften verzichtet. Zwar ist das Eröffnungsschreiben dieser Berufsgenossenschaft in einer bürgernahen Sprache abgefasst und daher gut verständlich. Ich halte es aber im Sinne einer informierten Beteiligung des Versicherten für erforderlich, dass nachvollziehbar ist, aus welcher gesetzlichen Grundlage seine Rechte und Pflichten resultieren. Ich habe daher empfohlen, wenigstens die wichtigsten Vorschriften zu nennen oder ihren Text beizufügen.

23.4.2 Umsetzung des Ersterhebungsgrundsatzes

Bei der Kontrolle der Einbeziehung des Versicherten in das Verfahren konnte ich in einem Fall feststellen, dass die Berufsgenossenschaft den Ersterhebungsgrundsatz nach Maßgabe des § 67a Abs. 2 Satz 1 SGB X i.V.m. § 60 Abs. 1 Nr. 1 zweite Alternative SGB I konsequent umsetzt. Der Versicherte wird darauf hingewiesen, dass die Berufsgenossenschaft nach den gesetzlichen Vorschriften des Sozialgesetzbuches verpflichtet ist, die für die Ermittlung erforderlichen Sozialdaten zunächst unter seiner

Mitwirkung, d. h. bei ihm oder mit seiner Zustimmung bei Dritten, zu erheben, da Sozialdaten nicht ohne Wissen des Betroffenen erhoben und gespeichert werden dürfen. Erst wenn der Betroffene seine Zustimmung erteilt oder nach einer Frist ohne Nennung von Gründen nicht antwortet, erhebt die Berufsgenossenschaft die Daten des Versicherten nach den gesetzlichen Vorschriften des SGB VII.

In einem anderen Fall überlässt die Berufsgenossenschaft dem Versicherten die Beibringung der für das Ermittlungsverfahren erforderlichen Unterlagen. Da es nach dem Ersterhebungsgrundsatz nicht darum geht, dass alle Anfragen im Sinne einer inhaltlichen Beantwortung an den Versicherten selbst zu richten sind, habe ich Bedenken, ob diese Art der Einbeziehung des Versicherten in das Verfahren datenschutzrechtlichen Grundsätzen entspricht. Das gilt insbesondere, wenn dem auf diese Weise in das Verfahren einbezogenen Antragsteller mangelnde Mitwirkung auch in den Fällen zur Last gelegt wird, in denen er die geforderten Daten und Angaben selbst nicht oder nicht vollständig erbringen kann. Denn ein Versicherter kann möglicherweise nicht immer zutreffend beurteilen, welche inhaltlichen Grenzen durch die datenschutzrechtlichen Vorschriften des Sozialgesetzbuches für das Auskunftsbegehren der Berufsgenossenschaft und die Auskunftsbefugnis der übermittelnden Stellen gezogen werden. Deshalb sollte dem Versicherten zumindest im Eröffnungsschreiben oder in einer beigefügten Verfahrensbeschreibung im einzelnen erläutert werden, welche Auskünfte unmittelbar von ihm und welche mit seiner Zustimmung beispielsweise bei Ärzten oder bei seiner Krankenkasse erhoben werden sollen.

23.4.3 Antragsformular und Vorerkrankungsverzeichnis

Aufgrund vieler Eingaben musste ich feststellen, dass sich die gesamten Vorerkrankungsverzeichnisse in den Akten der Berufsgenossenschaften befanden, obwohl das Auskunftsverlangen gegenüber den Krankenkassen nach § 188 Satz 2 SGB VII auf solche Erkrankungen beschränkt werden soll, die mit dem Versicherungsfall in einem ursächlichen Zusammenhang stehen können. Kontrollen bei Berufsgenossenschaften bestätigten diesen Eindruck, wobei zudem das Anfrageformular keine entsprechende Formulierung enthält. In einem Rundschreiben des HVBG an die Mitgliedsberufsgenossenschaften und die Landesverbände war sogar ausgeführt worden, dass eine Beschränkung des Auskunftsverlangens im Bereich des Feststellungsverfahrens von Berufskrankheiten nicht möglich sei. Der mit dem Rundschreiben versandte Formtext zur Anfrage von Vorerkrankungen entsprach denn auch in wesentlichen Punkten nicht datenschutzrechtlichen Anforderungen, da weder die angezeigte Berufskrankheit noch die angezeigte Erkrankung genannt wurden, obwohl die ersuchende Stelle diese Angaben benötigt, um die Voraussetzungen des § 188 Satz 2 SGB VII prüfen zu können. Ebenfalls fehlten Hinweise auf die Zulässigkeit der Erhebung und darauf, dass der Versicherte auf ein Widerspruchsrecht hingewiesen worden war.

Auf meine Intervention hin hat der Formularausschuss weitreichende Änderungen vorgenommen, so dass der Vordruck die gesetzlichen Vorgaben nunmehr berücksichtigt. Er enthält die Angabe der Erkrankung bzw. des Unfalls und die Möglichkeit, die Nummer einer Berufskrankheit einzutragen. Er stellt klar, dass die gesetzlichen Voraussetzungen für eine Datenübermittlung vorliegen. Diese datenschutzfreundlichen Grundsätze sollen auch für die Datenerhebungen nach §§ 201, 203 SGB VII bei behandelnden und vorbehandelnden Ärzten gelten.

Auch wenn Formulare von vielen oft als abschreckend empfunden werden, besteht für Betroffene die Chance, konkrete Informationen zu ihrem Verfahren, dessen Ablauf sowie zu den bestehenden Rechten und Pflichten zu erhalten und so ihre Mitwirkungsrechte wahrzunehmen. Wegen der großen Wirkung, die von der datenschutzgerechten Ausgestaltung von bestimmten Vordrucken für viele Verfahren und damit für zahlreiche Betroffene ausgeht, wird die Verbesserung von Vordrucken weiterhin eine meiner Aufgaben sein.

24 Pflegeversicherung Rehabilitations- und Schwerbehindertenrecht

24.1 Pflegeversicherung

24.1.1 Pflege-Qualitätssicherungsgesetz, Änderung des Heimgesetzes

Die Bundesregierung hat am 1. November 2000 die Entwürfe eines Pflege-Qualitätssicherungsgesetzes und eines Dritten Gesetzes zur Änderung des Heimgesetzes beschlossen. Die Ziele beider Gesetzentwürfe liegen in der Sicherung und in der Weiterentwicklung der Pflegequalität und die Stärkung der Verbraucherrechte. Beide Gesetzentwürfe ergänzen einander in dem Ziel, u. a. durch eine engere Zusammenarbeit zwischen der Pflegeselbstverwaltung und der staatlichen Heimaufsicht die Qualität der Betreuung in Heimen zu sichern.

Die in beiden Gesetzentwürfen vorgesehene Prüfung von Pflegeeinrichtungen und Heimen und die Einschaltung von Sachverständigen bei der Durchführung von Prüfungen sowie die verstärkte Zusammenarbeit von Heimaufsicht mit den Pflegekassen, dem medizinischen Dienst der Krankenversicherung und den Trägern der Sozialhilfe bei der Durchführung und der Umsetzung der Prüfungen führen zu einem verstärkten Informationsaustausch. Um Pflegeeinrichtungen qualifiziert kontrollieren zu können und um auf diese Weise eventuelle Missstände, gegen die sich vielfach die Betroffenen selbst oft nur bedingt wehren können, zu erkennen und zu beheben, ist es einerseits erforderlich, auch Einzelfälle personenbezogen zu überprüfen. Andererseits darf dies aber nicht dazu führen, dass die persönlichen Daten der betroffenen, häufig pflegebe-

dürftigen, älteren Menschen dem Qualitätsmanagement schutzlos geopfert werden.

Bei der Vorbereitung beider Gesetzentwürfe habe ich nach Abstimmung mit den Landesbeauftragten für den Datenschutz den federführenden Bundesministerien (BMG und BMFSFJ) Hinweise zum Datenschutz gegeben. Dabei habe ich insbesondere gebeten, zu überprüfen, ob die Datenübermittlungen in dem vorgesehenen Umfang tatsächlich erforderlich sind, ob der Kreis der Empfänger von Datenübermittlungen nicht eingeschränkt werden kann und ob Daten immer personenbezogen übermittelt werden müssen oder ob nicht eine anonymisierte Datenübermittlung ausreicht. Beide Bundesministerien waren bereit, die aus datenschutzrechtlicher Sicht erforderliche Ergänzung der Gesetzentwürfe vorzunehmen. Dabei sind die von mir gegebenen Anregungen im wesentlichen aufgegriffen worden.

Ich gehe davon aus, dass auch im Rahmen der parlamentarischen Beratungen der Gesetzentwürfe meinem Anliegen, den Datenschutz auch in diesem sensiblen Bereich der Pflegeeinrichtungen und Heime und deren Kontrolle zu stärken, Rechnung getragen wird.

24.1.2 Gemeinsame Verarbeitung und Nutzung personenbezogener Daten durch Kranken- und Pflegekassen

Mit der Umsetzung des § 96 SGB XI, der die Rahmenbedingungen für die gemeinsame Verarbeitung und Nutzung personenbezogener Daten durch Krankenkassen und Pflegekassen festlegt, durch die Spitzenverbände der Pflegekassen und der Krankenkassen habe ich mich bereits mehrfach befasst (vgl. 16. TB Nr. 24.1, 17. TB Nr. 24.1). § 96 SGB XI sieht eine Festlegung der von den Krankenkassen und Pflegekassen gemeinsam zu verarbeitenden und zu nutzenden Daten vor; im Hinblick auf die von den Kassen verwendeten unterschiedlichen Programme und Systeme ist es aber nicht gelungen, den Datenkatalog zu präzisieren (vgl. 16. TB Nr. 24.1). Im Interesse eines praktikablen Gesetzesvollzugs habe ich eine Änderung des § 96 SGB XI vorgeschlagen; hiernach dürfen die nach § 46 Abs. 1 SGB XI verbundenen Pflege- und Krankenkassen personenbezogene Daten, die zur Erfüllung gesetzlicher Aufgaben jeder Stelle erforderlich sind, gemeinsam verarbeiten und nutzen. Auf meine Initiative hin ist eine entsprechende Änderung des § 96 SGB XI während der parlamentarischen Beratungen in den Entwurf eines Gesetzes zur Reform der gesetzlichen Krankenversicherung ab dem Jahr 2000 (GKV-Gesundheitsreformgesetz 2000) aufgenommen worden (vgl. BT–Drs. 14/1977). In dem am 1. Januar 2000 in Kraft getretenen Gesetz (BGBl. I S. 2626), das Ergebnis eines Vermittlungsverfahrens ist, ist diese Änderung des § 96 SGB XI jedoch nicht mehr enthalten.

Auf meine Veranlassung ist die von mir vorgeschlagene Änderung des § 96 SGB XI aber nunmehr in den Entwurf eines Gesetzes zur Qualitätssicherung und zur Stärkung des Verbraucherschutzes in der Pflege (Pflege-Qualitätssicherungsgesetz) aufgenommen worden, der am 1. November 2000 von der Bundesregierung beschlossen worden ist. Es wäre zu begrüßen, wenn die nunmehr vorgesehene Änderung des § 96 SGB XI alsbald in Kraft treten würde.

24.2 Rehabilitations- und Schwerbehindertenrecht

Zum Ende des Berichtszeitraums wurde mir der Referentenentwurf zum Sozialgesetzbuch, Neuntes Buch – SGB IX – vom BMA zur Stellungnahme zugeleitet. Mit dem Gesetzesvorhaben werden die bundesrechtlichen Regelungen des Rehabilitationsrechts für behinderte Menschen weiterentwickelt und zusammengefasst in das Sozialgesetzbuch eingefügt. Mit diesem gesetzestechnischen Aufbau gelten die allgemeinen Bücher der Sozialgesetzbuches (SGB I, SGB IV, SGB X) auch für das SGB IX. Da das Rehabilitationsrecht – verstanden als Eingliederung von behinderten Menschen in Arbeit, Beruf und Gesellschaft – bereits als Teil-Aufgabe in alle sozialen Sicherungssysteme eingebettet ist, hat das SGB IX als Sonderregelung für Schwerbehinderte auch Geltung für die Arbeitslosenversicherung (SGB III), die Krankenversicherung (SGB V), die Rentenversicherung (SGB VI), die Unfallversicherung (SGB VII), die Kinder- und Jugendhilfe (SGB VIII) und die Pflegeversicherung (SGB XI). Bereichsspezifische datenschutzrechtliche Regelungen sind im Entwurf des SGB IX nicht vorgesehen, so dass die Datenschutzvorschriften der einzelnen Bücher, ergänzt durch die allgemeinen datenschutzrechtlichen Regelungen des SGB X, auch im Rehabilitationsrecht anzuwenden sind.

Mit dem Rehabilitations- und Schwerbehindertenrecht soll die Koordinierung der Leistungen für behinderte Menschen und die Kooperation der beteiligten Stellen (z. B. Hauptfürsorgestellen, Selbsthilfeverbände) verbessert werden. Diese begrüßenswerte Zielsetzung und der weitgehende Verzicht auf eine Festlegung von Organisation, Zuständigkeit und Verfahren bei verschiedenen Stellen erschweren jedoch eine datenschutzrechtliche Prüfung des Entwurfs zum SGB IX. Die datenschutzrechtliche Konzeption des Sozialgesetzbuches geht von abgrenzbaren Datenerhebungs- und Datenverarbeitungsschritten aus. Diese sind mit der Nennung von Koordinierungs- und Kooperationsaufgaben zwar vorausgesetzt, aus sich heraus aber nicht klar genug erkennbar. Das zeigt sich insbesondere bei den erstmals im Rehabilitations- und Schwerbehindertenrecht geschaffenen Servicestellen. Diese bieten erste Anlaufstellen für behinderte Menschen. Die Servicestellen haben nicht nur die Aufgabe, zu beraten und zu unterstützen, sondern sie sollen auch die Entscheidung des jeweiligen Rehabilitationsträgers vorbereiten und zwischen mehreren Leistungsträgern koordinieren. Für die mit dieser Aufgabenstellung nicht beschriebenen Datenflüsse sind aber keine Konkretisierungen vorgesehen. Entgegen der Absicht des Gesetzesvorhabens besteht damit das Risiko, dass Daten über schwerbehinderte Menschen ausgetauscht werden, ohne dass deren informationelles Selbstbestimmungsrecht ausreichend geschützt ist.

Deshalb sieht der Entwurf des SGB IX vor, dass die Rehabilitationsträger nähere Regelungen, wie die Zusammenarbeit erfolgen soll, welche Aufgaben im einzelnen bestehen und welche Organisationsformen gewählt werden sollen, in gemeinsamen Empfehlungen vereinbaren. Insgesamt erscheint es daher sinnvoll, datenschutzrechtliche Regelungen in diese Empfehlungen aufzunehmen, mit denen die einzelnen Vorhaben konkretisiert werden sollen. Ich habe gegenüber dem BMA auf eine gesetzliche Regelung gedrungen, nach der ich an der Vereinbarung der gemeinsamen Empfehlungen durch die Rehabilitationsträger zu beteiligen bin.

Zu meinem Bedauern habe ich ein Recht für behinderte Menschen, selbst einen Gutachter vorschlagen zu können, wenn eine Leistung von einer Begutachtung abhängt, nicht durchsetzen können. Das BMA hat sich in dieser Frage an der Regelung des SGB VII orientiert. Insofern sieht der Wortlaut des Entwurfs des SGB IX vor, dass der Rehabilitationsträger wenigstens drei Gutachter benennt. Nach der Begründung können auf Antrag des Leistungsberechtigten auch andere geeignete Sachverständige herangezogen werden.

25 Gesundheitswesen

25.1 Telematik in der Medizin

Gesundheits-Telematik ist der Sammelbegriff für viele unterschiedliche Anwendungen der Telekommunikation und der modernen Informatik im Gesundheitswesen. Dazu gehören das Unterstützen der Betreuung und Behandlung einzelner Patienten, das Gewinnen und Nutzen von Erfahrungen über den Erfolg verschiedener Therapien, aber auch das Rationalisieren von Verwaltungsarbeiten. Ein Musterbeispiel für Gesundheits-Telematik ist die schon heute praktizierte Teleradiologie. Dabei wird das von einer Einrichtung erzeugte digitalisierte Röntgenbild zu einem Spezialisten übertragen, der dazu seine Diagnose stellt und sofort an die Einrichtung sendet, die damit den Patienten ohne wesentliche Verzögerung sachgerecht behandeln kann. Andere, zum Teil erst in der Zukunft zu erwartende Anwendungen sind der elektronische Arztbrief (s. u.Nr. 25.1.2), die virtuelle elektronische Patientenakte (s. 17. TB Nr. 25.2.2) und die Vernetzung medizinischer Einrichtungen (s. 17. TB Nr. 25.2).

Bei den Bemühungen, aus Perspektiven der Telematik nützliche Anwendungen für die Medizin zu realisieren, ist Datenschutz stets ein wichtiges Projektziel. Es besteht ein breiter Konsens über das Prinzip, personenbezogene Gesundheitsdaten nur mit dem Wissen und Wollen des jeweiligen Patienten zu verarbeiten, und darüber, dass wirksame technische und organisatorische Maßnahmen zu treffen sind, damit diese Vorgabe stets eingehalten wird. Denn jede unzulässige Verarbeitung von Gesundheitsdaten schädigt nicht nur den Betroffenen, sondern sie kann auch das notwendige Vertrauen in die generelle Wahrung des Arztgeheimnisses untergraben. Deshalb wirken die Datenschutzbeauftragten des Bundes und der Länder in Gremien zur Förderung der Telematik in der Medizin aktiv mit und unterstützen mit ihrem Rat entsprechende Projekte. Und es ist keineswegs ein Einzelfall, dass Software-Firmen oder andere Akteure auf diesem Gebiet ihre Vorstellungen einem Datenschutzbeauftragten präsentieren, um sich schon bei der Entwicklung beraten zu lassen.

25.1.1 Das Aktionsforum Telematik im Gesundheitswesen

Gemessen an den technischen Möglichkeiten und der Leistungsfähigkeit der entsprechenden Sektoren der Wirtschaft bleibt die Nutzung der Telematik für das Gesundheitswesen deutlich zurück. Ein wesentlicher Grund dafür – vielleicht sogar der entscheidende – ist, dass die erforderliche und über die Grenzen der einzelnen Leistungserbringer hinausreichende Koordinationsarbeit nicht im ausreichenden Umfang geleistet wurde. Dabei geht es nicht nur um die Definition von Datensätzen, der notwendigen Basis automatisierter Kommunikation, sondern auch um die Einbettung der Kommunikation in die Datenverarbeitung der beteiligten Instanzen. Es müssen auch Sicherheits- und Garantiestrukturen erarbeitet werden, damit ein Arzt, der von Kryptografie und den Methoden zur Beurteilung der Angriffsresistenz einzelner Verfahren nichts versteht, nicht verstehen will und auch gar nichts zu verstehen braucht, sich auf die Sicherheit seiner Kommunikation verlassen kann. Nicht zuletzt ist auch dafür zu sorgen, dass derjenige, der für eine andere Einrichtung eine (Informations-)Leistung erbringt, dafür ein angemessenes Honorar enthält. Bezogen auf das Beispiel der Teleradiologie (s. o. Nr. 25.1) müssen u. a. die technischen Standards festgelegt werden, nach denen nicht nur der Spezialist in dem Zentrum, das ein Pilotprojekt durchführt, mit ausgewählten Stellen in seinem Einzugsbereich automatisch diese Daten gesichert austauschen kann, sondern möglichst alle interessierten Stellen das Wissen entsprechender Spezialisten nutzen können. Diese Standards müssen dann so überzeugend vertreten werden, dass die Firmen, die solche Geräte und die Kommunikationsprogramme herstellen, sich daran halten und nicht versuchen, mit Eigenentwicklungen sich Teilmärkte zu schaffen.

Außerdem ist zu klären, ob Namen und Anschriften der Patienten an den Spezialisten zu übermitteln sind. Ein Verzicht auf die medizinisch nicht notwendige Weitergabe dieser Daten wäre sinnvoll, um die Risiken der Datenübertragung so weit wie möglich zu vermindern. Er ist aber dann nicht möglich, wenn diese Daten zur Leis-tungsabrechnung durch den Spezialisten erforderlich sind.

Das Erarbeiten konsistenter Lösungen und ihr wirksames Vertreten im Markt und bei Bedarf auch in der Politik, die für die gesetzlichen Rahmenbedingungen zuständig ist, kann offenbar nicht nur von Personen geleistet werden, die am Rande ihrer beruflichen Tätigkeit sich aus besonderem Interesse auch mit diesen Problemen beschäftigen. Fortschritte in angemessener Zeit benötigen mehr Ar-

beitskraft und mehr Durchsetzungsmacht. Deshalb haben die in der Gesellschaft für Versicherungswissenschaft und -gestaltung e. V. (GVG) zusammen arbeitenden Institutionen das Aktionsforum Telematik im Gesundheitswesen (ATG) gegründet, das zu seiner ersten Plenumsveranstaltung im August 1999 die Interessenten an diesem Thema eingeladen hatte. In der GVG arbeiten die gesetzlichen Sozialversicherungen, private Kranken- und Lebensversicherungen, Ärzte, Apotheker, Krankenhäuser, Arzneimittelhersteller und andere Leistungserbringer sowie Sozialpartner und Wissenschaftler zusammen. Es ist zu hoffen, dass unter dem Dach dieser starken Gemeinschaft überzeugende und breit einsetzbare Verfahren zur Verbesserung der Kommunikation im Gesundheitswesen erarbeitet werden. Die Sachstandsberichte auf der zweiten Plenumsveranstaltung im Dezember 2000 waren ermutigend. Sie ließen aber auch die Grenzen der Leistungsfähigkeit überwiegend ehrenamtlich tätiger Arbeitsgruppen erkennen.

Eine erfolgreiche Fortsetzung dieser Aktivitäten ist auch im Interesse des Datenschutzes der Patienten zu wünschen, der in klaren und festen Strukturen besser zu gewährleisten ist, als durch das Entstehen von miteinander nicht kompatiblen Einzellösungen.

25.1.2 Der elektronische Arztbrief

Ein – leidiges – Thema der Zusammenarbeit verschiedener Einrichtungen bei der Behandlung eines Patienten ist die Weitergabe relevanter Angaben an den weiter behandelnden Arzt. Zulässig ist die Übermittlung von Patientendaten nach den Berufsordnungen für Ärzte, wenn der Patient damit einverstanden ist und die Angaben für seine weitere Behandlung beim Empfänger erforderlich sind. Das Einverständnis kann angenommen werden, wenn der Patient von der bevorstehenden Übermittlung weiß und nicht widersprochen hat. Obwohl diese sinnvolle Regelung einfach umzusetzen ist und die Informationen im Prinzip spätestens mit dem Patienten eintreffen müssten, kommt der Arztbrief mitunter zu spät oder enthält nicht alle benötigten Angaben in verwertbarer Form. Deshalb liegt es nahe, nach einem Verfahren zu suchen, das den Arztbrief mit automatisierter Unterstützung aus der – automatisiert geführten – ärztlichen Dokumentation leicht, z. B. parallel mit der Überweisung oder mit der Entlassung aus dem Krankenhaus, erstellen lässt, und das beim Empfänger die übermittelten Angaben in die dort ebenfalls automatisiert geführte Dokumentation integriert.

Außer einer gewissen technischen Standardisierung und einer Strukturierung der Kerninformationen müssen hier Schnittstellen zu den Dokumentationen und eine Art der Datenübermittlung festgelegt werden, die sicher gegen unbefugte Kenntnisnahme ist. Weil sich derartige Festlegungen nicht aus den jetzt stellenweise begonnenen Einzellösungen von selbst entwickeln, hat das ATG (s. o. Nr. 25.1.1) dies zu einem seiner Arbeitsschwerpunkte gemacht. Die Datenschutzbeauftragten des Bundes und der Länder beteiligen sich an dieser Entwicklung.

25.1.3 Das elektronische Rezept

Während in den Arztpraxen die Rezepte zunehmend mit Unterstützung durch automatisierte Datenverarbeitung ausgestellt werden und auch die Abrechnung in den Apotheken einschließlich der Bestandsführung weitgehend automatisiert wurde, steht das Rezept selbst noch immer recht konventionell auf Papier. Es wird außer zum Transport der Information vom Arzt zum Apotheker auch als Dokument der ärztlichen Verordnung und damit neben der automatisierten Abrechnung als Beleg dafür benötigt. Weil heute sowohl der Datentransport als auch die Belegfunktion ohne den lästigen Medienbruch „vollelektronisch“ realisiert werden können, liegt es nahe, hier wie schon beim Krankenschein, das Papier durch eine andere Form abzulösen. Wenn der Arzt die Daten seiner Verordnung elektronisch unterschreiben kann (s. dazu Nr. 9.1.2), müssen diese nur noch in der Apotheke vom Patienten präsentiert werden und alle weiteren Verwaltungsarbeiten erfolgen automatisch. Für den Transport der elektronischen Form der Daten zu der Apotheke, die der Patient oder sein Beauftragter aufsucht, werden zwei verschiedene Verfahren diskutiert:

- Das Rezept wird in den Speicher einer Chipkarte geschrieben. Weil es durch die Signatur des Arztes bereits gegen Verfälschungen geschützt ist, könnte dafür eine schlichte Speicherchipkarte ausreichen, z. B. die Krankenversichertenkarte (KVK). Die dazu notwendige Änderung des § 291 SGB V, der den Inhalt der KVK bestimmt, wäre möglich. Vorteilhafter wäre jedoch etwas mehr Sicherheit gegen das unbefugte Auslesen der Daten und dagegen, dass die Daten eines Rezepts kopiert und nach der Präsentation in der Apotheke, in der sie beim Ausgeben des Medikamentes gelöscht werden, erneut auf die Karte geschrieben werden, um das Medikament noch einmal zu erhalten. Diese Sicherheit könnte eine Chipkarte mit Prozessor bieten (s. Nr. 9), die mittelfristig auch als KVK sinnvoll wäre. Auch eine Gesundheitsdatenkarte käme als Rezeptträger in Frage (s. o. Nr. 9.1.1.). Als leseberechtigt für die Rezeptdaten könnte sich der Apotheker mit einer HPC ausweisen.
- Die Rezeptdaten werden auf einen Server geschrieben, von dem sie aus jeder Apotheke abrufbar sind, sobald die KVK oder ein anderes Mittel zum Finden des Rezepts dieses Patienten in der Apotheke vorgelegt wird. Dieses Verfahren stellt hohe Anforderungen an die Verfügbarkeit und an die Sicherheit des Servers und der Telekommunikationsverbindungen. Weil auf dem Server Gesundheitsdaten von Patienten liegen, sollten sie dort rechtlich so geschützt sein wie beim Arzt oder im Gewahrsam einer Krankenanstalt (s. o. Nr. 9.1.1).

Beide Verfahren lassen sich so ausgestalten, dass der behandelnde Arzt erfahren kann, ob und ggf. wann der Patient sein Rezept eingelöst hat. Einerseits kann diese Information für die weitere Behandlung von Interesse sein, andererseits kann ein Patient auch ein berechtigtes Interesse daran haben, dass sein Arzt das nicht erfährt. Darüber muss noch diskutiert und dann sachgerecht entschie-

den werden, jedenfalls sollten Offenlegung oder Geheimhaltung nicht das mehr oder minder zufällige Nebenprodukt einer technischen Realisierung sein. Weil die Umstellung unabhängig von der Wahl des Verfahrens einen erheblichen Rationalisierungsvorteil verspricht, der jedoch die Lösung einiger Organisationsprobleme voraussetzt, hat das Aktionsforum Telematik im Gesundheitswesen (s. o. Nr. 25.1.1) auch dies zu einem Schwerpunkt seiner Arbeit gemacht.

25.2 Genomanalyse

Die Analyse des Genoms hat insbesondere das Ziel, aus dem Erscheinungsbild des Genoms auf Eigenschaften des Trägers dieses Genoms zu schließen. Mit den gewonnenen Erkenntnissen lassen sich dann z. B. Pflanzen und Tiere mit gewünschten Eigenschaften gezielt und schneller züchten, als das mit den klassischen Methoden des Kreuzens und der erfolgsorientierten Auslese möglich ist.

Für die Probleme des Schutzes jener Daten, die aus der Analyse des Genoms eines Menschen gewonnen werden können, sind folgende Tatsachen von besonderer Bedeutung:

- Abgesehen von seltenen Ausnahmen bei (krankhaft) veränderten Zellen – beispielsweise bei krebsartigen Wucherungen – haben alle Körperzellen eines Menschen dasselbe Genom wie die befruchtete Eizelle, aus der dieser Mensch entstanden ist.
- Das Genom leiblicher Kinder ist eine Kombination aus je etwa der Hälfte des Genoms ihrer beiden Eltern. Weil die beiden Hälften in jedem Einzelfall andere Teile des Genoms der Eltern enthalten und weil die Vielzahl der möglichen Konstellationen extrem groß ist, haben nur eineiige Mehrlinge dasselbe Genom.

Daraus folgt u. a., dass man aus der Genomanalyse von z. B. an einer Zigarettenkippe hinterlassenen Zellen (aus dem Speichel) ein Muster erkennen kann, das nur in den Körperzellen des Lieferanten dieser Zellen (Ausnahme s. o.) auftritt. Diese Tatsache kann insbesondere für Zwecke der Strafverfolgung genutzt werden (s. 17. TB Nr. 6.3 und oben Nr. 6.3). Die dazu erforderlichen Vergleiche lassen sich so durchführen, dass dabei keine Erkenntnisse über Eigenschaften der betroffenen Personen anfallen. Das gilt auch für eine weitere Nutzungsmöglichkeit des Mustervergleichs, bei der aus dem Vergleich der Genome verschiedener Personen, Aussagen über deren genetischen Verwandtschaftsgrad abgeleitet werden können.

Bei genomanalytischen Verfahren mit dem Ziel, bestimmte Eigenschaften eines einzelnen Menschen zu erkennen, liegt der Schwerpunkt (noch ?) bei den genetisch bedingten Risiken oder Anfälligkeiten für Krankheiten.

25.2.1 Die „Entschlüsselung“ des menschlichen Genoms

Im Sommer 2000 machten Meldungen über die vollständige Entschlüsselung des menschlichen Genoms Schlagzeilen und fachten die vor rund zehn Jahren bereits einmal intensiv geführte öffentliche Diskussion über den Umgang mit den aus Genomanalysen zu gewinnenden Erkenntnissen wieder an. Tatsächlich enthielten die Meldungen nur die Aussage, dass die Abfolge der vier insgesamt etwas mehr als drei Milliarden mal auf den Chromosomen auftretenden Bausteine des menschlichen Erbgutes – Adenin (A), Cytosin (C), Guanin (G) und Thymin (T) – für ein Referenzgenom (fast) vollständig erkundet und kartiert worden war. Eine Entschlüsselung, also eine die Bedeutung der Reihenfolge der Bausteine offen legende Interpretation war damit nicht verbunden. Gleichwohl ist mit dieser Kartierung ein Meilenstein der Genomforschung erreicht worden, fünf Jahre früher, als es zu Beginn dieses internationalen Projektes erwartet wurde.

Zeitgleich betriebene Forschungen mit anderen Zielen führten zu der Entdeckung bestimmter selten vorkommender Sequenzen, deren Auftreten jeweils ein Indiz für das hohe Risiko der Träger dieses Merkmals ist, dass bei ihnen eine bestimmte Krankheit ausbricht. Es ist zu erwarten, dass die Kartierung eines Referenzgenoms und die dabei erfolgreich angewandten Methoden das Gewinnen von Erkenntnissen über den Zusammenhang zwischen besonderen Konstellationen eines Genoms und Eigenschaften seines Trägers erheblich fördern. Auch damit wird es noch Jahrzehnte dauern, bis das menschliche Genom tatsächlich vollständig entschlüsselt ist. Aber schon heute ist es notwendig, sich mit den Folgen der bereits erreichten und ständig wachsenden Möglichkeiten zum Gewinnen wesentlicher Teilerkenntnisse zu beschäftigen. Dafür lieferten die Schlagzeilen dieses Sommers einen nützlichen Anstoß.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich an der wieder aufgenommenen öffentlichen Diskussion mit einer Entschließung beteiligt, die wichtige Ergebnisse früherer Überlegungen wieder aufgreift (s. **Anlage 26**).

25.2.2 Kritische Zwecke von Genomanalysen

Jedem Menschen ist sein Genom in ganz besonderer Weise zu eigen. Das legt es nahe, die neuen Erkenntnismöglichkeiten in erster Linie zu seinen Gunsten zu nutzen. Denn wer seine genetische Konstellation bzw. die daraus abzuleitenden Chancen und Risiken kennt, der kann sich darauf einstellen und etwa seine Lebensführung so gestalten, dass er das für ihn Beste daraus macht. Dazu gehört dann auch, dass er diese Erkenntnisse für seine medizinische Behandlung und gesundheitliche Beratung nutzen lässt. Nicht jeder will jedoch im voraus Einblick in seine gesundheitliche Zukunft nehmen oder nehmen lassen, und man sollte dazu aus Respekt vor dem Persönlichkeitsrecht keinen Zwang ausüben. Vielmehr sollte die Freiheit, sein eigenes Genom analysieren zu lassen, nicht eingeschränkt werden, und diese Entscheidung sollte man auch nicht durch die Verknüpfung mit positiven oder negativen Konsequenzen lenken oder belasten. Ob und unter welchen besonderen Umständen von diesem Prinzip abgewichen werden darf, muss bald diskutiert und geregelt werden.

Weit kritischer als das Gewinnen von Erkenntnissen aus der Analyse des eigenen Genoms sind die Fälle zu sehen, in denen sich jemand Kenntnisse der genetischen Konstellation eines anderen Menschen verschafft, um sie bei seinen Entscheidungen zu berücksichtigen. Die Diskussion darüber ist längst noch nicht abgeschlossen, und die weitere Meinungsbildung wird wohl auch davon abhängen, was denn tatsächlich alles aus einer Genomanalyse einigermaßen zuverlässig abgeleitet werden kann und was vom Schicksal eines Menschen unkalkulierbares Geheimnis der Zukunft bleiben wird.

Die in diesem Bericht als **Anlage 26** abgedruckte Entschließung greift kritische Nutzungen der Genomanalyse (u. a. zur pränatalen Diagnostik und für Versicherungszwecke) auf und belegt damit die Notwendigkeit, gesetzlich Grenzen zu ziehen – auch mit dem Risiko einer neuen Festlegung auf der Grundlage heute noch nicht verfügbarer Erkenntnisse.

25.2.3 Genomanalyse als Privatgeheimnis

Wir alle hinterlassen an vielen Orten Zellmaterial, das schon heute oder in absehbarer Zukunft für eine Genomanalyse ausreicht: Etwas Speichel an einem Glas oder an einer Zigarettenkippe, ein ausgefallenes Haar mit Wurzel, eine Schuppe der Kopfhaut, etwas abgeschürfte Haut auf rauhem Putz oder etwas Blut auf dem bei einer kleinen Verletzung hilfreich angebotenen Taschentuch. Vermutlich wird es in einigen Jahren nur wenig Mühe und Kosten erfordern, um aus diesen Spuren zu analysieren, ob wir so einigermaßen normal sind oder für bestimmte Krankheiten ein besonders hohes Risiko tragen. Außerdem können aus mehreren solcher Proben die genetischen Verwandtschaftsbeziehungen zwischen den so ausgeforschten Personen erkannt werden, die z. B. bei Adoptionen aus guten Gründen geheim bleiben sollten. Anders als beispielsweise das unbefugte Öffnen eines Briefes sind derart gravierende Eingriffe in das Persönlichkeitsrecht derzeit nicht strafbar, lediglich die Datenschutzgesetze ziehen in ihrem Anwendungsbereich gewisse Grenzen für die Erhebung und Verarbeitung solcher Daten. Diese Vorschriften sind aber nicht anwendbar, wenn etwa ein Vater das Genom des Freundes seiner Tochter analysieren lässt, um bei Bedarf sein Kind vor dem weiteren Umgang warnen zu können, oder wenn jemand einfach aus Neugier untersuchen lässt, ob Geschwister wirklich Geschwister sind. Auch zur Diskriminierung eines Konkurrenten, z. B. bei Wahlen, könnte man so gewonnene Erkenntnisse nutzen oder nutzen lassen. Die Höhe der Kosten für solche Angriffe auf das Persönlichkeitsrecht wird bald keinen wirksamen Schutz mehr bieten. Denn der Einsatz eines speziell für solche Standard-Analysen konstruierten Chips wird vermutlich in einigen Jahren schätzungsweise nur etwa hundert Euro kosten.

Vordringlich scheint mir deshalb ein gegen jedermann gerichtetes, ausdrückliches und strafbewehrtes Verbot, ohne besondere Befugnis

- die Analyse des Genoms eines Anderen durchzuführen oder durchführen zu lassen oder
- Ergebnisse der Analyse des Genoms eines Anderen zu verarbeiten und zu nutzen.

Die Befugnis sollte nur durch eine ausdrückliche gesetzliche Vorschrift oder durch die Einwilligung des Betroffenen erlangt werden können. Dabei müssen jeweils Zweck und Umfang der Analyse bestimmt und die weitere Verwendung der Ergebnisse abschließend festgelegt werden.

Zu diskutieren wäre,

- ob man die Einwilligung nur für bestimmte Zwecke gelten lassen sollte, um das Erzwingen einer wirksamen Einwilligung, beispielsweise für Zwecke des Arbeitsverhältnisses, auszuschließen,
- unter welchen Bedingungen und für welche Zwecke die Einwilligung einer nicht einwilligungsfähigen Person durch eine andere Erklärung ersetzt werden kann und
- welche Regelungen für die Genomanalyse im Interesse des ungeborenen Kindes zu treffen sind.

Diese Schutzmaßnahmen für eines der wichtigsten Geheimnisse eines Menschen sollten getroffen werden, auch wenn das Risiko besteht, dass sie mangels international abgestimmter Regelungen nicht in allen Bereichen vollständig und zuverlässig greifen. Es ist besser, bald die internationale Diskussion damit anzustoßen, als auf ein sich irgendwann einmal einstellendes Ergebnis zu warten.

25.3 Krebsregister

Am 31. Dezember 1999 trat das Gesetz über Krebsregister (Krebsregistergesetz – KRG) vom 4. November 1994 außer Kraft. Damit fand ein langwieriger, aber erfolgreicher Diskussions- und Aufbauprozess seinen Abschluss.

Während die Wahrung des Arztgeheimnisses generell als geboten galt und gilt, war Datenschutz in der epidemiologischen Forschung und besonders bei der Führung von Krebsregistern vor Jahren Gegenstand engagiert und zum Teil polemisch geführter Auseinandersetzungen (s. dazu u. a. 4. TB S. 46 f. und S. 48 f.). Jedoch gab es gerade in den wesentlichen Prinzipien für den Datenschutz bei Krebsregistern schon Anfang der achtziger Jahre auch weitgehende Übereinstimmungen zwischen der Konferenz der für das Gesundheitswesen zuständigen Minister und Senatoren der Länder und der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (s. 6. TB S. 35f.).

Erhebliche neue Impulse erhielt diese Diskussion aus der erfolgreichen Zusammenarbeit – u. a. von Epidemiologen und Datenschützern – bei der „Rettung“ des Krebsregisters der ehemaligen DDR (s. 13. TB S. 32 f.). Bald darauf wurde eine praktikable Lösung für die schwierige Aufgabe erarbeitet, Krebsregister weitgehend anonym zu führen und trotzdem die darin enthaltenen Daten über die einzelnen Fälle um die jeweils neuen Angaben über den weiteren Verlauf zu ergänzen (s. 14. TB S. 103 f.). Hilfreich war dabei die Entwicklung von Krypto-Verfahren, die mit erträglichem, weitgehend automatisiert zu leistendem Aufwand einzusetzen waren.

Das Krebsregistergesetz griff diese Ergebnisse auf und führte im Laufe seiner fünfjährigen Geltungsdauer zu flächendeckenden Krebsregistern in – fast – allen Bundesländern, deren Zusammenarbeit – weitgehend – zufriedenstellend ist. Über ihre Bedeutung für die Krebsbekämpfung hinaus hat diese Entwicklung gezeigt, dass Datenschutz eine epidemiologische Forschung ermöglicht, die der Würde gerade des erkrankten Menschen Rechnung trägt. Eine andere sollten wir uns nicht wünschen.

26 Verteidigung

26.1 Neues Umzugskostenerstattungsverfahren bei der Bundeswehr

Das Bundesministerium der Verteidigung (BMVg) führte vom 1. November 1999 bis zum 31. Oktober 2000 ein IT-gestütztes Pilotprojekt zur Einsparung von Umzugskostenvergütungen durch. Hierfür war ein privates Dienstleistungsunternehmen vertraglich verpflichtet worden, auf Anforderung der zuständigen Bundeswehrdienststellen (i. d. R. Wehrbereichsverwaltungen – WBV) zusätzlich zu den Kostenvoranschlägen, die der Umziehende selbst beibringen muss, weitere Preisangebote von Speditionen einzuholen und zur Verfügung zu stellen.

Von einer WBV, die sich bei der Prüfung der Angemessenheit der zu erstattenden notwendigen Beförderungsauslagen bereits vor Projektbeginn versuchsweise der Unterstützung eines externen Dienstleistungsunternehmens bedient hatte, waren die vom Umziehenden selbst beigebrachten Kostenvoranschläge an das Dienstleistungsunternehmen übermittelt worden, damit dieses hieraus die umzugsrelevanten Daten entnehmen konnte. Eingaben von Betroffenen, die u. a. hiergegen datenschutzrechtliche Bedenken geäußert hatten, waren für mich Anlass für eine Kontrolle bei der betreffenden WBV. Hier konnte ich zunächst feststellen, dass das BMVg den datenschutzrechtlichen Bedenken der Betroffenen gegen die Weitergabe der in ihren Kostenvoranschlägen enthaltenen personenbezogenen Daten in dem Einführungserlass zu dem Pilotprojekt bereits Rechnung getragen hatte. Dieser Erlass legte fest, dass die vom Umziehenden eingereichten Kostenvoranschläge bzw. Angaben hieraus dem Dienstleistungsunternehmen nicht zur Kenntnis gelangen durften.

In der vom Umziehenden stattdessen auszufüllenden Umzugserfassungsliste wurden ausschließlich Daten erhoben, die das Dienstleistungsunternehmen benötigte, um die Menge des Umzugsguts und alle Kostenpositionen zu ermitteln. Auf die noch zu Beginn des Pilotprojekts vom Betroffenen auf der Umzugserfassungsliste abverlangte Unterschrift war bereits zum Zeitpunkt meiner Kontrolle verzichtet worden. Der Umziehende hatte die Richtigkeit und Vollständigkeit seiner Angaben danach ausschließlich auf einem gesonderten Formblatt zu bestätigen, das dem Dienstleistungsunternehmen nicht übermittelt wurde. Die Speditionen wiederum erhielten über eine Kommunikationsdatenbank des Dienstleistungsunternehmens lediglich von den Daten Kenntnis, die sie benötigten, um ein Preisangebot abgeben zu können. Die übermittelten Daten ließen somit weder beim Dienstleistungsunternehmen noch bei den angeschlossenen Speditionen Rückschlüsse auf die hinter dem geplanten Umzug stehende Person zu.

Erfolgte der Umzug tatsächlich mit einem vom Dienstleistungsunternehmen benannten Spediteur, hatte der umgezogene Bundeswehrangehörige hierüber einen Fragebogen zur Qualitätsbeurteilung auszufüllen, der in einen „Kontinuierlichen Verbesserungsprozess“ des Dienstleistungsunternehmens einfloss. Zum Zeitpunkt meines Kontrollbesuchs war diese Qualitätsbeurteilung von den umgezogenen Bundeswehrangehörigen unter Hinweis auf ihre Mitwirkungspflicht mit Name, Dienstgrad bzw. Vergütungsgruppe und Unterschrift auszufüllen. Auf diese Weise ließ sich beim Dienstleistungsunternehmen im nachhinein der Personenbezug herstellen. Dieser Mangel wurde auf meine Empfehlung hin jedoch unverzüglich abgestellt, indem auch der ausgefüllte Beurteilungsbogen anonymisiert unter Angabe der vom Dienstleistungsunternehmen vergebenen Auftragsnummer übermittelt wurde. Gleichzeitig entfiel der Hinweis auf die Mitwirkungspflicht, so dass die Datenerhebung im Rahmen der Qualitätsbewertung nur noch auf freiwilliger Basis erfolgte.

Von Petenten auch mehrfach an mich herangetragene Hinweise, ihre Umzugsdaten seien in das Internet eingestellt worden, haben sich als unbegründet herausgestellt.

Während meiner Kontrolle in der WBV konnte ich mich davon überzeugen, dass aus datenschutzrechtlicher Sicht keine grundsätzlichen Bedenken gegen dieses zunächst in Form eines Pilotprojekts betriebene Vorhaben zur Festsetzung der notwendigen Beförderungsauslagen bestehen. Ich habe das BMVg jedoch darauf hingewiesen, dass ich für die zur Zeit in Vorbereitung befindliche Folgeregelung für eine Dauerlösung zusätzliche datenschutzrechtliche Regelungen, wie z. B. die Erstellung eines IT–Sicherheitskonzepts, für erforderlich halte.

26.2 Kontrolle und Beratung des Personalamtes der Bundeswehr

Das zum 1. Juli 1997 aus dem Personalstammamt hervorgegangene Personalamt der Bundeswehr in Köln ist die zentrale personalbearbeitende Stelle für Zeit- und Berufsoffiziere der Bundeswehr bis einschließlich des Dienstgrades Oberstleutnant/Fregattenkapitän, der Offiziersanwärter und Offiziere im Studium sowie der Reserveoffiziere und Reserveoffiziersanwärter. Daneben betreut das Personalamt federführend das Personalführungs- und Informationssystem der Bundeswehr (PERFIS).

Bei der derzeitigen Nutzung von PERFIS konnte ich anlässlich eines Beratungs- und Kontrollbesuchs zwar keine durchgreifenden datenschutzrechtlichen Mängel feststellen. Gleichwohl wird das System in seiner jetzigen Form den an ein Personalinformationssystem gestellten Anfor-

derungen bei weitem nicht gerecht. Dies wird u. a. an der Vielzahl von zusätzlich individuell erstellten Anwendungen und Dateien („Hilfsdateien“) der Personalführer deutlich, die teilweise zu einer datenschutzrechtlich bedenklichen zusätzlichen – teilweise doppelten und mehrfachen – Datenhaltung führen. Dass sich die Pflege solcher Datenbestände schwierig gestaltet, hat meine Kontrolle bestätigt. So konnte ich Einträge feststellen, die für die Aufgabenerledigung nicht erforderlich oder aber nicht mehr aktuell waren bzw. aufgrund gesetzlicher Vorgaben (z. B. für Disziplinarmaßnahmen) längst hätten gelöscht werden müssen. Ich habe dem Personalamt daher dringend empfohlen, geeignete organisatorische Maßnahmen zu treffen, um diese Mängel abzustellen.

Darüber hinaus habe ich angeregt, die angesprochenen Mängel bei den bereits vor einiger Zeit begonnenen Planungen zur Weiterentwicklung von PERFIS zu berücksichtigen. Wenn es gelingt, den Personalführern mit PERFIS II, dessen Einführung ab 2004 vorgesehen ist, alle für ihre Aufgabenerfüllung erforderlichen Informationen zur Verfügung zu stellen, werden zusätzliche Hilfsdateien entbehrlich. Mit PERFIS II sollen die bisherigen Systeme PERFIS und WEWIS (Wehrersatzwesen-Informationssystem) zusammengeführt werden. Um es bei diesem Projekt beratend unterstützen zu können, habe ich das BMVg gebeten, mich über dessen Fortschritt auf dem Laufenden zu halten.

Bei der Kontrolle der Personalakten in der Registratur des Personalamtes fiel mir erneut auf, dass für die Führung der Personalunterlagen der Soldaten nach wie vor der Erlass des BMVg aus dem Jahre 1965 angewandt wird, dessen Überarbeitung immer noch nicht abgeschlossen ist (vgl. 17. TB Nr. 26.2). Die von mir festgestellten Mängel bei der Aktenführung beruhen in erster Linie darauf, dass die aufgrund des Neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften vom 11. Juni 1992 (hier: § 29 Soldatengesetz) sowie der hierzu ergangenen Verordnung über die Führung der Personalakten der Soldaten und der ehemaligen Soldaten (SPersAV) vom 31. August 1995 geltenden Neuerungen bei der Aktenführung zu einem Großteil nicht berücksichtigt werden. Dies mag teilweise damit erklärt werden, dass das Personalamt im Rahmen der Organisationsänderung erhebliche Aktenbestände von anderen Dienststellen übernommen hat, die eingearbeitet und gleichfalls den neuen Bestimmungen angepasst werden müssen, und dass diese „Altlasten“ trotz des Einsatzes von Aushilfskräften bisher nicht bewältigt werden konnten. Ich habe das BMVg aufgefordert, die Personalaktenführung der Soldaten nunmehr so zügig wie möglich der seit acht Jahren geltenden Gesetzeslage anzupassen.

26.3 Der behördliche Datenschutzbeauftragte – ein endloses Thema

Wegen der Erforderlichkeit eines behördlichen Datenschutzbeauftragten innerhalb der Teilstreitkräfte bestehen keine Meinungsverschiedenheiten mit dem BMVg. Dagegen bildet die Organisation des Datenschutzes, insbesondere die Anbindung des behördlichen Datenschutzbeauftragten innerhalb der Teilstreitkräfte, eine seit langem diskutierte Frage (s. 17. TB Nr. 26.1). Vor allem die Verbindung der Funktion des behördlichen Datenschutzbeauftragten mit dem Führungsgrundgebiet 1 (Personalwesen, Innere Führung, Presse-/Öffentlichkeitsarbeit) habe ich wegen möglicher Interessenkonflikte kritisiert: Denn in seiner Funktion als Personaloffizier trifft er in der Regel zwar keine Personalentscheidungen, ist aber fachlich gehalten, Personaldaten zu erheben und für Entscheidungen zu speichern. Im Zweifelsfall müsste sich der behördliche Datenschutzbeauftragte daher selbst kontrollieren.

Eine Möglichkeit, die unterschiedlichen Auffassungen auszuräumen, eröffnet die Novellierung des BDSG. Gerade auch wegen der Struktur der Bundeswehr wurde in Art. 1 § 4f Abs. 1 Satz 5 des Entwurfs eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes (BT–Drs. 14/4329) die Möglichkeit vorgesehen, interne Datenschutzbeauftragte für mehrere Bereiche zu bestellen. Ich habe daher dem BMVg empfohlen, die Novellierung des BDSG zu nutzen, die Struktur des Datenschutzes in der Bundeswehr – insbesondere innerhalb des militärischen Bereichs – zu überdenken und folgendes vorgeschlagen:

- **Anpassung der Durchführungsbestimmungen an die neue Rechtslage**
  Bei der anstehenden Novellierung der „Durchführungsbestimmungen zum Bundesdatenschutzgesetz (BDSG) im Geschäftsbereich des BMVg“ sollten die Ausführungen zu § 18 Abs. 1 BDSG, wonach „behördliche/interne Datenschutzbeauftragte ... nicht zu bestellen (sind)“ [Erlass vom 30. April 1998 – Org 2 – Az 14–01–01 –, VBMl. S. 153 (162)], der neuen Rechtslage und der Realität in der Bundeswehr angepasst werden. Denn die mit dem Datenschutz beauftragten Offiziere sehen sich bereits heute als interne Datenschutzbeauftragte und üben diese Funktion de facto auch aus.

- **Festlegung einer geeigneten Ebene für das Amt des internen Datenschutzbeauftragten**
  Bei der Novellierung der Durchführungsbestimmungen zum BDSG sollte innerhalb der Truppe eine geeignete Ebene (z. B. Division/Brigade) bestimmt werden, bei der ein interner Datenschutzbeauftragter angebunden werden kann. Bei größeren eigenständigen Verwaltungsstellen der Bundeswehr, wie z. B. dem Personalamt, den Bundeswehrkrankenhäusern oder dem Institut für Wehrmedizinalstatistik und Berichtswesen, sollten eigene, d. h. außerhalb der Truppenhierarchie stehende, interne Datenschutzbeauftragte eingerichtet werden. Ausdrücklich halte ich es nicht für erforderlich, bei jedem Truppenteil einen eigenen internen Datenschutzbeauftragten einzurichten.

- **Neuorganisation der Eingliederung des Datenschutzes und der Anbindung des internen Datenschutzbeauftragten**
  Die organisatorische Anbindung der internen Datenschutzbeauftragten der Bundeswehr sollte neu überdacht und der Bereich Datenschutz in ein anderes Führungsgrundgebiet eingegliedert werden. Dafür

käme etwa das Führungsgrundgebiet 3 – Führung, Organisation, Ausbildung – in Betracht. Für einige Organisationseinheiten halte ich auch die Schaffung eines eigenen Datenschutzbeauftragten außerhalb eines Führungsgrundgebietes für sinnvoll, insbesondere dann, wenn dessen Aufgabe der Umgang mit sensitiven Daten – etwa Personal– oder Gesundheitsdaten – ist. Ich denke dabei z. B. an das Personalamt, die Bundeswehrkrankenhäuser oder das Institut für Wehrmedizinalstatistik und Berichtswesen. Beachtet werden muss in jedem Fall die direkte Unterstellung unter den Dienststellenleiter bzw. Kommandeur (vgl. § 4f Abs. 3 BDSG–E).

Für die neue organisatorische Anbindung des internen Datenschutzbeauftragten innerhalb der Bundeswehr kommt die bereits oben angesprochene Möglichkeit in Betracht, einen internen Datenschutzbeauftragten nach § 4f Abs. 1 Satz 5 BDSG-E für mehrere Bereiche zu bestellen. Dies bedeutet, dass innerhalb der Truppe der interne Datenschutzbeauftragte nicht nur funktionell, etwa als Datenschutzbeauftragter auf Divisionsebene, sondern auch regional für mehrere Bereiche zuständig sein kann (z. B. ein interner Datenschutzbeauftragter für mehrere Bundeswehrkrankenhäuser). Dabei sollte die Möglichkeit bedacht werden, unterhalb der nach § 4f Abs. 1 BDSG-E förmlich bestellten internen Datenschutzbeauftragten Ansprechpartner für den Datenschutz vorzusehen. Auf bewährte Strukturen innerhalb der Bundeswehr kann dabei zurückgegriffen werden. Dies erscheint deshalb von Bedeutung, weil zu befürchten ist, dass der Weg zum förmlich bestellten Datenschutzbeauftragten für den Soldaten zu lang werden könnte. Der Ansprechpartner für den Datenschutz innerhalb der Truppe könnte vor Ort bereits datenschutzrechtlichen Rat erteilen und erforderlichenfalls auf den zuständigen Datenschutzbeauftragten verweisen.

Eine Antwort auf die von mir gemachten Vorschläge stand bei Redaktionsschluss noch aus.

27 Zivildienst – Personalaktenverordnung für Zivildienstleistende –

Bereits in meinem 16. TB (Nr. 27) hatte ich über den Entwurf einer Verordnung über die Führung der Personalakten im Zivildienst (ZDPersAV) berichtet. Allerdings war schon 1997 von den beteiligten Ressorts einvernehmlich festgestellt worden, dass die beim Verordnungsentwurf aufgetretenen grundsätzlichen Probleme nur durch Ergänzungen des Zivildienstgesetzes (ZDG) und des Kriegsdienstverweigerungsgesetzes (KDVG) gelöst werden können. Nachdem das ZDG und das KDVG ursprünglich gemeinsam mit der anstehenden Novellierung des BDSG (s. o. Nr. 2.1) ergänzt werden sollte, wurden die Änderungen nunmehr in Art. 3 (ZDG) und Art. 4 (KDVG) des Gesetzes zur Änderung des Opferentschädigungsgesetzes und anderer Gesetze aufgenommen. In dem Änderungsgesetz wurde u. a. die aus datenschutzrechtlicher Sicht erforderliche Klarstellung getroffen, dass die die Feststellung der Tauglichkeit betreffenden Unterlagen aus der Tauglichkeitsakte zur Personalakte und nicht zu den Unterlagen des § 36 Abs. 1 Satz 3 ZDG (u. a. Unterlagen über ärztliche Untersuchungen und Behandlungen, die nicht Bestandteil der Personalakte sind, und zu denen nur der ärztliche Dienst und das für die Heilfürsorge zuständige Personal Zugang haben dürfen) gehören. Die noch in meinem 16. TB (Nr. 27) geschilderten Bedenken gegen § 3 Abs. 2 Satz 4 des Verordnungsentwurfs, wonach im Falle eines Rechtsstreits, bei dem die Tauglichkeitsakte beigezogen wird, auch das mit der Durchführung des Rechtsstreits beauftragte Personal des Bundesamtes für den Zivildienst (BAZ) diese Akte einsehen darf, wurden dadurch ausgeräumt. Nach der Klarstellung, dass die die Feststellung der Tauglichkeit betreffenden Unterlagen nicht zu den ärztlichen Unterlagen zählen, zu denen nur der ärztliche Dienst Zugang haben darf, kann ich mich dem berechtigten Interesse des Prozessreferates des BAZ an der Einsicht in diese Tauglichkeitsunterlagen bei Verfahren, die eben gerade die Feststellung der Tauglichkeit betreffen, nicht mehr verschließen.

Wegen einiger aus datenschutzrechtlicher Sicht nicht einwandfreier Regelungen des Verordnungsentwurfs befinde ich mich allerdings noch weiterhin mit dem BMFSFJ im Gespräch. So hatte ich im Hinblick auf die angestrebte möglichst weitgehende Übereinstimmung des Personalaktenrechts im Bereich des Zivildienstes mit dem Personalaktenrecht der Beamten und Soldaten gebeten, § 2 Abs. 3 Satz 2 ZDPersAV in Anlehnung an die für Beamte, Soldaten und ungediente Wehrpflichtige geltenden Regelungen dahingehend zu ergänzen, dass in die Nebenakte nur Unterlagen aufgenommen werden dürfen, die sich – im Original oder als Kopie – auch in der Grundakte oder einer Teilakte befinden. Der vom BMFSFJ hiergegen vorgebrachte Einwand, wonach es erforderlich sei, bei den Zivildienststellen zusätzliche Unterlagen in die Nebenakte aufzunehmen, überzeugt nicht, weil die von ihm als Beispiel genannten Unterlagen nicht in die Nebenakte, sondern in eine Teilakte (Urlaubsgewährungen) und teilweise auch gar nicht in die Personalakte, sondern in eine Sachakte (Dienstplaneinteilungen) gehören.

§ 4 Abs. 1 Nr. 3 des Verordnungsentwurfs ordnet Unterlagen, die den Dienstpflichtigen betreffen und mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Berufsförderung, Familienheimfahrten, Reisebeihilfen, Einführungslehrgänge) und somit unter den Personalaktenbegriff des § 36 Abs. 1 Satz 2 ZDG fallen, in Abweichung von den für Beamte und Soldaten geltenden Grundsätzen den Sachakten zu. Da es von der Zuordnung zum Personal- bzw. Sachaktendatenbegriff abhängt, ob die einen stärkeren Schutz gewährenden speziellen Regelungen des Personalaktenrechts Anwendung finden, führt diese Zuordnung ebenfalls dazu, dass die Zivildienstleistenden personalaktenrechtlich schlechter gestellt werden als Beamte und Soldaten.

Das BMFSFJ war bisher nicht bereit, meinen datenschutzrechtlichen Bedenken zu folgen. Die endgültige Fassung der ZDPersAV bleibt abzuwarten.

28 Verkehrswesen

28.1 Umsetzung der neuen straßenverkehrsrechtlichen Regelungen

Nachdem zum 1. Januar 1999 neue straßenverkehrsrechtliche Regelungen in Kraft getreten waren (s. 17. TB Nr. 28.1), habe ich im Berichtszeitraum geprüft, ob diese in der Praxis anwendbar sind und durch die zuständigen Stellen auch im Sinne des Gesetzgebers umgesetzt werden. Dabei zeigte sich, dass einige Probleme in der Anwendung nur durch Rechtsänderungen zu beseitigen sind, andere durch sachgerechte Auslegung der Vorschriften geklärt oder wegen technischer Bedingungen erst zu einem – vertretbaren – späteren Zeitpunkt gelöst werden können.

28.1.1 Straßenverkehrsgesetz

Ich begrüße, dass die Bundesregierung aufgrund der inzwischen gemachten Erfahrungen mit den neuen Regelungen zum Fahrerlaubnisrecht und zum Fahrlehrerrecht einen Gesetzentwurf zur Änderung des Straßenverkehrsgesetzes und anderer straßenverkehrsrechtlicher Vorschriften (StVRÄndG – BT–Drs. 14/4304) auf den parlamentarischen Weg gebracht hat, der u. a. die entstandenen Unsicherheiten hinsichtlich der Übergangsregelungen für die Tilgung und Verwertung von Eintragungen im Verkehrszentralregister nach altem Recht beseitigt (s. § 65 Abs. 4 und 9 StVG). Bei der Beratung des Gesetzentwurfs mit dem Bundesministerium für Verkehr, Bau- und Wohnungswesen (BMVBW) stellte sich im übrigen heraus, dass die ursprünglich vernünftige Festlegung technischer Details im Gesetz selber wegen der rasch fortschreitenden technischen Entwicklung heute nicht mehr sinnvoll ist. Ich halte es daher für angebracht, zukünftig in der verfassungsrechtlich gebotenen Detaillierung die Informationsstrukturen und die Sicherungsanforderungen gesetzlich zu bestimmen, dagegen die auch von den jeweils zu nutzenden technischen Mitteln abhängenden Details aber untergesetzlich zu regeln. Eine solche eher die Ziele als die Mittel bestimmende Gesetzgebung erleichtert die effiziente Nutzung neuer Techniken bei der Verarbeitung von Daten über den Straßenverkehr, ohne den gebotenen Schutz personenbezogener Daten zu vernachlässigen. Die Zweckmäßigkeit eines solchen Vorgehens zeigt sich auch bei dem inzwischen weit fortgeschrittenen Vorhaben des BKA zu INPOL-neu (s. o. Nr. 11.2), das nach Auffassung des BKA wegen der Umstellung auf Internet-Technologie auch bei ZEVIS gewisse Änderungen der Zugriffsverfahren bedingt. Mit den beteiligten Stellen wird zur Zeit besprochen, welche gesetzlichen Änderungen aus Anlass der technischen Änderungen bei INPOL-neu geboten sind. Fraglich ist, ob die geltenden Vorschriften für die Nutzung der Kraftfahrzeug- und Fahrerlaubnisregister – einschließlich der Protokollierungsvorgaben als Garant für die Feststellung der Zulässigkeit der Abrufe – lediglich neu zu formulieren sind oder ob darüber hinaus auch ihre generelle Zielsetzung geändert werden soll.

28.1.1.1 Fahrerlaubnis-Verordnung

Über die aus meiner Sicht problematischen fahrerlaubnisrechtlichen Regelungen habe ich berichtet (s. 17 TB Nr. 28.1.1). Leider wurde die Fahrerlaubnis–Verordnung (FeV) trotz Ankündigung durch das BMVBW bis heute nicht novelliert. Damit ist der Widerspruch zwischen der zu weit gehenden untergesetzlichen Öffnung der Abrufe im automatisierten Verfahren aus dem VZR auf bestimmte Stellen (ohne Zweckbegrenzung – § 61 Abs. 4a FeV) einerseits und der gesetzlichen Beschränkung der VZR-Nutzung (mit Zweckbegrenzung – § 30 Abs. 1 StVG) andererseits noch immer nicht aufgehoben. Wie aus dem BMVBW zu erfahren war, liegt zwar ein Arbeitsentwurf zur Änderung der Verordnung vor; eine Erörterung aus datenschutzrechtlicher Sicht fand mit mir jedoch noch nicht statt. Unabhängig hiervon traten im Berichtszeitraum u. a. Probleme bei folgenden Regelungen der Verordnung auf:

- Umfang und Inhalt ärztlicher und medizinisch-psychologischer Gutachten nach § 11 FeV,
- Umfang und Inhalt von augenärztlichen Gutachten/Zeugnissen und Sehtestbescheinigungen nach § 12 FeV,
- Übersendung von Unterlagen und Akten an Gutachter nach § 12 FeV,
- Übersendung von Verfahrensakten zwischen den Fahrerlaubnisbehörden nach § 58 Abs. 2 FeV,
- Datenaustausch zwischen den Fahrerlaubnisbehörden und Technischen Prüfstellen gemäß § 22 Abs. 4 und 5 FeV.

Bei meinen Bewertungen – auch gegenüber dem BMVBW – vertrete ich die Auffassung, dass nur die Daten erhoben und übermittelt werden dürfen, die für die Aufgabenerfüllung der zuständigen Stellen erforderlich sind. Das Mitschicken nicht erforderlicher Daten mag für den Absender bequem sein; im Interesse des Persönlichkeitsrechtes der Betroffenen muss es aber unterlassen werden. In diesem Zusammenhang habe ich auch darauf hingewiesen, dass die Fahrerlaubnisbehörden bei Zweifeln an der Befähigung und Eignung von Bewerbern auch nur die Informationen und Unterlagen verlangen dürfen, die für die Klärung dieser Zweifel erforderlich sind.

28.1.1.2 Fahrzeugregisterverordnung

Bei einer Kontrolle und Beratung des BKA habe ich u. a. festgestellt, dass trotz des im Straßenverkehrsgesetz und in der Fahrzeugregisterverordnung (FRV) vorgesehenen internationalen Datenaustausches im Zusammenhang mit der Zulassung von Kraftfahrzeugen im Ausland nach wie vor Interpol genutzt wird, um zulassungsrechtliche Hindernisse (z. B. Diebstahl) zu einem bisher in der Bundesrepublik Deutschland zugelassenen Kraftfahrzeug zu ermitteln. Derartige Anfragen beantwortet das BKA nach Klärung der Fragen durch Abruf der Fahrzeug- und Halterdaten aus ZEVIS des KBA. Dieser Umweg ist nicht mehr erforderlich, weil auch die zuständigen ausländi-

schen Stellen Erkenntnisse über zulassungsrechtliche Hindernisse aus ZEVIS online oder über andere Medien beim KBA abfragen können. Denn auch zu diesem Zweck werden die Kfz-Fahndungsdaten des BKA an das KBA geliefert. Sofern vor einer Zulassung im Ausland keine anderen Fragen, z. B. strafrechtlicher Art, abgeklärt werden müssen, halte ich daher eine direkte Anfrage ausländischer Zulassungsbehörden an das KBA für sachgerecht. Ich habe das BMVBW gebeten, die Frage der Abgrenzung von zulassungsrechtlichen und strafrechtlichen Verfahren für die Zulassung von Kraftfahrzeugen im Ausland zu klären.

28.1.1.3 Straßenverkehrs-Zulassung-Ordnung

Bei Mitarbeitern der Technischen Prüfstellen und amtlich anerkannten Überwachungsorganisationen entstand Unruhe, weil die zuständigen Aufsichtsbehörden einiger Länder von diesen Stellen ein Qualitätsmanagement forderten, das auch die Möglichkeit zur Durchführung verdeckter Tests vorsieht. Sie beriefen sich insofern auf den Arbeitsentwurf eines Bund/Länder-Arbeitskreises zur Änderung der StVZO, der in einer Anlage detaillierte Vorgaben für ein Qualitätsmanagementsystem enthält. In einem Gespräch mit den beteiligten Stellen habe ich zu den verdeckten Tests darauf hingewiesen, dass vor deren Einführung eine Auseinandersetzung mit der Frage stattfinden muss, inwieweit mildere Mittel (von der Erfolgskontrolle abgesehen) organisatorischer oder technischer Art zu dem gleichen Ergebnis wie die (obligatorischen) verdeckten Tests führen können. Verdeckte Tests zielen nämlich in erster Linie auf die Tätigkeit des jeweils betroffenen Prüfers und stellen deshalb jeden Prüfer subjektiv ständig unter das Risiko der verdeckten Beobachtung. Diese Belastung ist ein ständiger Eingriff in die Rechte des Prüfenden, seine Arbeit eigenverantwortlich und ohne Überwachungsdruck leisten zu können. Verdeckte Tests sind deshalb mit dem Grundsatz der Verhältnismäßigkeit nur zu vereinbaren, wenn es kein milderes Mittel mit hinreichender Wirkung gibt. Hierzu habe ich dem BMVBW u. a. einen Vorschlag zum verstärkten Einsatz von Erfolgskontrollen in einem geänderten Qualitätsmanagement-System unterbreitet. Es bleibt abzuwarten, ob das Ministerium dieses bei der Vorlage des Verordnungsentwurfs berücksichtigen wird.

28.1.2 Güterkraftverkehrsgesetz

Bei meiner Kontrolle und Beratung des Bundesamtes für Güterkraftverkehr (BAG) habe ich mich vorwiegend über die Speicherung und Übermittlung personenbezogener Daten in und aus dem Unternehmensverwaltungssystem dieses Amtes unterrichtet. Dabei habe ich festgestellt, dass Mitteilungen an Unternehmen über die von ihren Angehörigen begangenen Ordnungswidrigkeiten nur noch bei ausländischen Unternehmen erfolgen und Mitteilungen an deutsche Unternehmen aus nachvollziehbaren Gründen unterbleiben. Ich habe daher um Prüfung gebeten, ob die Änderung des Mitteilungsverfahrens auch eine Änderung der Regelungen des § 16 Abs. 2 und Abs. 3 GüKG (zentrale Speicherung sämtlicher abgeschlossener Bußgeldverfahren, Mitteilung an Unternehmen) erforderlich macht, damit der Umfang der Datenspeicherung und -übermittlung eindeutig bestimmt wird.

28.2 Kraftfahrt-Bundesamt

Bei meiner Beratung und Kontrolle des KBA im Mai 1999 habe ich festgestellt, dass das Amt die gesetzlichen Änderungen des Straßenverkehrsgesetzes, insbesondere aber die neue Fahrerlaubnis-Verordnung (FeV) hinsichtlich der Anforderungen an die zentralen Register umgesetzt und im wesentlichen auch die technischen Voraussetzungen für die Funktionalität und Sicherheit der Register geschaffen hat. Insbesondere begrüße ich die Entscheidung des Amtes, hinsichtlich der Datenübertragungen auf Leitungen für alle Register die alten Verfahren schrittweise abzulösen und stattdessen die ISDN-Technik, später auch die zukunftsorientierten Internet-Protokolle TCP/IP einzusetzen und dabei zugleich Kryptoverfahren anzuwenden. Ob dazu auch Rechtsvorschriften anzupassen sind (s. o. Nr. 28.1.1), bedarf noch der Klärung.

28.2.1 Zentrales Fahrerlaubnisregister

Der Aufbau dieses Registers, beginnend ab Januar 1999, war zunächst geprägt durch die anfangs schleppend eingehenden Meldungen der örtlichen Fahrerlaubnisbehörden über die neu erteilten Fahrerlaubnisse und durch eine relativ hohe Fehlerquote. Diese Mängel, die zum Teil auch auf Schwierigkeiten mit der technischen Umstellung bei den örtlichen Fahrerlaubnisbehörden zurückzuführen waren, konnten inzwischen behoben werden. Hierzu mag auch die Weitergabe entsprechender Informationen an die Landesbeauftragten für den Datenschutz und deren Beratung im kommunalen Bereich beigetragen haben.

Darüber hinaus konnten Einzelprobleme im Zusammenhang mit dem Aufbau des Registers geklärt und Vorschläge zur Fortentwicklung des Registerrechts erörtert werden.

28.2.2 Verkehrszentralregister

Die Einführung der Unentgeltlichkeit von Selbstauskünften aus dem Verkehrszentralregister (VZR) führte beim KBA zu einem deutlichen Anstieg der Auskunftsersuchen. Das KBA regte daher an, das bisher vorgeschriebene und für die Bürger sehr lästige Verfahren (Antrag mit Beglaubigung der Unterschrift) durch Vorlage einer unbeglaubigten Kopie des Personalausweises zu ersetzen und dieses durch Änderung der Verordnung als ausreichende Legitimation festzulegen. Eine derartige Vereinfachung der derzeitigen Auskunftsregelung für Selbstauskünfte aus dem VZR, die der für den wesentlich sensibleren Inhalt des Bundeszentralregisters (BZR) nachgebildet ist, halte ich für möglich. Denn das Geheimhaltungsinteresse der Bürger an diesen Daten, vor allem bei niedrigem Punktestand oder keinen Eintragungen, dürfte – im Vergleich zu den BZR-Daten – geringer sein. Die Belastung der Betroffenen mit Formalien sollte daher verringert werden. Ich habe allerdings vorgeschlagen, zur

Sammlung von Erfahrungen mit diesem Verfahren die Aufbewahrungsfrist für diese Anfragen an das VZR zunächst auf zwei Jahre festzulegen und später aufgrund der gewonnenen Erkenntnisse neu festzusetzen. Der Entwurf zu einer entsprechenden Änderung der Verordnung liegt mir noch nicht vor.

Als ein weiteres Problem im Zusammenhang mit den VZR-Auskünften wurde das Auskunftsverfahren an Behörden mittels Telefax erörtert. Neben verschiedenen anderen Sicherungsmaßnahmen zur Reduzierung der Risiken bei Telefaxauskünften schlug ich vor, Positiv-Auskünfte nur mit Zustimmung des Betroffenen zu erteilen. Diesen Vorschlag setzte das BMVBW auch um und nahm eine entsprechende Formulierung in den Entwurf einer Allgemeinen Verwaltungs- vorschrift zur Datenübermittlung aus dem VZR auf. Diese Ergänzung wurde allerdings auf Empfehlung des Bundesrates wieder gestrichen, da nach Auffassung der Länder auch die Polizei in die Lage versetzt werden müsste, in begründeten Einzelfällen (z. B. Erlass eines Haftbefehls) Telefaxauskünfte zu erhalten. Ich habe mich – leider vergeblich – gegen diese Streichung ausgesprochen, da aus § 30 Abs. 1 StVG kein Zweck abgeleitet werden kann, der diese Übermittlungsform an die Polizei zwingend erforderlich macht. Verlässliche Informationen für den angegebenen Zweck können nicht aus dem VZR gewonnen werden, da die Eintragungen im VZR ausschließlich die Vergangenheit betreffen. Hinweise auf aktuelle Anschriften sollten daher besser auf anderen Wegen eingeholt werden. Ich habe das KBA gebeten, solche kritischen Auskunftsersuchen gesondert zu dokumentieren, damit ich zu gegebener Zeit über die Sinnhaftigkeit dieser Regelung berichten kann.

28.2.3 Zentrales Verkehrsinformationssystem

Auch bei ZEVIS zeigten sich im Zusammenhang mit der Anwendung der neuen straßenverkehrsrechtlichen Regelungen lediglich kleinere Probleme technischer Art. So konnte z. B. die Erhöhung der Auswahlprotokollierung auf 10 % noch nicht umgesetzt werden, da unter den gegebenen technischen Möglichkeiten eine Kapazitätsüberlastung entstand. Ich stimmte daher der Auffassung des KBA zu, dass diese nicht vorhersehbaren und kurzfristig nicht zu ändernden technischen Restriktionen hingenommen werden müssen. Die Beschränkung auf das Machbare (Auswahlprotokollierung von ca. 4 %) habe ich nicht beanstandet, jedoch darauf hingewiesen, dass so bald wie möglich auch diese rechtlichen Vorgaben zu erfüllen sind. Mit Realisierung der 1. Stufe des Datenbanksystems beim KBA Mitte 2001 werden dieses und andere kleinere technische Probleme gelöst sein. Auch die Vorbereitungsarbeiten für „Euro–ZEVIS“ waren zum Zeitpunkt meines Besuchs abgeschlossen. Bei der Aufnahme dieses Betriebes werden selbstverständlich dieselben Sicherheitsanforderungen wie im Inland gelten.

28.3 Verkehrstelematik

Angesichts der begrenzten Ressource Straße ist es folgerichtig, dass die zur Verfügung stehenden technischen Mittel eingesetzt werden, diesen Verkehrsraum optimal zu nutzen. Deshalb bieten verschiedene Firmen Telematikdienste an, die sowohl die allgemeine Verkehrslenkung als auch die individuelle Verkehrsführung umfassen. In diesem Zusammenhang ist die Schnittstelle zwischen anonymer Erfassung des Verkehrsgeschehens und der Erhebung personenbezogener Daten von Verkehrsteilnehmern aus datenschutzrechtlicher Sicht von Interesse.

Neben den klassischen Meldungen über das aktuelle Staugeschehen werden zunehmend Primärdaten über den Verkehrsfluss durch private Firmen erhoben (z. B. über Infrarotschranken) und in deren Rechenzentren mit den übrigen Daten gemeinsam ausgewertet. Darüber hinaus befinden sich sogenannte Floating Car Data-Systems im Aufbau. Die mit Einverständnis der Kunden in ihren Fahrzeugen eingebauten Telematikendgeräte liefern über Mobilfunknetze Daten über die mit Hilfe des Satellitensystems GPS selbst bestimmte Position, Geschwindigkeit und Fahrtrichtung des Fahrzeugs. Aus diesen Daten ist sofort erkennbar, ob das im Verkehrsfluss „mitschwimmende“ Fahrzeug freie Fahrt hat oder im Stau steht. Zusammen mit den übrigen vorhandenen Daten ergibt sich hieraus ein relativ gutes Bild über die Verkehrslage, das die Verkehrstelematikdienste den Interessenten für die Routenplanung und den tatsächlich einzuschlagenden Fahrtweg anbieten können. In Floating Car Data-Systems werden (mit Einwilligung der Betroffenen) lediglich fahrzeugbezogene Daten erhoben, aber nicht fahrzeug- oder personenbezogen verarbeitet. Das ist aus datenschutzrechtlicher Sicht unbedenklich.

Diese und weitere technische und datenschutzrechtliche Fragen der Verkehrstelematik wurden in einem Workshop des Bundesministeriums für Verkehr, Bau- und Wohnungswesen diskutiert. Ein wesentliches Ergebnis dieser Diskussion, an der neben mir u. a. auch Vertreter der Gerätehersteller und der Diensteanbieter teilnahmen, war, dass grundsätzlich anonyme Verfahren ausreichen, um Verkehrslenkungs- und Verkehrsmanagementsysteme betreiben zu können. Hierzu benötige man zwar eine geeignete Technik, um einen ausreichenden Abstraktionsgrad zu erreichen, dieses sei aber zu erträglichen Bedingungen (Einbau von Geräten mit entsprechender Software zu vertretbaren Kosten) bereits heute zu realisieren. Dadurch kann den zu erwartenden Bedenken gegen unerwünschte Überwachung begegnet und durch Offenlegung der Erfassungs- und Verarbeitungsmöglichkeiten eine breite Akzeptanz erreicht werden. Soweit eine zweckfremde Nutzung der gewonnenen Daten durch Weitergabe an Dritte (z. B. an Unternehmen der Verkehrsverbünde, an Betroffene zur Durchsetzung schutzwürdiger Interessen, an die Polizei zur Aufgabenerfüllung – Unfalldaten zur Strafverfolgung –) erlaubt werde, bestünden hiergegen keine Bedenken, soweit die Daten für die Aufgabenerfüllung dieser Stellen erforderlich seien und allgemeine oder spezielle Datenschutzregelungen dieses zuließen. Alle zu erwartenden personenbezogenen Nutzungen sollten jedoch offengelegt und entweder auf freiwilliger Basis erfolgen oder, soweit eine Einwilligung der Betroffenen nicht angestrebt werde oder nicht möglich sei, gesetzlich festgelegt werden.

Einen breiten Raum der Diskussion nahm die Videoerfassung des Verkehrsgeschehens und deren Einstellung in das Internet ein. Es bestand Einvernehmen, dass dieses bereits nach geltendem Recht zulässig sei, sofern damit keine Offenlegung personenbezogener Daten (Erkennen von Personen, Lesbarkeit von Kfz-Kennzeichen) verbunden sei. Verkehrslenkung mittels Videotechnik wurde und wird z. B. im Raum Hannover praktiziert, um den Verkehrsfluss (u. a. bei der Expo) zu beobachten und bei Bedarf schnell Maßnahmen zu ergreifen, ihn umzulenken oder zu entzerren. Das Erkennen von Nummernschildern oder Personen ist auch dazu nicht erforderlich.

28.4 Autobahnbenutzungsgebühren für schwere LKW

Vor einigen Jahren hat die Bundesregierung beschlossen, für die Benutzung von Autobahnen eine streckenbezogene Gebühr für schwere Nutzfahrzeuge einzuführen. Sie soll – voraussichtlich ab 2003 – die derzeitige zeitbezogene Autobahngebühr (Euro-Vignette) ablösen.

Aus überzeugenden Gründen will man statt Mautschranken oder ähnlichen Verkehrshindernissen ein fahrleistungsabhängiges elektronisches Gebührensystem einrichten, das auch eine Erhebung und Verarbeitung personenbezogener Daten erforderlich machen kann. Deshalb wurde ich vom Bundesministerium für Verkehr, Bau- und Wohnungswesen bereits im Rahmen der Systemausschreibung um eine Bewertung der datenschutzrechtlichen Vorgaben gebeten. Die datenschutzrechtlichen Anforderungen an die Kontrollverfahren für schwere Nutzfahrzeuge sind zwar nicht so kritisch wie bei der Pkw-Maut (vgl. 16. TB Nr. 28.1), gleichwohl konnte ich Anregungen zur Formulierung datenschutzrechtlicher Bedingungen geben. Dabei habe ich auch darauf hingewiesen, dass das BDSG nach seiner Novellierung voraussichtlich eine Regelung enthalten wird, nach der die Gestaltung und Auswahl von Datenverarbeitungssystemen sich an dem Ziel auszurichten haben, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Ich gehe davon aus, dass die Systemauswahl und die gesetzliche Regelung für die ggf. unvermeidliche Erhebung personenbezogener Daten diesem Grundsatz Rechnung tragen werden.

28.5 Luftverkehr

Bei Rechtsetzungsvorhaben im Bereich des Luftverkehrs werde ich immer wieder mit Verpflichtungen zur Umsetzung von internationalen Übereinkommen in deutsches Recht konfrontiert. Auch wenn der Luftsicherheit zu Recht eine hohe Priorität einzuräumen ist und international abgestimmte Regelungen dazu besonders wirksam sind, müssen auch diese Vorhaben kritisch bewertet und die Notwendigkeit hierzu begründet werden, wenn in diesem Zusammenhang ein Austausch personenbezogener Daten stattfindet.

28.5.1 Datenaustausch für Zwecke der Luftsicherheit

Über die Errichtung eines Kommunikations- und Informationssystems Luftsicherheit (KISLS) habe ich berichtet (vgl. 17. TB Nr. 28.3.2). Das vom Luftfahrt–Bundesamt (LBA) eingerichtete und in seiner Verantwortung liegende System ist nach Mitteilung des BMVBW inzwischen voll funktionsfähig. Angeschlossen sind neben der Gruppe Luftverkehrs-Sicherheit (LVS) des LBA und den Luftaufsichtsstellen der Länder auch das BMVBW (u. a. für Zwecke der Flughafenkoordinierung), die DFS Deutsche Flugsicherung GmbH und deutsche Verkehrsflughäfen. Für die KISLS-Anwender sind jeweils geschlossene Benutzergruppen eingerichtet worden, die auf das System über ein speziell für ihre Anwendungen zugeschnittenes Menü lesende oder schreibende Zugriffe auf die im System enthaltenen Informationen (über Flugbewegungen, Einflugverbote und durchgeführte Kontrollen technischer oder personeller Art) haben. Lediglich die LVS und das BMVBW haben größere Zugriffsrechte, um bundesweite Auswertungen erstellen zu können. Zugriffe von außen auf dieses Netz sind nach Auskunft des BMVBW nicht möglich. Damit wurde meine Forderung erfüllt, den angeschlossenen Stellen lediglich die Zugriffsrechte auf die Daten zu gewähren, die sie für ihre Aufgabenerfüllung benötigen. Da ich entgegen der Auffassung des BMVBW der Ansicht bin, dass in KISLS auch personenbezogene Daten gespeichert und genutzt werden, habe ich dem BMVBW empfohlen, die Anwender insbesondere auf § 5 BDSG (Verpflichtung auf das Datengeheimnis) hinzuweisen. Das BDSG bietet für die Speicherung und Verarbeitung personenbezogener Daten innerhalb dieses Systems eine ausreichende Rechtsgrundlage, wenn die Zweckbindung dieser für die Luftaufsicht erhobenen und für die Luftsicherheit verarbeiteten personenbezogenen Daten eingehalten wird.

28.5.2 Speicherung von Einzelbefunden der Fliegerärztlichen Untersuchungsstellen

Überrascht wurde ich durch eine vorsorgliche Beschwerde gegen die Absicht des LBA, sich sämtliche von den – privaten – Fliegerärztlichen Untersuchungsstellen festgestellten Einzelbefunde von Luftfahrzeugführern übermitteln zu lassen und in eine noch zu errichtende sogenannte Fliegerdatenbank einzustellen. Meine Rückfrage bei dem zuständigen BMVBW ergab, dass durch eine Änderung der Luftverkehrs-Zulassungs-Ordnung (LuftVZO) die Errichtung dieser Datenbank und das hierfür erforderliche Meldeverfahren angeordnet werden sollten. Die Notwendigkeit für die Errichtung der Fliegerdatenbank beim LBA wurde seitens des BMVBW und des LBA mit der Verpflichtung aus internationalen Verträgen begründet. Hier wurde insbesondere auf den Anhang 1 (Ziffer 1.2.4.6) des ICAO-Abkommens (International Civil Aviation Organization) verwiesen, der die Speicherung von Einzelbefunden vorsehe. Die europäische JAR FCL-Richtlinie (Joint Aviation Requirement

Flight Crew Licensing Medical) verpflichte deshalb folgerichtig die Mitgliedstaaten, dieses in nationales Recht umzusetzen. Meine Prüfung ergab, dass der o. a. Anhang des ICAO-Abkommens lediglich die Speicherung der „angeforderten" Einzelbefunde vorsieht. Eine Verpflichtung zur Speicherung sämtlicher personenbezogener Einzelbefunde (zentrale medizinische Dokumentation) konnte ich darin nicht erkennen. Um sowohl der Rechtslage als auch den berechtigten Interessen der Beteiligten Rechnung zu tragen, habe ich mit Vertretern des BMVBW, des Fliegerärztlichen Ausschusses beim LBA, der Fliegerärztlichen Untersuchungsstellen und der Fachverbände folgende Grundlagen für das weitere Vorgehen erarbeitet:

1. Einzelbefunde dürfen im Rahmen der Zweckbestimmung des § 65 Abs. 2 des Luftverkehrsgesetzes (LuftVG) nur dann gespeichert werden, wenn sie für Erlaubnisse und Berechtigungen (Anordnung von Auflagen und Beschränkungen) relevant sind und als Grundlage für Verwaltungsentscheidungen dienen.
2. Eine vollständige Dokumentation sämtlicher Einzelbefunde im Rahmen der Erstellung fliegerärztlicher Tauglichkeitszeugnisse ist weder für die Erteilung von Erlaubnissen und Berechtigungen erforderlich, noch darf sie zu anderen als den im Gesetz genannten Zwecken genutzt werden (z. B. zur Kontrolle der Fliegerärzte).
3. Für die Arbeit der Fliegerärztlichen Untersuchungsstellen zur Beurteilung von Krankheitsverläufen an Hand einer Beispielsammlung genügt die Speicherung anonymisierter Einzelbefunde.
4. Sofern auf Wunsch des Betroffenen der Fliegerärztliche Ausschuss eine Entscheidung über die Aufrechterhaltung einer Lizenz (evtl. unter bestimmten Auflagen) aus gesundheitlicher Sicht treffen soll, kann dafür mit Zustimmung des Betroffenen die Akte von der jeweiligen Fliegerärztlichen Untersuchungsstelle angefordert werden. Für diesen Zweck ist eine zentrale Speicherung sämtlicher Einzelbefunde aller Fliegerärztlichen Untersuchungsstellen nicht erforderlich.
5. Die sogenannte Fliegerdatenbank wird nicht beim LBA errichtet. Ob – wie vermutet – eine anonymisierte Speicherung von Einzelbefunden bei einem privaten Träger (Fliegerärztliches Zentrum oder Deutscher Fliegerarztverband) ohne Änderung der Rechtslage möglich ist, wird derzeit im BMVBW untersucht.
6. Internationales Recht steht dieser datenschutzgerechten und nach deutschem Recht gebotenen Vorgehensweise nicht entgegen.

28.5.3 Rechtsetzung aufgrund internationaler Verpflichtungen

Wie vorstehend ausgeführt (s. o. Nr. 28.5.2), wird bei Rechtsetzungsvorhaben auf dem Gebiet der Luftfahrt oft auf Verpflichtungen aus dem Abkommen vom 7. Dezember 1944 über die Internationale Zivilluftfahrt (ICAO–Abkommen) verwiesen. Die konkreten Vorgaben für nationale Regelungen und Maßnahmen ergeben sich jedoch nicht aus diesem Abkommen in der Fassung des Ratifizierungsgesetzes vom 7. April 1956 selbst, sondern aus den von Luftfahrtexperten der einzelnen Staaten im Auftrag ihrer Regierungen erarbeiteten Anhängen hierzu, die drei Monate nach Vorlage bei den Vertragsstaaten oder nach Ablauf eines vom Rat festgelegten längeren Zeitraumes wirksam werden. Wie stark die nationale Rechtsetzung durch derartig erarbeitete internationale Vorgaben gebunden sein kann, zeigt die Begründung des damaligen BMV zum Erlass der Dritten Verordnung zur Änderung der Verordnung über Luftfahrtpersonal, in der es heißt: *„Im Rahmen der Arbeitsgemeinschaft europäischer Luftfahrtbehörden (Joint Aviation Authorities, JAA), zu deren Beitritt die Bundesrepublik Deutschland nach Artikel 5 der Verordnung (EWG) Nr. 3922/91 des Rates vom 16. Dezember 1991 zur Harmonisierung der technischen Vorschriften und der Verwaltungsverfahren in der Zivilluftfahrt (Abl. EG Nr. L 373 S 4) verpflichtet ist, wurden die Joint Aviation Requirements JAR–66 und JAR 147 erstellt und im Rat der JAA verabschiedet. Auf Grund ihrer Mitgliedschaft in der JAA sind die Mitgliedstaaten verpflichtet, JAR in ihr nationales Recht zu überführen."*

Das belegt, welche große Verantwortung die Vertreter in internationalen Gremien hinsichtlich der Regelungstiefe von Abkommen/Verträgen/Richtlinien unter Beachtung deutscher Rechtsnomen tragen. Dass hierbei aber auch ein großer Verhandlungsspielraum vorhanden ist, zeigen vielfach internationale Abkommen und Europäische Richtlinien, die Formulierungen wie „soweit er (der Staat) es für durchführbar hält", „in Übereinstimmung mit Richtlinien und Verfahren, die aufgrund dieses Abkommens empfohlen werden", „geeignete einheitliche Verfahren", enthalten. Die Vertreter in internationalen Gremien/Organisationen sind somit in der Lage, eine zu enge Bindung des Gesetz- und Verordnungsgebers zu vermeiden und den nationalen Prinzipien Geltung zu verschaffen. Soweit jedoch grundrechtsrelevante Einschränkungen vorgesehen werden, kann ein evtl. entstehender Konflikt zwischen internationaler Bindung und nationalen gesetzlichen Schranken nur durch den Parlamentsvorbehalt aufgelöst werden.

29 Post

29.1 Das Wirtschaftsministerium greift meine Kritik auf!

Seit der Liberalisierung des Postmarktes haben mich viele Anfragen erreicht, die die nähere Ausgestaltung einiger wichtiger Vorschriften des neuen Postgesetzes (PostG) betreffen. Häufig ging es dabei um Probleme, die mit der dringend benötigten Novellierung der Postdienstunternehmen–Datenschutzverordnung (PDSV) längst hätten behoben sein können (s. 17. TB Nr. 29.1).

Ein besonders kritischer Punkt war die Weitergabe von Daten aus Nachsendeanträgen nach § 29 Abs. 2 PostG an Wettbewerber. Dazu hatte der Bundesrat in seiner Stellungnahme zum Gesetzentwurf der Bundesregierung – Entwurf eines Postgesetzes (BT-Drs. 13/7774) – gebeten, *„im weiteren Gesetzgebungsverfahren in den § 28 Abs. 2 (jetzt § 29 Abs. 2), in den § 41 oder in die nach § 41 Abs. 1 zu erlassende Datenschutzverordnung eine Bestimmung aufzunehmen, nach der Informationen über Adressänderungen an andere Anbieter von Postdienstleistungen nur mit Einwilligung der betroffenen Postkunden weitergegeben werden dürfen"*. Die Bundesregierung hat in ihrer Gegenäußerung zugesichert, dass dieses Anliegen *„im Rahmen der nach § 41 Abs. 1 zu erlassenden Datenschutzverordnung Berücksichtigung finden"* wird. Das ist auch drei Jahre nach Inkrafttreten des neuen Postgesetzes noch nicht erfolgt, obwohl die Regelung in § 29 Abs. 2 PostG dringend der Präzisierung bedarf. Deshalb sind bei der Regulierungsbehörde für Post und Telekommunikation mittlerweile von mehreren Wettbewerbern Anträge auf Schlichtung gestellt worden, nachdem es zwischen dem marktbeherrschenden Unternehmen und diesen Mitbewerbern nicht zu vertraglichen Vereinbarungen gekommen war. Neben unterschiedlichen Preisvorstellungen sind insbesondere die datenschutzrechtlichen Voraussetzungen einer Weitergabe der Nachsendeadressen umstritten. Der Regulierungsbehörde liegen dazu als Entscheidungshilfen nur die Absichtserklärungen aus dem Gesetzgebungsverfahren vor. An der gebotenen Umsetzung durch eine Novellierung der PDSV fehlt es aber, so dass die zeitnahe Umsetzung des im Postgesetz ausgedrückten Willen des Gesetzgebers dadurch verhindert, zumindest aber erschwert wird.

In zähen Verhandlungen zwischen der Regulierungsbehörde, der Deutschen Post AG und mir konnte zwar eine Lösung erarbeitet werden. Dies löst aber nicht die Fälle der nur vorübergehenden Nachsendung und macht eine Regelung in der Verordnung nicht entbehrlich. Darüber hinaus müssen auch zu weiteren Sachverhalten Regelungen in einer neu zu erarbeitenden PDSV getroffen werden.

- Für Pressepost, die aus Kostengründen nicht nachgesandt wird, fehlt eine praktikable Regelung für die Information der Verlage über Adressänderungen ihrer Abonnenten.
- Für im Postlauf eines Unternehmens aufgefundene Sendungen eines anderen Unternehmens ist zu regeln, ob und zu welchen Zwecken das auffindende Unternehmen die Anschriften des Absenders und des Empfängers verwenden darf.
- Es ist zu regeln, wie Postdienstunternehmen mit Postsendungen für Verstorbene verfahren dürfen. Dabei ist fraglich, ob Hinterbliebene einen Nachsendeantrag stellen können und wie sie gegenüber den Postdienstunternehmen die Berechtigung zum Empfang der Postsendungen des Verstorbenen nachweisen müssen.
- Der Einsatz von Arbeitshilfen zur Ermittlung einer zustellfähigen Anschrift (z. B. Telefonbücher oder Telefonbuch-CD-ROM bei Brief- und Frachtpostermittlungsstellen), der sinnvoll und aus Sicht der Unternehmen beinahe unentbehrlich ist, verstößt zum Teil gegen die noch geltenden Regelungen der PDSV.
- Darüber hinaus fehlen datenschutzrechtliche Regelungen für den Einsatz von modernen Technologien in der Zustellung, zum Beispiel zum Einsatz von automatisierten Verfahren zur Steuerung und Überwachung des Sendungslaufs und zum Verbleib der dabei verarbeiteten Daten.

Das Fehlen der notwendigen Regelungen zu diesen und weiteren Sachverhalten führt dazu, dass der Wille des Gesetzgebers – den Wettbewerb unter den Postunternehmen zu eröffnen und mit dem Wettbewerbsdruck die rationelle Leistungserbringung zu fördern – zur Zeit nicht im gewollten Maße umgesetzt werden kann. Nunmehr hat das BMWi auf meine Kritik reagiert und Ende 2000 mit den Arbeiten an einem Verordnungsentwurf begonnen.

29.2 Neue Unternehmen am Postmarkt

Durch die Liberalisierung des Postmarktes zum 1. Januar 1998 sind inzwischen mehr als achthundert neue Unternehmen entstanden, die bundesweit, landesweit oder innerhalb ihrer Stadtgrenzen geschäftsmäßig Postdienstleistungen anbieten. Ich habe in den letzten zwei Jahren den jungen Unternehmen im Rahmen meiner Beratungs- und Kontrollaufgabe Hilfestellungen zu datenschutzrechtlichen Themen gegeben. Dabei stand die Beratung der Postdienstunternehmen im Vordergrund.

Den Unternehmen waren bereits durch die Regulierungsbehörde für Telekommunikation und Post mit den Lizenzunterlagen erste Informationen zur Beachtung des Postgeheimnisses und zum Datenschutz übersandt worden. Aber die postspezifischen datenschutzrechtlichen Regelungen des Postgesetzes und der Postdienstunternehmen-Datenschutzverordnung waren überwiegend nicht bekannt. Dies habe ich zum Anlass genommen, die Unternehmen hierüber zu beraten und zusammen mit der Regulierungsbehörde ein Merkblatt „Postgeheimnis und Datenschutz" zu entwickeln, das den Unternehmen künftig zur Verfügung gestellt wird. Das Merkblatt sowie das Muster einer Verpflichtungserklärung zur Wahrung des Postgeheimnisses und des Datengeheimnisses sind als **Anlagen 31 und 32** abgedruckt.

Denn den Postdienstunternehmen war häufig noch nicht bekannt, dass die Mitarbeiter wegen des täglichen Umgangs mit besonders sensiblen Daten sowohl auf das Datengeheimnis als auch auf das mit Geld- und Freiheitsstrafe bewehrte Postgeheimnis verpflichtet sein sollten. Vereinzelt bestand auch Unsicherheit darüber, wann im Unternehmen ein betrieblicher Datenschutzbeauftragter bestellt werden muss. Dies und auch die Aufgaben, die organisatorische Stellung und die Bekanntmachung des betrieblichen Datenschutzbeauftragten im Unternehmen wurde den Verantwortlichen der Postdienstunternehmen erläutert.

Auf Grund der in den letzten zwei Jahren gewonnenen Erkenntnisse gehe ich insgesamt von einer datenschutzge-

rechten Erbringung von Postdienstleistungen bei den jungen Unternehmen aus. Ich werde die Beratung und Kontrolle neuer Postdienstunternehmen in den kommenden Jahren intensivieren, damit bei der großen Anzahl neuer Unternehmen der Datenschutz im Postbereich im Interesse der Kunden und der Postempfänger allgemein beachtet und das Postgeheimnis gewahrt wird.

29.3 Luftpost ohne Postgeheimnis?

Durch die Eingabe eines Bürgers bin ich auf einen Sachverhalt bei dem Transport von Expresssendungen per Luftpost aufmerksam geworden, der mich in seinen Ausmaßen überrascht hat. Der Bürger hatte mit einem großen Postdienstleister eine Expresssendung an einen Empfänger in England gesandt. In dieser Sendung befanden sich etwa 30 adressierte und verschlossene Standardbriefe. Als diese Sendung den Empfänger mit deutlicher Verspätung erreichte, stellte dieser beim Öffnen des Hauptumschlages fest, dass alle innenliegende Briefe geöffnet waren. Auf dem Hauptumschlag befand sich ein roter Aufkleber mit dem Hinweis „Security checked“ und einer achtstelligen Nummer.

Die Erklärung war einfach: Der große Postdienstleister nahm solche Sendungen an und beauftragte dann ein Partnerunternehmen mit dem Weitertransport der Expresssendung im Luftverkehr. Das Partnerunternehmen nahm sie in Empfang und öffnete alle Sendungen vor dem Lufttransport, um sie auf die Luftsicherheit beeinträchtigende Stoffe oder Güter (z. B. Chemikalien, entzündliche Stoffe) sowie auf nicht zur Beförderung zugelassene Inhalte (z. B. Banknoten, Medikamente) zu prüfen. Dieses Verfahren kompensiert die Tatsache, dass das Partnerunternehmen im Gegensatz zu anderen Lufttransporteuren, die im direkten Kontakt mit den Absendern stehen und deren Kuriere schon beim Abholen das Transportgut auf die Luftsicherheit gefährdende Stoffe überprüfen können, nicht die Möglichkeit dieser Vorabprüfung hat. Diese Erklärung lieferte aber keinen Rechtsgrund für das Öffnen der Briefe, von denen offensichtlich keine Gefahr für den Luftverkehr ausging.

Deshalb kontrollierte ich das Verfahren vor Ort und habe bei diesem Besuch die Sach- und Rechtslage mit den Verantwortlichen diskutiert. Das Öffnen der Sendungen und ihre Prüfung fanden an einem separaten Arbeitsplatz nach dem Vier-Augen-Prinzip statt, wobei der zweite Mitarbeiter parallel mit dem Öffnen und Prüfen anderer Sendungen beschäftigt war. Bei dieser Prüfung lasen die kontrollierenden Mitarbeiter offenbar keine der zu versendenden Schriftstücke. Soweit der Inhalt des Umschlags nicht zu beanstanden war und mit der Inhaltsangabe auf dem Begleitschein übereinstimmte, wurde die Sendung wieder verschlossen.

Das Unternehmen begründete die generelle Öffnung von Sendungen sog. unbekannter Versender mit luftfahrtrechtlichen Erfordernissen und Vorschriften zur Sicherung des Luftverkehrs. Diese erwiesen sich aber bei genauer Prüfung als nicht so weitreichend, als dass sie das Öffnen aller Sendungen einschließlich dünner Briefe rechtfertigen könnten. Eine Anfrage bei anderen Luftposttransporteuren ergab, dass diese solche Sendungen nicht öffnen, sondern z. B. die an den Flughäfen vorhandenen Durchleuchtungsgeräte nutzen, so dass das Postgeheimnis gewahrt bleibt.

Ich vertrete hierzu die Auffassung, dass auch unter den besonderen Bedingungen des Luftverkehrs ein Öffnen von Sendungen durch Postunternehmen nur mit der ausdrücklichen Einwilligung des Absenders oder in den abschließend gesetzlich geregelten Ausnahmefällen des § 39 Abs.4 PostG gestattet ist. Diese Vorschrift erlaubt das Öffnen, z. B. um körperliche Gefahren abzuwenden, die von der Sendung für Personen oder Sachen ausgehen. Da Ausnahmeregelungen stets eng auszulegen sind, ist hiermit nicht das anlasslose Öffnen jeder Sendung erlaubt.

Nachdem ich meine Auffassung dem Unternehmen mitgeteilt hatte, stellte es die bisherige Verfahrensweise umgehend ein. Zukünftig möchte das Unternehmen jedoch – außer für Zwecke der Luftsicherheit – auch vor einer notwendigen Zollgestellung eine Vorabprüfung der jeweiligen Luftpostsendung vornehmen, um seine Haftungsrisiken zu minimieren. Prüfungen zu anderen Zwecken sollen jedoch unterbleiben, und die Prüfungsergebnisse sollen auch nicht zu anderen Zwecken verwendet werden. Die Einzelheiten dieses geplanten Verfahrens bedürfen noch der Konkretisierung. Es besteht Einigkeit darüber, dass die Absender auf die Möglichkeit des Öffnens zu bestimmten Zwecken deutlich hinzuweisen sind.

29.4 Elektronische Quittung für Pakete

Die Deutsche Post AG hatte Anfang 1999 nach Abschluss eines Pilotprojektes gerade bundesweit damit begonnen, Handscanner bei der Zustellung von Paketsendungen einzusetzen, als mich schon kurze Zeit danach die ersten Eingaben von besorgten Bürgerinnen und Bürgern erreichten. Diese beunruhigte bei dem neuen Verfahren vor allem, dass sie auf einer kleinen grauen Fläche – dem Display des Handscanners – blanco unterschreiben sollten, um den Paketempfang ohne Überprüfungsmöglichkeit zu quittieren. Sie wussten nicht und bekamen auch keine Information darüber, dass der Zusteller zuvor bereits die wesentlichen Sendungsdaten eingegeben hatte. Darüber hinaus bestand bei Petenten die Sorge, dass die Unterschrift möglicherweise kopiert und dann missbräuchlich genutzt werden könnte.

Die Deutsche Post AG hat mir das neue Verfahren erläutert und an einem praktischen Beispiel einer Paketbeförderung von der Einlieferung bis zur Zustellung die hierbei stattfindende Datenverarbeitung dargestellt.

Bei der Einlieferung eines Paketes wird in der Einlieferungspostfiliale ein zwölfstelliger Identcode vergeben und auf das Paket aufgeklebt. Er dient der Identifizierung des Postpaketes und befindet sich auch auf dem Einlieferungsschein des Absenders. Dieser kann über den Identcode eine sog. Statusabfrage bei einer auf der Rückseite seines Einlieferungsscheines angegebenen Service–Telefonnummer durchführen. Um darüber Auskunft geben zu

können, welche Stationen das Paket auf dem Beförderungsweg bereits durchlaufen hat, wird erstmals im Einlieferungs-Frachtpostzentrum der Identcode eingescannt, so dass Tag und Uhrzeit später für den Absender abrufbar sind. Zugleich erhält das Paket im Einlieferungs–Frachtpostzentrum einen sog. Leitcode, der die Zieladresse (Postleitzahl, Straßen–Kennzahl, Hausnummer) des Paketes angibt und mit dem das Paket vom Transportsystem im Einlieferungs–Frachtpostzentrum automatisch zur Beladestelle des LKW's gelenkt wird, der die Pakete während der Nacht zum Auslieferungs–Frachtpostzentrum transportiert. Im Auslieferungs–Frachtpostzentrum wird der Identcode der dort angekommenen Pakete erfasst, bevor sie zu den Zustellstützpunkten transportiert werden. Dort übernimmt der für die Zustelladresse zuständige Frachtpostzusteller das Paket.

Der Zusteller stellt das Paket bei der angegebenen Empfängeranschrift, ggf. bei einem Ersatzempfänger (z. B. Hausbewohner, Nachbar), zu. Dieser Vorgang beginnt mit dem Einscannen des auf dem abzuliefernden Paket aufgeklebten Identcodes in den Handscanner. Danach gibt der Zusteller die Empfängerdaten ein, z. B. den Namen des Empfängers oder – bei einer Ersatzzustellung – den Namen des Ersatzempfängers. Automatisch gespeichert werden im System ferner die Auslieferungsdaten; dazu gehören als Information über das Auslieferungsereignis der Name des Zustellers, Datum und Uhrzeit. Zum Nachweis der ordnungsgemäßen Auslieferung läßt sich der Zusteller abschließend den Empfang des Paketes auf einem Handscanner-Pad durch Unterschriftsleistung quittieren.

Die anläßlich der Auslieferung des Paketes auf dem Scanner geleistete Unterschrift wird für evtl. Nachweisungen archiviert, z. B. um dem Absender einen Auslieferungsnachweis über sein Paket zur Verfügung stellen zu können. Dieser Auslieferungsnachweis enthält Empfängernamen und -anschrift bzw. die entsprechenden Daten eines Ersatzempfängers, die vorgenannten Auslieferungsdaten sowie eine grafische Wiedergabe der Unterschrift als „Beweis" der Auslieferung des Paketes.

Die Deutsche Post AG erläuterte, dass ein Zugriff auf die gespeicherte elektronische Unterschrift nur bei Eingabe des Identcodes der Frachtpostsendung besteht. Andere Zugriffsmöglichkeiten seien vom Programm ausgeschlossen. Es sei gewährleistet, dass kein direkter Zugriff von außen auf die Unterschrift sowie auf die sonstigen personenbezogenen Daten oder auf die Sendungsdaten möglich ist. Eine Datenübermittlung an Dritte bzw. Zugriffsmöglichkeiten von Dritten wurde ausgeschlossen. Lediglich der Absender kann die entsprechenden Daten seines Postpaketes nach Angabe des Identcodes abfragen.

Diese Datenverarbeitung ist zulässig. Denn nach § 41 Abs. 2 Postgesetz i. V. m. § 3 Abs. 3 Postdienstunternehmen-Datenschutzverordnung (PDSV) darf ein Postdienstunternehmen Daten, die zum Nachweis einer ordnungsgemäßen Behandlung, Zustellung oder Rückführung der Sendung erforderlich sind (Auslieferungsdaten), für diesen Zweck erheben, verarbeiten und nutzen. Diese Daten dürfen wie bisher schriftlich oder – wie jetzt begonnen – mittels Handscanners elektronisch erhoben werden. Die Deutsche Post AG hat sich bisher den Empfang einer nachweispflichtigen Sendung auf einer Liste durch Unterschriftsleistung quittieren lassen; dies ist nach Angaben der Post auch weiterhin möglich, etwa dann, wenn der Empfänger die Unterschriftsleistung auf dem Scanner ablehnt. Auf keinen Fall darf der Zusteller die Sendung aus diesem Grund wegen Annahmeverweigerung zurücksenden.

Ich habe ferner darauf hingewiesen, dass die Zusteller in die Lage versetzt werden müssen, auf Nachfragen zu dem neuen Scannerverfahren den Empfänger mündlich oder schriftlich zu informieren. Die Deutsche Post AG hat angekündigt, die Zusteller mit einer Informationskarte für nachfragende Empfänger von Frachtpostsendungen auszustatten. Für evtl. weitergehende Fragen sollte ein speziell geschulter Mitarbeiter unter der Kunden-Hotline erreichbar sein. Darüber hinaus soll der Handscanner – im Rahmen einer späteren Neu- oder Ersatzbeschaffung – künftig ein Display mit den wesentlichen Informationen enthalten, die der Empfänger bei der Übergabe der Sendung und vor Unterschriftsleistung ablesen kann. Dies führt zu einer spürbaren Verbesserung der jetzigen Situation. Letztlich halte ich das Verfahren aber auch deshalb für datenschutzrechtlich nicht bedenklich, weil die geleistete Unterschrift in Verbindung mit den sonstigen Auslieferungsdaten nicht mehr als die zur Klärung in Zweifelsfällen erforderlichen Angaben über den Zustellvorgang liefert.

29.5 Wann dürfen Pakete geöffnet oder gar vernichtet werden?

Immer wieder erreichen mich Beschwerden von Bürgern, deren Pakete von Postdienstunternehmen geöffnet wurden. Für die Bürger ist es häufig nur schwer nachvollziehbar, warum das geschehen durfte oder gar musste.

Eine Fallgruppe bilden die Sendungen, die „durch den Zoll müssen". Die Zollverwaltung darf von den Postdienstunternehmen die „Gestellung" einer Sendung verlangen, um den Inhalt nach den Ein- bzw. Ausfuhrbestimmungen zu kontrollieren. Dabei lässt der Zollbeamte die Sendung von einem Mitarbeiter des Postdienstunternehmens öffnen. Das staatliche Interesse an der Einhaltung der Ein- bzw. Ausfuhrbestimmungen wird insoweit dem Postgeheimnis übergeordnet. Nach der Prüfung des Inhalts wird die Sendung wieder verschlossen und mit einem Hinweis auf die zollrechtliche Prüfung versehen. Dieses Verfahren ist praktikabel, und die Erläuterung trifft bei den Bürgern in der Regel auf Verständnis, weil deren Beteiligung an dem Verfahren zu aufwändig wäre.

Auch darüber hinaus gibt es Gründe, aus denen das Postgeheimnis durchbrochen werden darf, z. B. um den Inhalt beschädigter Postsendungen zu sichern oder den auf anderem Weg nicht feststellbaren Empfänger oder Absender einer – wie es im Gesetz heißt – „unanbringlichen" Postsendung zu ermitteln.

Ich habe mich bei der Frachtpostermittlungsstelle der Deutschen Post AG in Bamberg über die Verfahrensab-

läufe bei der Ermittlung von Absendern oder Empfängern unanbringlicher Sendungen informiert. Eine Paketsendung wird dort erst dann geöffnet, wenn anders keine zustellfähige Anschrift ermittelt werden kann. Die Sendungsöffnung führt häufig zum Erfolg, da dem Paket meist ein Schreiben oder Lieferschein mit Absender- oder Empfängerangaben beigefügt ist. In diesem Fall wird die Sendung – mit einem Hinweis auf die Berechtigung zur Sendungsöffnung versehen – wieder verschlossen und an die ermittelte Anschrift gesandt. Führt dagegen die „Beschau des Inhalts“ nicht zum gewünschten Erfolg, wird der Inhalt stichwortartig erfasst, um dadurch bei einer späteren Nachforschung des Absenders über die Inhaltsangabe die richtige Sendung finden und dem Absender senden zu können. Die Sendung wird für diesen Zweck 3 bzw. 6 Monate gelagert. Wenn die Sendung bis zum Ablauf der Lagerzeit nicht im Wege des Nachforschungsauftrages abgerufen wurde, wird sie an eine Verwertungsfirma veräußert, die den Inhalt kommerziell verwertet oder entsorgt.

Vernichtet werden auch Sendungen, deren Beförderung nicht bezahlt wird. In einem mir bekannt gewordenen Fall ist sogar eine Gerichtsakte von einer Verwertungsfirma vernichtet worden, nachdem die unfrei versandte Sendung mit der Gerichtsakte vom Empfänger – einem Landessozialgericht – nicht entgegengenommen wurde. Da auch der Absender, ein vom Gericht beauftragter Gutachter, der Deutschen Post AG das Beförderungsentgelt nicht zahlen wollte und die Entgegennahme der zurück gesandten Sendung verweigerte, wurde sie der Frachtpostermittlungsstelle zugesandt. Hier blieb die Sendung verschlossen, da ja Absender und Empfänger bekannt waren, weshalb sie nicht unanbringlich war und folglich nicht geöffnet werden durfte. Ein Nachforschungsauftrag lag während der anschließenden Lagerfrist nicht vor, so dass die Sendung schließlich an die Verwertungsfirma veräußert und dort datenschutzgerecht entsorgt wurde. Der nach über einem halben Jahr gestellte Nachforschungsauftrag konnte nur noch dieses Ergebnis bestätigen.

Im Rahmen meiner Nachprüfung dieses Ablaufes habe ich festgestellt, dass es kein Einzelfall war. Nach Angaben der Verwertungsfirma habe man schon häufiger Behörden- oder Gerichtsakten gefunden, so u. a. auch Steuerakten von Finanzbehörden. Für die Firma ist eine solche Sendung ein schlechtes Geschäft, da sie die Sendung bezahlt hat, der Inhalt aber nicht nur nicht zu verwerten ist, sondern auch noch auf eigene Kosten datenschutzgerecht entsorgt werden muss.

Sowohl die Deutsche Post AG als auch die mit der Verwertung beauftragte Firma haben völlig korrekt und datenschutzgerecht gehandelt. Es ist aber schon sehr verwunderlich, dass Behörden- und Gerichtsakten monatelang nicht vermisst werden und erst dann nach ihnen geforscht wird, wenn die Akten unwiederbringlich verloren sind. Insbesondere sollten Gerichte und Verwaltungen, denen häufiger Akten zugesandt werden, darüber nachdenken, zu welchen Konsequenzen die Annahmeverweigerung einer unfrei zugesandten Sendung führen kann. Ich habe die Bundesministerien der Justiz, der Finanzen und für Arbeit und Sozialordnung auf dieses Problem hingewiesen.

29.6 Datenschutzauftritt der Post im Internet – Licht und Schatten

Die Deutsche Post AG bietet neben den klassischen Postdienstleistungen, die über Postfilialen und Postagenturen vertrieben werden, verstärkt auch Dienstleistungen im Internet an. So hat sie u. a. ein Geschäftsfeld eröffnet, das dem Nutzer mit dem Internet-Marktplatz eVITA einen virtuellen Einkaufsbummel ermöglicht. Bei eVITA kann der Nutzer des Internetangebotes auf einer umfangreichen und durchaus informativen Seite zum Thema „Datenschutz bei eVITA“ nachlesen, was mit seinen personenbezogenen Daten geschieht. Bei Fragen oder Anregungen kann sich der Nutzer per Email unter „datenschutz@evita.de“ an eVITA wenden. Wenn diese Seite auch noch nicht alle aus datenschutzrechtlicher Sicht erforderlichen bzw. wünschenswerten Informationen enthält, etwa zur Verwendung der mit Hilfe von Cookies gewonnenen Daten oder zur Speicherung der IP-Adresse bei dem beauftragten Provider, so handelt es sich doch um eine gelungene Präsentation einer Datenschutzseite im Internet.

Solche Datenschutzinformationen sind zwar bei eVITA, leider aber nicht auf der Website der Deutsche Post AG selbst zu finden. Dort sucht der Nutzer bisher vergeblich nach einer Datenschutz-Erklärung. Darüber hinaus wäre es verbraucherfreundlich, wenn die Deutsche Post AG in ihr Internetangebot auch Informationen zum Postgeheimnis oder zum Datenschutz bei der Erbringung von Postdienstleistungen aufnehmen würde. So könnte sie beispielsweise die im Jahre 1999 herausgegebene eigene Datenschutzbroschüre entsprechend aufbereitet auch im Internet präsentieren. Darüber hinaus wäre es für die Postkunden, aber auch für die Postmitarbeiter hilfreich, wenn sie im Internet die Namen und Adressen der zehn bundesweit eingesetzten Datenschutzberater finden könnten, die den betrieblichen Datenschutzbeauftragten der Deutschen Post AG seit Ende 1999 unterstützen.

Ich habe die Post auf die Bedeutung einer eigenen Datenschutzseite für ihren Internetauftritt hingewiesen und ihr empfohlen, den Nutzer bereits auf der Startseite mit einem eigenen Button zum Thema „Datenschutz“ zu führen. Hier kann die Deutsche Post AG noch einiges von eVITA lernen!

29.7 Mehr Eingaben zum Datenschutz bei Postdienstunternehmen

Die Liberalisierung des Postmarktes und die damit einhergehenden Veränderungen haben sich auch in der Anzahl und den Themen der mich erreichenden Bürgereingaben niedergeschlagen. So haben mich im Jahr 2000 neben zahlreichen telefonischen Anfragen auch rund einhundert schriftliche Eingaben zu Datenschutzfragen bei Postdienstleistungen der Deutschen Post AG erreicht. Damit hat sich die Zahl der Eingaben im gesamten Berichtszeitraum gegenüber den Jahren 1997 und 1998 um rund

fünfzig Prozent erhöht. Darüber hinaus erreichten mich auch vermehrt Beschwerden und Fragen zu Dienstleistungen anderer Anbieter.

Ein Themenschwerpunkt war das Nachsendeverfahren der Deutschen Post AG. Viele Eingaben wiesen auf Fehler der Zustellkräfte bei der Behandlung der Nachsendeaufträge hin. Der häufigste Fehler war die Weitergabe der Umzugsanschrift an Dritte durch Aushilfskräfte, die den Hinweis *„Keine Anschriftenweitergabe!“* auf einer Merkkarte im Zustellstützpunkt nicht beachteten und den Absendern auf deren Vorausverfügung *„Bitte nicht nachsenden, sondern mit neuer Anschrift zurück“* die Umzugsadresse mitteilten. Ich habe die Deutsche Post AG aufgefordert, diese Mängel durch entsprechende Schulung des Personals abzustellen.

Auch Fehlzustellungen und damit gelegentlich einhergehende Eingriffe in das Briefgeheimnis wurden von Petenten vorgetragen. Auch hier war eine starke Zunahme der Eingaben in Ferienzeiten festzustellen, in denen verstärkt Aushilfskräfte eingesetzt wurden. Dies bestätigten auch die bei der Deutschen Post AG eingeholten Stellungnahmen.

Neben weiteren Eingaben zu den Themen Postphilatelie (s. Nr. 29.9) und Handscannerverfahren (s. Nr. 29.4) erreichten mich auch häufig Beschwerden von Postempfängern, deren Sendungen in der Nachbarschaft abgegeben wurden. Hier verwies die Deutsche Post AG zutreffend auf § 39 Postgesetz, der es den Postdienstunternehmen gestattet, Postsendungen an Ersatzempfänger aufgrund der vertraglichen Vereinbarung mit dem Absender zuzustellen.

Die Eingaben zu datenschutzrechtlichen Problemen bei neuen Postdienstunternehmen ließen noch keine Themenschwerpunkte erkennen. Einigen Eingaben war aber eine noch bestehende Unsicherheit zu entnehmen, ob denn die jungen Postdienstunternehmen auch das Postgeheimnis und den Datenschutz wie die „gute alte“ Post einhielten. Ich konnte den Bürgerinnen und Bürger ihre Sorgen durch den Hinweis nehmen, dass ich über Missstände zumeist schnell durch ihre Eingaben informiert werde, dabei aber nur vereinzelte minderschwere datenschutzrechtliche Verstöße aufgefallen sind. Ein Unterschied in der Wahrung des Postgeheimnisses und des Datenschutzes zwischen der Deutschen Post AG und den neuen Postdienstunternehmen ist für mich jedenfalls nicht feststellbar.

29.8 Die Post wird elektronisch

Der digitale Fortschritt macht auch vor den Postdienstunternehmen nicht Halt. Neben den traditionellen Leistungen wie Brief- und Paketdienst werden immer mehr elektronische „Leistungen“ rund um die traditionellen Dienste angeboten. In meinem 17. TB (Nr. 29.3) habe ich bereits den Dienst ePOST dargestellt, bei dem die Post ihren Kunden anbietet, aus Daten, die online über Internet oder offline auf Datenträgern (Magnetbänder, Disketten, CD's) angeliefert werden, standardisierte Briefsendungen anzufertigen und zu versenden. Jetzt wird auch der umgekehrte Weg angeboten. Bei dem neuen Produkt eDOC erfolgt eine Datenextraktion aus Papier- und Faxdokumenten. Dabei werden die Inhalte der Papierbelege digitalisiert und in den gewünschten digitalen Formatierungen zur Verfügung gestellt. Es spielt kaum eine Rolle, in welcher Form – als Formular, Hand-, Maschinenschrift oder Fax – der Beleg vorliegt und in welchem Format das Ergebnis übermittelt werden soll. Passend zu diesem Angebot kann der Kunde die digitalisierten Belege von der Post AG archivieren lassen. Es geht auch ganz ohne Papier. Bei dem Produkt eDI können – ohne dass die sonst nötige Infrastruktur bei allen Kommunikationspartnern vorhanden sein muss – Daten elektronisch vom Unternehmen in praktisch jeder beliebigen Form eingeliefert werden und erreichen die Empfänger je nachdem per eDI, per Fax oder per Brief.

Die Post AG unterstützt mit diesen Produkten ihre Kunden bei der Bewältigung des immer häufiger auftretenden Medienbruchs zwischen Papier und elektronischem Dokument.

Meine frühere Auffassung zur rechtlichen Einordnung von ePOST als Postdienstleistung (17. TB Nr. 29.3.3) halte ich nach eingehender Prüfung nicht mehr aufrecht.

Meines Erachtens wirkt das Postgeheimnis erst ab dem Zeitpunkt, in dem der Brief körperlich existiert. Das Verarbeiten der Daten zum Herstellen des Briefes (Drucken und Kuvertieren) ist als Datenverarbeitung im Auftrag durch das BDSG nur geschützt, so weit die Daten personenbezogen sind, und dann auch nur in diesem Rahmen. Entsprechend gilt für die Postbearbeitung im eDOC–Dienst, dass mit dem Beginn dieser Dienstleistung die Schutzwirkung des Postgeheimnisses endet.

Unternehmen und Behörden müssen also vor der Nutzung dieser modernen Dienstleistungen prüfen, ob sie die in Postsendungen enthaltenen personenbezogenen Daten dieser Schutzlockerung aussetzen dürfen, woraus sich mitunter Hemmnisse für die Innovation ergeben können. Deshalb sollte von der Bundesregierung geprüft werden, ob die enge materialorientierte Definition des Postgeheimnisses nicht funktionsorientiert ausgedehnt werden kann. Das könnte nicht nur neue Postdienste, sondern auch den Wettbewerb auf diesem Zukunftsmarkt fördern.

29.9 Immer noch Ärger mit der Philatelie!

In meinem 17. TB (Nr. 29.5.2) habe ich über unerwünschte Werbesendungen für postphilatelistische Produkte berichtet. Dabei habe ich erläutert, dass die Bearbeitungszeit von Anträgen auf Löschung der Adressdaten, die der von der Post beauftragte Dienstleister durchführt, noch viel zu lange ist. Denn viele Bürger hatten noch Monate nach ihrer Antragstellung wiederholt Werbeschreiben der Post erhalten.

Zahlreiche Eingaben verärgerter Bürger und Philateliekunden zeigten mir schon kurze Zeit nach meiner Kontrolle, dass die Probleme weiterhin bestanden und die

Deutsche Post AG noch keine ausreichende Abhilfe geschaffen hatte. Die Postphilatelie hatte zwar die Löschung zeitnah in ihrem Kundenbestand durchgeführt bzw. die Daten der Kunden, die nur keine Werbung mehr wünschten, aber Kunde bleiben wollten, entsprechend gekennzeichnet. Darüber hinaus wurden die Daten als Werbeverweigerdaten in die „Postphilatelie-Robinsonliste“ aufgenommen. Dieses und die Löschung der Daten aus den Adressbeständen des mit der Aussendung der Werbesendungen beauftragten Dienstleisters erfolgten aber mitunter erst zwölf Wochen später, so dass in der Zwischenzeit weiterhin Werbesendungen an diese Bürger gesandt wurden. Der Ärger dieser Bürger ist verständlich, wurde doch ihrem Wunsch auf Nichtbelästigung durch Werbung und Löschung ihrer Daten nicht zeitnah Rechnung getragen. Bearbeitungszeiten von bis zu zwölf Wochen können im Computer- und Internetzeitalter von mir weder toleriert noch den betroffenen Bürgern vermittelt werden. Ich habe die Post eindringlich darauf hingewiesen, dass ich eine so lange Bearbeitungsdauer künftig beanstanden werde.

Mein erneutes Tätigwerden hat inzwischen dazu geführt, dass die Post offensichtlich erfolgreich auf eine Beschleunigung hingewirkt hat. Die Eingaben zu diesem Thema sind in den letzten Monaten vor Redaktionsschluss dieses Berichtes jedenfalls spürbar weniger geworden.

30 Statistik

30.1 Volkszählung

In meinem 17. TB (Nr. 30.1) hatte ich über die Modellvorstellungen für die 2001 geplante, gemeinschaftsweite Volkszählung berichtet. Der Deutsche Bundestag hatte für den skizzierten Methodenwechsel votiert und in seinem Beschluss vom 23. Juni 1998 begrüßt, dass bei der nächsten Volkszählung von einer Totalerhebung abgesehen und eine stichtagsbezogene Auswertung der Melderegister vorgenommen werden soll (BT-Drs. 13/11168).

Der vom BMI 1998 vorgelegte Gesetzentwurf zur Vorbereitung des Zensus 2001 begegnete jedoch erheblichen Bedenken von Ländern und Gemeinden. Es wurde eingewandt, das Konzept trage ihren Informationsbedürfnissen nicht ausreichend Rechnung. Zudem müsse die Qualität der Melderegister hinsichtlich ihrer Eignung als Basis der amtlichen Einwohnerzahlen eingehender untersucht werden. Die daraufhin im BMI mit Vertretern der Länder und Kommunen, des Statistischen Bundesamtes und mir geführten Gespräche mündeten in die Empfehlung, zunächst Testuntersuchungen für beide Modellvarianten sowie Qualitätsuntersuchungen für die relevanten Register vorzusehen. Im Frühjahr 1999 wurde eine Arbeitsgruppe von Statistikexperten aus Bund und Ländern eingerichtet, die geeignete Verfahren entwickelt und fachstatistische Vorschläge gemacht hat, auf deren Grundlage das BMI im Sommer 2000 einen Gesetzentwurf zur Vorbereitung eines registergestützten Zensus (Zensusvorbereitungsgesetz – ZensVorG) vorgelegt hat. Der Entwurf sieht vor:

- Eine etwa 1 % große Stichprobe bei allen Meldebehörden, um zu prüfen, wie viele Bürger mehrfach gemeldet sind (s. Abb. 5).
- Testerhebungen bei Meldebehörden und Personen in ausgewählten Gemeinden (ca. 560) und Gebäuden (maximal 38 000) zur Untersuchung von Über- und Untererfassungen (Karteileichen, Fehlbestände) in Melderegistern.
- Testerhebungen (als Unterstichprobe) bei Meldebehörden, Gebäudeeigentümern und Haushalten in ausgewählten Gemeinden (ca. 230) und Gebäuden (maximal 16 000) sowie bei der Bundesanstalt für Arbeit, um Verfahren – wie z. B. die „Zusammenführung“ von Personen zu Haushalten – zu testen (s. Abb. 6).

Mit den Tests wird teilweise statistisch-wissenschaftliches Neuland betreten, für das es auch im Ausland keine Erfahrungen gibt. Skandinavien kennt zwar seit langem den registergestützten Zensus, aber dort gibt es auch das – jedem Bürger zugeordnete – Personenkennzeichen (PK) als Verknüpfungsmerkmal. In Deutschland gibt es aus guten Gründen kein allgemeines PK, so dass die Zusammenfassung von Daten aus unterschiedlichen Dateien auf andere Weise erreicht werden muss.

Eine andere Schwierigkeit der registergestützten Volkszählung zeigt sich bei der statistischen Bildung von Haushalten. Bei der herkömmlichen Volkszählung wird die „Zugehörigkeit zu einem Haushalt“ als Datum auf dem Haushaltsmantelbogen direkt erfragt. Da dieses Merkmal in keiner Verwaltungsdatei geführt wird, die Information über die Zahl, Größe und Struktur der Haushalte jedoch eine wichtige Grundlage für die Beschreibung und Analyse der sozialen und wirtschaftlichen Verhältnisse unserer Gesellschaft darstellt und in Verbindung mit Wohnungsdaten auch Aufschluss über die Wohnsituation der Bevölkerung gibt, muss der haushaltsmäßige Zusammenhang statistisch „errechnet“ werden. Dies geschieht, indem Zusammenhänge zwischen den Daten der Einwohner aus den Melderegistern sowie Angaben aus der Gebäude- und Wohnungserhebung gesucht werden, die darauf schließen lassen, dass Personen einen gemeinsamen Haushalt bilden (Haushaltegenerierung).

Die Erprobung von Verfahren und die Qualitätsuntersuchungen der relevanten Register erfordern auch die Erhebung von Angaben, die überwiegend Hilfsfunktionen haben, um die Richtigkeit, Übertragbarkeit und Zusammenführung von Daten und Dateien auszutesten. Das eigentliche Fragenprogramm ist gegenüber der Volkszählung von 1987 wesentlich reduziert worden; seinerzeit gab es rund 40 Fragenkomplexe (d. h. Fragen mit Unterfragen), davon sind über ein Drittel entfallen; die Zahl der Hilfsmerkmale, die für die Verknüpfung von Daten benötigt und aus denen Antworten „errechnet“ werden, ist dagegen stark angestiegen.

Im Rahmen des Gesetzgebungsverfahrens habe ich folgende Empfehlungen gegeben:

Abbildung 5 (zu Nr. 30.1)

Testerhebung zur Vorbereitung des Zensus

GEBURTSTAGSAUSWAHL MELDEREGISTER

Stichprobengrösse: ca. 1,2% der Bevölkerung

Umfasst alle Einwohner

- ❏ geboren am 1. Janurar, 15. Mai oder 1. September
- ❏ mit unvollständigen Angaben zum Geburtsdatum

STICHPROBE KARTEILICHEN/FEHLBESTAND

Stichprobengrösse: ca. 560 Gemeinden und 38 000 Gebäude

Zweistufig geschichtetes Auswahlverfahren, jeweils größenproportionale Auswahl.

1. Stufe: Gemeindeauswahl
2. Stufe: Gebäudeauswahl
   - ❏ Für die ausgewählten Gebäude werden die Melderegisterangaben der dort gemeldeten Personen angefordert.
   - ❏ Im Rahmen einer Begehung werden alle in den ausgewählten Gebäuden wohnenden Personen befragt.
   - ❏ Begehungsergebnis und Ergebnis der Melderegisterauswertung werden verglichen.

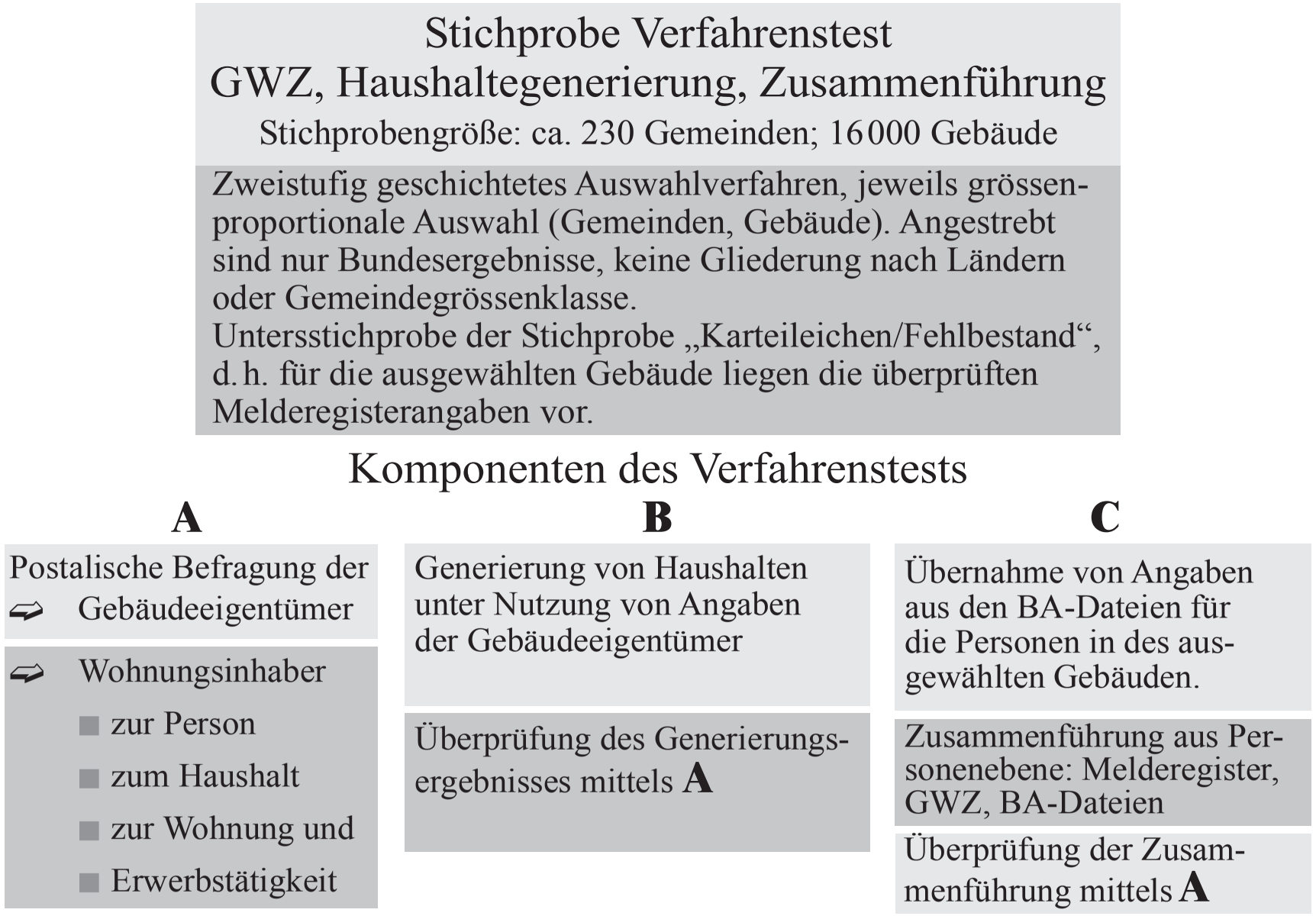
Ziele:

1. Prüfung Datentransfers Gemeinden/GRZ zu StaLÄ
2. Vereinheitlichung Datenformate/Erstellung eines bundeseinheitslichen Datensatzes
3. Tests von Verfahren zu Prüfung eines Datenbestandes auf Vollständigkeit und Mehrfachfälle
4. Klärung von Zweifelsfällen vor Ort (telefonisch, postalisch, persönlich)
5. Zuverlässige Schätzung von Zahl und Struktur der Mehrfachfälle und des Aufwandes zur Klärung von Zweifelsfällen

Ziel:

Zuverlässige Schätzung der Karteileichenrate und Fehlbestandsrate für Deutschland insgesamt, vier Gemeindegrössenklassen (Bundesebene) und für alle 16 Bundesländer.

Abbildung 6 (zu Nr. 30.1)



- Die Probeerhebung ist als Bundesstatistik anzusehen, mit der Folge, dass die strengen Auflagen des Bundesstatistikgesetzes zu beachten sind: Geheimhaltung, Abschottung, Löschungsverpflichtung, Strafbewehrung, technische und organisatorische Sicherungen, Transparenz gegenüber dem Betroffenen.
- Es dürfen keine Daten in den Verwaltungsvollzug zurückfließen. Unstimmigkeiten bei den Meldedaten werden ausschließlich durch die Statistischen Ämter und nur für statistische Zwecke geklärt.
- Durch die Testerhebung erfolgt keine Festlegung der Methodik für einen späteren Zensus. Es handelt sich jetzt nur um eine Sondierung, welche Daten und Verfahren tragfähig und welche es nicht sind. Erst nach Auswertung dieser Probeerhebung wird bestimmt, wie eine künftige Volkszählung durchgeführt werden soll.
- Für jede zu erhebende Angabe – einschließlich aller Hilfsmerkmale – muss es eine gesetzliche Grundlage mit einer plausiblen Erklärung der Notwendigkeit geben.
- Die Löschungsverpflichtungen müssen differenziert ausgestaltet sein, damit Daten, die für Test- und Auswertungszwecke nicht mehr benötigt werden, sobald wie möglich gelöscht werden können.

Weil es sich um eine Testphase mit zahlreichen Unwägbarkeiten und Ungewissheiten handelt, ist es m. E. hinnehmbar, das bei statistischen Erhebungen außerordentlich strenge Erforderlichkeitsgebot diesem Umstand anzupassen. Denn sonst wäre es nicht möglich auszutesten, welche Daten sich für Hochrechnungen und Verknüpfungen als stabil erweisen und auf welche Erhebungsmerkmale bei einer künftigen Volkszählung verzichtet werden muss, weil sie sich nicht als erforderlich erwiesen haben. Ich halte die im Gesetzentwurf getroffenen Regelungen für ausgewogen und mit dem Datenschutz vereinbar.

Kritiker einer Volkszählung durch Registerauswertung verweisen auf die Aussagen der Verfassungsrichter im Volkszählungs-Urteil von 1983, dass *„...die Übernahme sämtlicher Daten aus bereits vorhandenen Dateien der Verwaltung (...) keine zulässige Alternative zu der vorgesehenen Totalerhebung“* sei. Die Verfassungsrichter begründeten das damit, dass die Zusammenführung von Daten aus verschiedenen Registern der *„Einführung eines einheitlichen für alle Register und Dateien geltenden Personenkennzeichens oder dessen Substitut (gleichkomme). Dies wäre aber gerade ein entscheidender Schritt, den einzelnen Bürger in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren.“* (BVerfGE 65,1..S. 56, 57)

Diese von den Verfassungsrichtern aufgezeigten Grenzen der Informationsverarbeitung werden hier jedoch nicht tangiert. Es wird kein – wie auch immer geartetes – Personenkennzeichen geben, das über alle Register und Dateien hinweg eine Verknüpfungsmöglichkeit schafft. Es werden nur die Register der Meldebehörden und 3 Dateien der Bundesanstalt für Arbeit einbezogen; und zwar die Datei für sozialversicherungspflichtig Beschäftigte, die Arbeitslosendatei und die Datei der Teilnehmer an Maßnahmen zur beruflichen Weiterbildung. Auch werden keine Daten zusammengeführt, die den Bürger in seiner ganzen Persönlichkeit registrieren können.

Die von den Verfassungsrichtern aufgestellte Messlatte für Eingriffe in das informationelle Selbstbestimmungsrecht des Bürgers bleibt somit unangetastet.

Die Terminplanungen für das Testverfahren sehen vor, das Gesetz Anfang 2001 einzubringen, die Testerhebungen im Herbst 2001 durchzuführen und die Auswertungen im Jahre 2003 zu präsentieren.

30.2 Die einheitliche Unternehmensnummer

Zu den Vorschlägen, bürokratische Hemmnisse zwischen Unternehmen und Behörden sowie zwischen Behörden untereinander abzubauen, gehört die Entwicklung und Einführung einer einheitlichen Unternehmensnummer. Zur Zeit haben Unternehmen bei Ämtern und Behörden jeweils unterschiedliche Nummern, die im Kommunikationsverkehr jeweils anzugeben sind (z. B. Steuer-Nr., Betriebs-Nr., Sozialversicherungs-Nr., Zoll-Nr., Statistik-Nr.).

Einen weiteren wesentlichen Vorteil einer einheitlichen Unternehmensnummer sehen die Befürworter aus Verwaltung und Wirtschaft in der mit der Nummer verknüpften zentral geführten Stammdatendatei, in der Grunddaten zum Unternehmen wie Name, Firmenbezeichnung, Anschrift, Rechtsform, Handelsregistereintrag gespeichert werden. Diese Datei soll bei der Arbeitsverwaltung geführt werden. Um Unternehmen von Meldepflichten zu entlasten, erhalten bestimmte Behörden regelmäßig Informationen, während andere Behörden im Einzelfall auf Anfrage unterrichtet werden.

Der datenschutzrechtliche Aspekt dieses Vorhabens wird in den Fällen deutlich, in denen das Unternehmen mit einer natürlichen Person weitgehend identisch ist, wie z. B. bei Freiberuflern, Landwirten und anderen Selbständigen, weil hier die bundeseinheitliche und behördenübergreifende Nummer dieser natürlichen Person zugeteilt wird. Hier ist zu beachten, dass der Rechtsausschuss des Deutschen Bundestages am 5. Mai 1976 in seiner Stellungnahme zum Entwurf eines Bundesdatenschutzgesetzes, die Beachtung des folgenden Grundsatzes gefordert hat*: „Die Entwicklung, Einführung und Verwendung von Numerierungssystemen, die eine einheitliche Numerierung der Bevölkerung im Geltungsbereich dieses Gesetzes ermöglichen (Personenkennzeichen), ist unzulässig.“*

Daraufhin wurden seinerzeit die bereits angelaufenen Arbeiten zur Einführung eines Personenkennzeichens eingestellt, und auch in späteren Gesetzen spiegelt sich diese politische Ansicht wieder. Das Bundesverfassungsgericht hat in seinem „Volkszählungsurteil“ von 1983 den Grundgedanken der Unvereinbarkeit eines allgemeinen Personenkennzeichens mit dem informationellen Selbstbestimmungsrecht unmissverständlich wiederholt und auch der Einigungsvertrag von 1990 fordert dazu auf, Dateien der ehemaligen DDR, die nach Personenkennzahlen geordnet sind, unverzüglich nach anderen Merkmalen umzuordnen

und die Personenkennzahlen zum frühestmöglichen Zeitpunkt zu löschen.

In den unter Federführung des Bundesministeriums für Wirtschaft und Technologie geführten Gesprächen über Aufbau, Vergabe und Verwendung der Unternehmensnummer wirke ich darauf hin, dass sie nicht die Funktion eines allgemein verwendbaren Personenkennzeichens bekommen kann. Um dies zu verdeutlichen sollen für die Verwendung der Nummer und der mit ihr verbundenen Stammdaten klare und abschließende gesetzliche Vorgaben getroffen werden. Die bisherigen Ergebnisse der Beratungen entsprechen diesem Anliegen.

Im Jahr 2001 soll zunächst ein Gesetz für eine Testphase im Jahr 2002 erarbeitet und verabschiedet werden. Bei Erfolg soll mit den dabei gemachten Erfahrungen in den folgenden beiden Jahren das eigentliche Gesetzgebungsverfahren durchgeführt werden, damit die Einführung der Unternehmensnummer zum 1. Januar 2005 erfolgen kann.

30.3 Wahlstatistik

30.3.1 Regelungen bei Urnenwahl

Der Deutsche Bundestag hatte für die Bundestagswahlen 1994 und 1998 die Durchführung der Wahlstatistik wegen verfassungsrechtlicher Bedenken ausgesetzt (s. 15. TB Nr. 22.6). Zuvor war die Sonderauszählung eines Teils der Stimmen zur Untersuchung des Wahlverhaltens nach Alter, Geschlecht und Region wegen erheblicher Zweifel an der Gewährleistung des Wahlgeheimnisses in die Kritik geraten, obwohl konkrete Verletzungen des Wahlgeheimnisses nicht bekannt geworden waren. Zweifelhaft schien, ob die Rechtsgrundlage hinreichend präzise sei und das Wahl- und Statistikgeheimnis ausreichend gewährleistet werde. Die Bedenken richteten sich u. a. gegen die Zumutbarkeit der Auflage für einen Teil der Wähler, ihr Wahlrecht nur mit einem nach Alter und Geschlecht gekennzeichneten Stimmzettel ausüben zu können.

Die repräsentative Wahlstatistik sollte aber nicht endgültig abgeschafft, sondern nur zeitlich bis zur rechtlichen Absicherung ausgesetzt werden. Die Novellierung hatte in erster Linie die Sicherung des Wahlgeheimnisses zum Ziel, aber auch die Sicherung der Aussagekraft und die Beschleunigung der repräsentativen Wahlstatistik. Denn Wahlforscher und auch Politiker wünschten sie weiterhin als unverzichtbares Instrument zur Überprüfung der Umfragedaten der Wahlforschung. Bei einer Abschaffung der amtlichen Sonderauszählung würden wichtige Daten über das tatsächliche Wahlverhalten verloren gehen; so könnten z. B. rechtsradikale Tendenzen bestimmter Wählergruppen oder das Wahlverhalten von Jugendlichen nur mit Hilfe dieser Statistik erkannt werden. Da somit an der Fortführung der repräsentativen Wahlstatistik sowohl aus der Sicht der politischen Parteien und der wissenschaftlichen Einrichtungen als auch des Parlaments, der Regierung und Behörden ein erhebliches Allgemeininteresse bestand, musste eine für alle Wähler zumutbare Lösung gefunden werden. An den Beratungen dazu habe ich mich beteiligt.

Am 31. Mai 1999 trat das Gesetz über die allgemeine und repräsentative Wahlstatistik mit folgenden wesentlichen Schutzvorkehrungen, um Rückschlüsse auf das Wahlverhalten einzelner Wähler auszuschließen, in Kraft (BGBl I S. 1023):

- Die Festlegung einer Mindestzahl von 400 Wahlberechtigten für die Stichprobenwahlkreise (§ 3).
- Eine Zusammenfassung der Geburtsjahrgänge (§ 4).
- Die Trennung der für die statistische Auswertung von den für die Stimmauszählung zuständigen Stellen (§ 5).
- Das Verbot der Zusammenführung von Wählerverzeichnis und gekennzeichneten Stimmzetteln bzw. Ergebnisausdrucken der Wahlgeräte (§ 5).
- Eine strenge Zweckbindung für die Statistikstellen hinsichtlich der ihnen zur Auswertung überlassenen Wahlunterlagen (§§ 7,8).
- Die öffentliche Bekanntmachung in den ausgewählten Wahlbezirken über die Durchführung der Repräsentativerhebung (§ 3).

In einem Punkt habe ich mich nicht durchsetzen können, obwohl sich der Innenausschuss des Bundestages meinem Votum angeschlossen hatte. Ich hätte es vorgezogen, wenn die Unterscheidungsmerkmale nach Alter und Geschlecht auf der Rückseite des Stimmzettels aufgedruckt worden wären – als zusätzliche Sicherung der Vertraulichkeit der Stimmabgabe. Dadurch wäre die Zuordnung eines Stimmzettels zu einer bestimmten Person bei der Auszählung noch unwahrscheinlicher geworden als dies durch die im Gesetz vorgesehenen Verfahrensregeln der Fall ist. Das BMI hatte dagegen eingewandt, dass die Druckkosten pro Stimmzettel um bis zu 200 % steigen würden, und die Befürchtung geäußert, durch die rückseitige Kennzeichnung könnten Wähler eher misstrauisch werden; außerdem seien die Stimmzettel anlässlich der Europawahl 1999 z. T. bereits auf der Grundlage der bisherigen Praxis vorbereitet worden.

Ich bin gleichwohl – übereinstimmend mit dem Ausschuss – davon überzeugt, dass es sich hierbei um eine wichtige Vertrauen bildende Maßnahme handelt, die auch ohne ausdrückliche Regelung im Gesetz künftig so durchgesetzt werden kann und auch werden sollte.

30.3.2 Einbeziehung der Briefwähler

Das verabschiedete Wahlstatistikgesetz sieht noch keine Verpflichtung zur Einbeziehung der Briefwähler vor. Diese Entscheidung hatte der Bundesgesetzgeber für eine spätere Klärung zurückgestellt. Briefwähler waren in der Vergangenheit nicht in der Sonderauswertung erfasst. Angesichts wachsender Briefwahlquoten wird darin jedoch eine Verzerrung der Repräsentativ-Stichprobe gesehen. Nach Auskunft des Statistischen Bundesamtes lag die Briefwahlquote 1998 bei 15,5 %, Tendenz steigend. Wahlforscher, Politiker und Parteien sehen in der Einbeziehung der Briefwähler eine notwendige Verfeinerung des Instruments der amtlichen Sonderauszählung und le-

gen dafür Auswertungsergebnisse vor, die signifikante Unterschiede von bis zu 6 % bei Brief- und Urnenwählern ausweisen.

Für die Einbeziehung der Briefwähler wurden verschiedene Modelle entwickelt. Im Wesentlichen konzentrierten sich die Lösungen auf zwei Varianten: Bildung eigener Briefwahlbezirke oder Zuordnung der Stimmzettel von Briefwählern zu den entsprechenden Urnenwahlbezirken. Im vorliegenden Gesetzentwurf des BMI, der sich Ende 2000 in der Länderabstimmung befand, haben sich die Befürworter eigener Briefwahlbezirke durchgesetzt.

Aus meiner Sicht ist diese Lösung unter dem Gesichtspunkt der technisch-organisatorischen Absicherung des Wahlgeheimnisses die vorteilhaftere. Sie gewährleistet die gleiche Vorgehensweise wie bei der von mir befürworteten Regelung für die Urnenwahl. Das Wahlstatistikgesetz soll demnach so novelliert werden, dass die gesetzlichen Bestimmungen gleichermaßen für ausgewählte Briefwahlbezirke gelten. Lediglich bei der sog. Abschneidgrenze, d. h. der Mindestzahl zu erwartender Briefwähler pro Briefwahlbezirk, wird die Anforderung auf 500 Wahlscheininhaber – gegenüber 400 Wahlberechtigten bei Urnenwahl – angehoben. Damit soll dem Unsicherheitsfaktor der Briefwahlquote Rechnung getragen werden.

Ich habe gegen den Novellierungsentwurf keine datenschutzrechtlichen Bedenken.

31 Nicht-öffentlicher Bereich

31.1 SCHUFA

31.1.1 Die neue „SCHUFA-Klausel“: Transparenz im Scoring-Verfahren genügt nicht

Im Berichtszeitraum hat die SCHUFA in Zusammenarbeit mit dem Zentralen Kreditausschuss und Vertretern der Datenschutzaufsichtsbehörden eine neue „SCHUFA-Klausel 2000“ entwickelt (s. **Anlage 30**). Anlass hierfür war in erster Linie eine Weiterentwicklung des Marktes, der das Unternehmen entsprechen wollte. In diesem Zusammenhang wurden auch Anregungen der Datenschutzaufsichtsbehörden berücksichtigt. Folgende Punkte wurden geändert:

- Neben Verbrauchern im Sinne des Verbraucherkreditgesetzes sollte auch die Verarbeitung von Bonitätsdaten über Freiberufler und Einzelkaufleute im SCHUFA-Verfahren ermöglicht werden. Dies setzte eine Änderung des bisherigen Konsumentenbegriffs voraus.
- Die geplante Zusammenarbeit der SCHUFA mit anderen europäischen Kreditinstituten – datenschutzrechtlich ein eher unproblematischer Schritt, da die Europäische Datenschutzrichtlinie für Datenübermittlungen innerhalb der EU-Mitgliedstaaten die gleichen Rahmenbedingungen vorsieht wie auf nationaler Ebene – machte eine entsprechende Anpassung der SCHUFA-Klausel notwendig.
- Aufgrund der Privatisierung des Telekommunikationssektors haben sich die Telekommunikationsunternehmen zu einer neuen Gruppe von Vertragspartnern der SCHUFA entwickelt, so dass diese Gruppe explizit in der SCHUFA-Klausel erwähnt wurde (s. auch oben Nr. 10.11).

Der problematischste Punkt war die Transparenz für die Betroffenen hinsichtlich des **Scoring-Verfahrens** (s. 17. TB Nr. 31.3). Neben einem Hinweis in der Klausel selbst, dass die SCHUFA ihren Vertragspartnern einen Score-Wert mitteilen kann, forderten die Aufsichtsbehörden deutlich mehr an Transparenz zum Scoring-Verfahren selbst. So sollte den Betroffenen beispielsweise ermöglicht werden, die im Score-Wert erfassten Daten auf ihre Richtigkeit hin zu überprüfen, und ihnen anhand von Beispielsfällen die Relevanz bestimmter Daten (z. B. Zahl der Wohnungswechsel, Zahl der Girokonten etc.) deutlich gemacht werden. Diese weitergehenden Informationen sollten in einem SCHUFA-Merkblatt enthalten sein, das jedem Betroffenen, der die SCHUFA-Klausel unterschreibt, ausgehändigt wird.

Ein Ergebnis über den Umfang der Transparenz, die die SCHUFA den Betroffenen zubilligen will, lag bei Redaktionsschluss noch nicht vor. Hauptforderung der Aufsichtsbehörden ist nach wie vor, den Score-Wert in die Auskunft an den Betroffenen aufzunehmen; sei es, dass die SCHUFA als „Urheber“ des Wertes dies übernimmt, oder aber das Vertragsunternehmen der SCHUFA, das mit dem Wert arbeitet. In diesem Punkt konnte bislang weder mit der SCHUFA noch mit dem Zentralen Kreditausschuss, als Vertreter der Kreditwirtschaft, Einigkeit erzielt werden. Beide Seiten berufen sich darauf, dass die Auskunft nach dem BDSG nur gespeicherte Daten enthalten müsse und der Score-Wert weder bei der SCHUFA noch – in der Regel – beim Kreditinstitut gespeichert würde. So bleibt für den Verbraucher der für ihn oft so entscheidende Wert im Dunkeln.

Dieser Zustand ist nicht länger akzeptabel. Sollten sich die SCHUFA oder die Kreditwirtschaft nicht zu dieser Auskunft bereit erklären, sollte der Gesetzgeber eine Verpflichtung zur Auskunft über solche Daten schaffen, die genutzt aber nicht dauerhaft gespeichert werden.

31.1.2 Das Auskunftsrecht darf nicht schaden!

Das Scoring-Verfahren ist nach wie vor Gegenstand der Diskussion zwischen den Datenschutzaufsichtsbehörden und der SCHUFA (vgl. 16.TB Nr. 31.2.3 sowie 17.TB Nr. 31.3). Dabei geht es um mehr Transparenz für den Verbraucher durch eine möglichst weitgehende Offenlegung des Verfahrens (s. o. Nr. 31.1.1).

Erhebliche Kritik sowohl der Öffentlichkeit als auch der Datenschutzaufsichtsbehörden hat die SCHUFA durch ihre Praxis erfahren, das gesetzlich garantierte Recht eines jeden auf Einholung einer Selbstauskunft nach dem BDSG als Negativkriterium im Rahmen einer Bonitätsrisikoprognose zu bewerten. Der Score-Wert verschlechtert sich automatisch für den Betroffenen, wenn er sein Auskunftsrecht ausübt. Diese Praxis ist rechtlich äußerst bedenklich. Jedermann hat nach dem BDSG einen Anspruch auf Auskunft über die zu seiner Person bei der SCHUFA gespeicherten Daten. Wird er aufgrund der Inanspruchnahme dieses Rechts quasi bestraft, indem sich allein das Auskunftsbegehren negativ auf seine Risikoprognose auswirkt, stellt das eine nicht hinnehmbare Einschränkung seines Persönlichkeitsrechts dar. Dieser Auffassung haben sich auch die obersten Datenschutzaufsichtsbehörden der Länder angeschlossen.

In meiner Eigenschaft als Datenschutzaufsichtsbehörde für die Telekommunikationsunternehmen, die Vertragspartner der SCHUFA sind, habe ich nach Bekanntgabe dieser Praxis die SCHUFA aufgefordert, das Problem auszuräumen (s. o. Nr. 10.11).

Die SCHUFA hat sich mittlerweile bereit erklärt, zukünftig auf dieses Verfahren, nämlich Einbeziehung der Anzahl der Selbstauskünfte in den Score-Wert, zu verzichten. Ein sich derzeit in der Entwicklung befindliches neues Verfahren sieht keine Einbeziehung der Selbstauskünfte in die Score-Wert Ermittlung mehr vor. Die Umsetzung und Einführung dieses neuen Scoring-Verfahrens, wird nach Angaben der SCHUFA Mitte 2001 erfolgen. Die Aufsichtsbehörden werden die zeitgerechte Umsetzung beobachten.

31.2 Datenschutz bei Fusionen und Unternehmensspaltungen

Aufgrund der Globalisierung der Wirtschaft und des so entstandenen verstärkten Wettbewerbs kam es in den letzten Jahren zu einem Boom bei Unternehmensfusionen, -übernahmen und der Ausgliederung von Geschäftsbereichen, der wohl nach wie vor anhält.

Neben den für die Unternehmen ausschlaggebenden wirtschaftlichen Auswirkungen haben diese Umstrukturierungen aber auch eine datenschutzrechtliche Komponente. Die Zusammenlegung ganzer Unternehmen, Unternehmenszweige oder aber die Veräußerung derselben, bedeutet auch immer, dass Kundendaten von einer Stelle an eine andere weitergegeben werden. Ob das ohne Einwilligung der Betroffenen zulässig ist, hat die obersten Datenschutzaufsichtsbehörden beschäftigt.

So ist hier zwischen folgenden Umstrukturierungen von Unternehmen zu unterscheiden: Bei der Verschmelzung, der sog. Fusion, wird ein Unternehmen von einem anderen vollständig aufgenommen oder aber zwei Unternehmen verschmelzen zu einem neuen (§ 2 Umwandlungsgesetz – UmwG –). Bei der sog. Spaltung von Unternehmen werden Teile desselben aufgespalten, abgespalten oder ausgegliedert (§ 123 UmwG). Entscheidend im Rahmen sämtlicher Umwandlungsformen ist die rechtliche Einordnung der „Verschiebung“ von personenbezogenen Kundendaten der Unternehmen.

Hinsichtlich des Tatbestandes der Fusion sind die obersten Datenschutzaufsichtsbehörden übereinstimmend der Auffassung, dass die Datenbestände der fusionierenden Unternehmen im Wege der Gesamtrechtsnachfolge auf das neue Unternehmen übergehen (§ 120 UmwG), ohne dass eine „Übermittlung“ von Daten im Sinne des Datenschutzrechts erfolgt. Das neu entstandene oder das ein anderes übernehmende Unternehmen tritt in die bestehenden Kundenverträge des übernommenen Betriebes ein. Es ist damit nicht Dritter im Sinne des Bundesdatenschutzgesetzes. Es bedarf mithin auch keiner Einwilligung des Kunden in den „Datentransfer“.

Bei der Abspaltung und Ausgliederung von Betriebsteilen stellt sich die Frage nach dem Erfordernis der Einwilligung gleichfalls nicht. Es tritt hier eine partielle Gesamtrechtsnachfolge ein mit der Konsequenz, dass Verträge zwischen dem „Altunternehmen“ und dessen Kunden im ganzen, also mit ihren Ansprüchen, Rechten und Verbindlichkeiten und natürlich den dazu notwendigen personenbezogenen Daten, auf den übernehmenden Rechtsträger, den neuen Betrieb, übergehen.

Anders als bei dem separaten Verkauf von Kundendaten als eigenständiges Vermögensgut (in diesem Fall würden die Regelungen des BDSG zum Zuge kommen), erfüllen Verschmelzungen und Spaltungen von Unternehmen grundsätzlich keine datenschutzrechtlichen Tatbestände. Sie richten sich vielmehr nach dem Umwandlungsgesetz.

31.3 Gebäude-Bild-Datenbank der Firma Tele-Info

Die niedersächsische Firma Tele-Info erfasst mit digitalen Kameras einen Großteil des Gebäudebestandes in Deutschland. Ihre Planung geht dahin, „eine der größten Bilddatenbanken der Welt“ unter dem Produktnamen „City-Server“ aufzubauen.

Mit einem gebäudeorientierten Selektionsverfahren sollen sich Wirtschaft, Industrie oder Behörden, ohne selbst vor Ort gehen zu müssen, über bebaute Grundstücke ein Bild machen können. Das Produkt soll nach Angaben des Verlages an Rettungsdienste, Notärzte, Polizei oder die Einsatzleitung der Feuerwehr verkauft werden. Als weitere Anwendungen nennt die Firma das Gebäude- und Anlagenmanagement, das Risk-Assessment bei Banken und Versicherungen, die Versorgungsunternehmen, Städte- und Verkehrsplanung und sog. Carriers (Zuteildienste, Speditionen, Taxizentralen).

Die Reaktionen der Bevölkerung und der datenschutzrechtlichen Fachkreise auf das Projekt sind beinahe durchgängig kritisch. Die Kritik bezieht sich insbesondere auf die Gefahr, dass die Aufnahmen der Gebäude zunächst ohne Wissen und ausdrückliche Einwilligung der betroffenen Hauseigentümer angefertigt werden und die weitere Verwendung des Datenmaterials nicht eingegrenzt ist. Die für das Projekt örtlich zuständige Daten-

schutzaufsichtsbehörde, der Landesbeauftragte für den Datenschutz Niedersachsen, vertritt die – von der überwiegenden Zahl der anderen Datenschutzaufsichtsbehörden jedoch nicht geteilte – Rechtsauffassung, dass das Bundesdatenschutzgesetz in seiner zur Zeit geltenden Fassung auf das umstrittene Projekt nicht anwendbar ist, da die Voraussetzungen des Dateibegriffs nach § 3 Abs. 2 BDSG nicht vorliegen.

Dieses für die Betroffenen wenig befriedigende Ergebnis zeigt die besondere Notwendigkeit für den Gesetzgeber, einer Entwicklung von Datenmacht in privater Hand, wie sie sich an dem Projekt „City-Server " beispielhaft zeigt, klare rechtliche Vorgaben zu geben und die Rechtsgrundlage für deren Beurteilung zu präzisieren. Dementsprechend habe ich dem Gesetzgeber konkrete Vorschläge für die Novellierung des BDSG unterbreitet und hoffe auf eine schnellstmögliche Realisierung.

Bis dahin bleibt den betroffenen Bürgern nur, einen Widerspruch gegen die Bildaufnahme ihres Gebäudes gegenüber der Firma Tele-Info einzulegen. Dessen Beachtung beruht jedoch auf freiwilliger Basis.

31.4 Neue Methoden zur Kundenwerbung und Kundenbindung: Data Warehouse und Data Mining

Data Warehouse und Data Mining, sind Schlagworte, die seit einigen Jahren durch die Computerszene geistern. Im Data Warehouse werden alle verwendbaren Daten in einem einheitlichen Datenpool losgelöst von ihrer ursprünglichen Verwendung zusammengeführt. Data Mining bietet Werkzeuge, die die scheinbar zusammenhanglosen Daten nach noch nicht bekannten, wissenswerten Zusammenhängen durchsuchen, Daten aufspüren, kombinieren und neue Informationen zur Verfügung stellen (s. auch 17. TB Nr. 8.2.4).

Während die werbenden Unternehmen den Vorteil dieser Methoden für den Kunden herausstellen, seinen Briefkasten von unerwünschter Werbung zu entrümpeln und ihm gezielt das Produkt anzubieten, an dem er – angeblich – interessiert ist, werden die Gefahren für das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger vielfach unterschätzt. Als Reaktion auf diese Entwicklung fasste die 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 14./15. März 2000 hierzu eine Entschließung (s. **Anlage 27**). Ohne die Entschließung vollständig wiederzugeben, ist festzuhalten, dass die Verfahren so auszugestalten sind, dass die Bürger hinreichend Kenntnis über sie haben. Wer persönliche Daten preisgibt, muss wissen, welche Risiken er eingeht, und in der Lage sein, seine Rechte wahrzunehmen. Datensammlungen dürfen nicht für beliebig wechselnde Zwecke verwandt und vorgehalten werden. Zweckändernde Verwendungen setzen eine wirksame Einwilligung der Betroffenen voraus. Die anstehende Umsetzung der Europäischen Datenschutzrichtlinie im Bundesdatenschutzgesetz stärkt den Grundsatz der Zweckbindung auch und gerade im Bereich der Privatwirtschaft (§ 28 Entwurf BDSG; insbesondere Absatz 1, Satz 2, wonach bereits bei der Erhebung personenbezogener Daten die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen sind; s. auch oben Nr. 2.1).

Wo die Grenze von der kundenorientierten Werbung hin zur Bildung von Persönlichkeitsprofilen überschritten wird, ist der Kern des informationellen Selbstbestimmungsrechtes berührt. Auf die Gefahr der Erstellung partieller oder weitgehend vollständiger Persönlichkeitsbilder, ohne dass der Betroffene deren Richtigkeit und Verwendung zureichend kontrollieren kann, hat bereits das Bundesverfassungsgericht in seinem Grundsatzurteil zum Volkszählungsgesetz vom 15. Dezember 1983, BVerfGE 65, 1 ff., hingewiesen und daraus folgend den notwendigen Schutz für die freie Entfaltung der Persönlichkeit aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs.1 GG abgeleitet. Das künftige BDSG bietet über die Einführung einer anlassfreien Kontrolle in § 38 BDSG-Entwurf und die erwähnte Umsetzung des strengen Zweckbindungsgrundsatzes der Europäischen Datenschutzrichtlinie die Handhabe für eine verstärkte Kontrolle der Aufsichtsbehörden. Auch der vom Bundesrat in das noch laufende Gesetzgebungsverfahren eingebrachte Änderungsvorschlag für eine Überarbeitung des Bußgeldkataloges in § 44 Abs. 2 BDSG-Entwurf, der die Sanktionierung von Verstößen gegen den Zweckbindungsgrundsatz ermöglichen würde, weist in diese Richtung und wird von mir unterstützt.

31.5 Datenschutz auch im Medienbereich

Das Spannungsverhältnis zwischen Datenschutz auf der einen und Presse- und Rundfunkfreiheit auf der anderen Seite hat im geltenden Recht zum sog. Medienprivileg des § 41 BDSG geführt, durch das datenschutzrechtlich weitreichende Ausnahmeregelungen für die Medien begründet werden. Art. 9 der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995 sieht hingegen für die Verarbeitung personenbezogener Daten allein zu journalistischen, künstlerischen oder literarischen Zwecken Abweichungen und Ausnahmen von den einschlägigen Vorschriften der Richtlinie nur insofern vor, als dies notwendig ist, um das Recht auf Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen. Dementsprechend sah der ursprüngliche Gesetzentwurf der Bundesregierung in § 41 vor, dass zahlreiche Vorschriften des BDSG künftig von den Ländern auch für die Datenverarbeitung von Unternehmen oder Hilfsunternehmen der Presse zu ausschließlich eigenen journalistisch-redaktionellen Zwecken angewandt werden sollten, so insbesondere Regelungen zum internen Datenschutzbeauftragten und zu Auskunftsrechten der Betroffenen. Hiergegen erhob sich in den Medien heftiger Widerstand, die hierin eine Beschränkung der vom Grundgesetz gewährleisteten Pressefreiheit sahen, obwohl auch das Grundrecht auf informationelle Selbstbestimmung Verfassungsrang hat und es lediglich um einen Ausgleich gleichrangiger Grundrechte gehen kann. Der schließlich im Mai 2000 gefundene Kompromiss sieht vor, dass zum einen das BDSG

die Standards im Hinblick insbesondere auf den technischen Datenschutz sowie eine Verpflichtung zum Schadensersatz bei Verletzung dieser Standards vorgibt und zum anderen der Deutsche Presserat sich verpflichtet, eine wirksame freiwillige Selbstkontrolle der redaktionellen Datenverarbeitung zu schaffen. Dementsprechend wurden der Entwurf zu § 41 BDSG und seine Begründung angepasst.

Zwischenzeitlich hat der Deutsche Presserat ein Konzept entwickelt, mit dem ein wirkungsvoller Schutz personenbezogener Daten in den Redaktionen und dessen Kontrolle durch den Presserat gewährleistet werden soll. Dieses sieht Verhaltenregeln und Empfehlungen zur Beachtung des Datenschutzes in den Redaktionen unter Beachtung der §§ 5, 9 und 38 a BDSG-E vor, wobei die Verlage dem Presserat über die durchgeführten Maßnahmen und grundsätzliche Änderungen berichten müssen. Anlaßunabhängig sollen zwischen einem Beauftragten des Deutschen Presserates und den Verlagen bzw. Redaktionen regelmäßig Gespräche über Stand und Entwicklung des Redaktionsdatenschutzes stattfinden. Der Presserat berichtet seinerseits regelmäßig der Öffentlichkeit hierüber.

Daneben soll bei begründeten Datenschutz-Beschwerden oder Anhaltspunkten für datenschutzrechtliche Mängel eine Anlassaufsicht treten. Diese wird durch einen besonderen Beschwerdeausschuss beim Deutschen Presserat für Beschwerden aus dem Bereich des Redaktionsdatenschutzes unterstützt, an den sich jedermann wenden kann, wenn er sich in seinen Persönlichkeitsrechten, speziell in seinem Recht auf Datenschutz, verletzt fühlt. Die daraufhin gegebenenfalls verhängten Sanktionen sind aufgrund einer Selbstverpflichtung der Verlage zu befolgen, entsprechendes gilt für die Veröffentlichung von Entscheidungen.

Schließlich sind auch die vom Deutschen Presserat entwickelten Richtlinien für die publizistische Arbeit (sog. Pressekodex), die auch bisher schon eine Reihe von Schutzbestimmungen zur Wahrung der Persönlichkeitsrechte Betroffener enthielten, um eine Reihe datenschutzrelevanter Regelungen erweitert worden. Für besonders wichtig halte ich hier den Auskunftsanspruch in Nr. 3.3 des Pressekodex, der allerdings weitreichenden Einschränkungen unterliegt, und den Anspruch auf Löschung personenbezogener Daten (Nr. 4.3 des Pressekodex), wenn diese unter Verstoß des Pressekodex erhoben wurden. In der Vergangenheit war es besonders unbefriedigend, wenn personenbezogene Daten unter Verletzung der publizistischen Grundsätze erlangt und unter Umständen sogar trotz erfolgreicher Beschwerde beim Deutschen Presserat weiter gespeichert, genutzt und übermittelt werden konnten. Dies ist künftig ausgeschlossen.

Wenn auch noch nicht alle datenschutzrechtlichen Wünsche und Vorstellungen erfüllt sind, so halte ich das vom Deutschen Presserat vorgelegte Konzept im Rahmen der gesetzgeberischen Vorgaben grundsätzlich für tragfähig. Zugleich ist es ein gutes Beispiel für Selbstregulierung durch Verhaltenskodizes, das künftig auch für andere Bereiche Bedeutung erlangen kann. Allerdings bleibt abzuwarten, wie es konkret umgesetzt und mit Leben erfüllt wird. Dies werde ich kritisch beobachten.

31.6 Auch das Aktienrecht muss datenschutzgerecht sein

Seit Sommer 1998 geht der Trend aller großen Unter-nehmen – hierunter Namen wie Daimler Chrysler AG, Lufthansa, Siemens oder die Deutsche Bank – von der bisher gängigen Inhaberaktie hin zur Namensaktie. Diese ist international üblich und erleichtert den Firmen den direkten Kontakt zum Geldgeber (Investor relations). Der Siegeszug der Namensaktie hatte jedoch auch seine Schattenseite. Die aktienrechtlichen Vorschriften im Zusammenhang mit der Namensaktie stammten aus einer Zeit, als es weder einen elektronischen Börsenhandel, ein digitales Aktienregister noch einen schwunghaften Adresshandel gab. Die Renaissance dieser Aktienform führte daher zunächst zu problematischen datenschutzrechtlichen Konsequenzen. So musste z. B. jeder Anleger seinen Beruf zur Eintragung in das Aktienbuch angeben. Ein persönliches Datum, das seinen ursprünglichen Zweck, der besseren Identifizierung, heute gar nicht mehr erfüllen kann. Das im Aktiengesetz normierte Einsichtsrecht eines jeden Anlegers in alle Einträge des Aktienbuchs begründete das Risiko, dass der einzelne Aktionär ganz einfach zu einem „Objekt der Begierde“ für Adresshändler werden konnte, denen der freie Zugang zu den Aktienbüchern theoretisch durch den Kauf nur einer Aktie möglich gewesen wäre. Auch galt es der Möglichkeit zu begegnen, dass Anleger prüfen konnten, ob und wie viele Aktien der Nachbar, Arbeitskollege oder Prominente halten. Für die Unternehmen ist es sicherlich von Vorteil, wenn sie auf die Namen ihrer Anleger zugreifen können, um sie im Rahmen der Aktionärspflege zu informieren. Dies ist aus meiner Sicht nicht zu kritisieren. Es musste aber ausgeschlossen werden, dass die Aktienbücher zu allen möglichen Marketingzwecken missbraucht werden, also beispielsweise der Inhaber einer Automobilaktie ungewollt Werbung für Waschmaschinen in seinem Briefkasten vorfindet.

Ich habe deshalb die Bundesregierung aufgefordert, schnell zu handeln und die datenschutzrechtlichen Probleme zu lösen. Seit Kurzem ist nunmehr ein neues Namensaktiengesetz (NaStrAG) in Kraft, das die bisherigen Regelungen zur Namensaktie den heutigen datenschutzrechtlichen Erfordernissen anpasst (s. BGBl. 2001 I Nr. 4, S. 123). So sieht das Gesetz vor, das Einsichtsrecht in das Aktienregister erheblich einzuschränken und auf die eigenen Daten des jeweiligen Aktionärs zu begrenzen.

Ferner wurde eine Zweckverwendungsregelung für die Daten aufgenommen, die bestimmt, wofür die Gesellschaft die Daten aus dem Aktienregister verwenden darf und wofür nicht. Auch wurden die in das Aktienregister aufzunehmenden Daten neu bestimmt. So soll nicht mehr die gesamte Adresse eines Aktionärs in das Register aufgenommen werden, sondern lediglich die Gemeinde – unter Weglassung von Strasse und Hausnummer.

Mit diesen Regelungen ist die Bundesregierung meinen Empfehlungen gefolgt. Eine unbefriedigende Regelung ist jedoch die aktienrechtliche Pflicht zur Veröffentlichung des Teilnehmerverzeichnisses der Aktionärsversammlung. Zwar soll es dem Namensaktionär künftig ermöglicht werden, sich der Offenlegung seines Aktienbesitzes dadurch zu entziehen, dass er sich auf der Hauptversammlung durch sein Kreditinstitut vertreten lässt. Darüber hinaus streicht das Gesetz das Teilnehmerverzeichnis aus der Liste der zum Handelsregister einzureichenden und dort jedermann zugänglichen Unterlagen. Das Recht der Aktionäre, die Teilnehmerliste der Hauptversammlung während eines Zeitraums von zwei Jahren bei der Gesellschaft einzusehen, soll jedoch bestehen bleiben. Wer seinen Datenschutz wirksam gewahrt wissen will, dem bleibt daher nichts anderes übrig, als auf die persönliche Teilnahme an der Hauptversammlung zu verzichten. Um hier einen datenschutzrechtlichen Missbrauch auszuschließen, hätte ich mir gewünscht, dass zumindest die Nutzung der in der Teilnehmerliste enthaltenen Daten auf berechtigte, gesellschaftsbezogene Zwecke beschränkt worden wäre.

31.7 Einzelfragen aus dem Düsseldorfer Kreis

Im „Düsseldorfer Kreis“ sind die obersten Aufsichtsbehörden der Länder für den Datenschutz im nicht-öffentlichen Bereich vertreten (s. auch 17. TB Nr. 31.5). Interessante Einzelfragen im Berichtszeitraums waren u. a.:

31.7.1 Bonitätsprüfungen vor Durchführung ärztlicher Behandlungen

Immer häufiger ist es für Ärzte, besonders auch Zahnärzte, notwendig, bei umfangreichen Behandlungen die Bonität ihrer Patienten zu prüfen. Es handelt sich hier um Fälle, bei denen die behandelnden Ärzte, etwa durch das Hinzuziehen von Zahntechnikern, Vorleistungen erbringen müssen. Wegen der damit verbundenen finanziellen Risiken vergewissern sich die Ärzte durch Anfragen bei einem Kreditschutzunternehmen oder einer Auskunftei über die Bonität der zu behandelnden Patienten.

Solche Bonitätsanfragen sind wegen ihres Bezugs zu den Gesundheitsdaten der Patienten besonders problematisch. Zur Beantwortung der Anfragen müssen personenbezogene Daten übermittelt werden, mit denen eindeutig die Identität der Patienten oder bei minderjährigen Patienten die Identität der zahlungspflichtigen Erziehungsberechtigten festgestellt werden kann. Zugleich wird offenbart, dass jemand ärztlich behandelt wird, was eine unbefugte Preisgabe eines nach § 203 StGB geschützten fremden Geheimnisses bedeutet.

Nach gemeinsamer Auffassung der Aufsichtsbehörden ist daher vor einer solchen Bonitätsanfrage eine Einwilligung des Patienten oder je nach Fallgestaltung des Erziehungsberechtigten einzuholen. Der Arzt muss den Patienten informieren, an welches Unternehmen die Bonitätsanfrage gerichtet wird. Bei der Anfrage selbst dürfen nur im unbedingt notwendigen Umfang Daten übermittelt werden. Keinesfalls dürfen hier Angaben zur Erkrankung oder zur Behandlung weitergegeben werden.

31.7.2 Informationsaustausch der privaten Krankenversicherer nach Vertragsabschluss

Rückfragen von privaten Krankenversicherungen nach bis zu zehn Jahren zurückliegenden Gesundheitsdaten beim Vorversicherer boten Anlass für eine Erörterung der Aufsichtsbehörden mit den Vertretern der Versicherungswirtschaft. In diesen Einzelfällen fehlte ein konkreter Bezug der Abfragen zu den aktuellen Kostenerstattungsanträgen der Versicherten.

Mit der Versicherungswirtschaft bestand Einigkeit darüber, dass ein so umfassender Datenaustausch zur Risikoprüfung grundsätzlich nur vor Vertragsabschluss aufgrund der Schweigepflichtentbindungserklärung zulässig ist. Danach sind nur noch innerhalb eines Zeitraumes von fünf Jahren anlassbezogene Rückfragen zulässig, die mit den aufgetretenen Krankheits- oder Beschwerdebildern in Zusammenhang stehen.

31.7.3 Datenschutz im Call-Center

Viele Unternehmen bedienen sich sog. Call-Center zur Beantwortung von Kundenanfragen und -problemen. Call-Center sind hochtechnisierte computergestützte Unternehmen, die anbieten, Kunden, Lieferanten und Mitarbeiter insbesondere mittels TK-Einrichtungen zu betreuen.

Insbesondere die Frage, ob Kundengespräche mit den jeweiligen Beratern des Call-Centers durch zum Beispiel einen Teamleiter mitgehört oder aufgezeichnet werden dürfen, beschäftigte die Aufsichtsbehörden. Auf Seiten der Call-Center besteht hier ein Interesse, die Qualität der Kundenbetreuung auf diese Weise überprüfen zu können.

Die Aufsichtsbehörden sind sich einig, dass eine Aufzeichnung von Gesprächen nur nach vorheriger Einwilligung des Kunden in Betracht kommt. Eine Aufzeichnung ohne eine solche Einwilligung ist grundsätzlich nach § 201 StGB als „*Verletzung der Vertraulichkeit des Wortes*“ strafbar. Beim Mithören eines Kundengespräches zu Überprüfungs- oder Ausbildungszwecken empfehle ich ebenfalls regelmäßig eine Information des Anrufers. Auch der Arbeitnehmer, dessen Gesprächsführung durch das Mithören auf Seiten des Arbeitgebers überprüft wird, ist nicht schutzlos. Ein heimliches Mithören von Gesprächen ist generell unzulässig. Wenn der Arbeitgeber beispielsweise in der Probezeit oder stichprobenweise Gespräche des Arbeitnehmers mithören möchte, muss er ihn vorher darüber informieren.

31.7.4 Der gläserne Kunde oder die Wiederkehr der Rabattmarke?

Das Rabattmarkensystem der Vergangenheit feiert Wiederauferstehung. Aber, geht es hier wirklich nur darum,

dem treuen Kunden über ein Bonussystem Rabatte zu gewähren?

Im stationären Handel gibt es die PAYBACK-Karte, mit der beim täglichen Einkauf oder auch beispielsweise beim Tanken bei zahlreichen angeschlossenen Partnerunternehmen PAYBACK-Bonuspunkte gesammelt werden können. Wenn der Kunde genug Punkte beisammen hat, kann er sie sich auszahlen lassen. Auch beim Surfen im Internet haben die digitalen Rabattmarken Einzug gehalten.

Ohne dass es für die Rabattgewährung erforderlich wäre, werden auch mit Einverständniserklärungen der Kundinnen und Kunden eine Vielzahl persönlicher Daten gesammelt. Diese dienen dazu, gezielt auf persönliche Interessen abgestimmte Werbung zu verschicken und allgemein für Werbe-, Marketing und Marktforschungszwecke genutzt zu werden. Die Aufsichtsbehörden haben begonnen, sich mit den Rabattgewährungsverfahren auseinander zu setzen. So ist deren Transparenz von hoher Bedeutung und der Kunde muss informiert und sich bewusst sein, dass die Vorteile des Rabattes bei den derzeitigen Systemen mit einer Preisgabe seiner persönlichen Daten einhergehen.

31.8 Private Sicherheitsdienste

Schon in früheren Tätigkeitsberichten (16. TB Nrn. 1.4 und 31.1; 17. TB Nr. 1.2.4) habe ich über die datenschutzrechtlichen Aspekte der Tätigkeit privater Sicherheitsdienste berichtet.

Das Thema hat von seiner Aktualität nichts verloren. Auch in den vergangenen zwei Jahren war das Erfordernis datenschutzrechtlicher Regelungen für die Sicherheitsdienste Gegenstand intensiver Diskussionen. Angestoßen wurden diese durch die Absicht der Bundesregierung, den Rechtsrahmen für das private Sicherheitsgewerbe durch Änderung der Gewerbeordnung neu zu regeln. Zum datenschutzrechtlichen Handlungsbedarf hat mich die Bundesregierung um Stellungnahme gebeten.

Nach dem BDSG habe ich in weiten Teilen des nicht-öffentlichen Bereiches keine Beratungs- und Kontrollkompetenz. Insofern kann ich mir Kenntnisse über Arbeitsweise und Betätigungsfelder privater Sicherheitsdienste sowie über die ihnen zur Verfügung stehenden und zum Einsatz gebrachten technischen Mittel nicht mittels Kontrollen bei den Sicherheitsdiensten verschaffen. Um der Bitte der Bundesregierung gleichwohl nachkommen zu können, habe ich intensive Gespräche mit Unternehmen des privaten Sicherheitsgewerbes geführt, die wertvolle Erkenntnisse über den Umfang der von ihnen durchgeführten personenbezogenen Datenverarbeitung ergaben.

Der Inhalt der Gespräche betraf im wesentlichen den Umgang mit Daten von Dritten, die z. B. im Rahmen von Personen- oder Objektschutzdienstleistungen von Bewachungsunternehmen erhoben werden. Ich wurde darüber informiert, dass eine Verarbeitung von Daten Dritter in Bewachungsunternehmen selbst nur in einem sehr geringen Maße erfolgt. Zwar sei es üblich, dass in nahezu allen Tätigkeitsfeldern der privaten Sicherheitsunternehmen Daten von Dritten, z. B. von Störern, Kaufhausdieben oder unberechtigt an einem Schutzobjekt sich aufhaltenden Personen erhoben würden. Diese Daten würden jedoch unverzüglich dem Auftraggeber übermittelt. Nur zum Nachweis der Tätigkeit des Sicherheitsdienstleisters vor Ort würden Kopien von diesen Meldungen, die im konkreten Einzelfall Daten zu dritten Personen enthalten können, zu den im Sicherheitsunternehmen geführten Akten genommen. Eigene Zentraldateien zur Erfüllung diverser Geschäftszweige oder „Warndateien“ mit personenbezogenen Daten über „Wiederholungstäter“ würden nicht geführt. Lediglich im Bereich der Personenschutzdienstleistungen würden in geringem Umfang Daten zu Dritten aus dem Umfeld der zu schützenden Person beim Sicherheitsunternehmen gespeichert. Dies erfolge in der Regel nicht dateigestützt, sondern nur in Akten.

Auf der Grundlage dieses Kenntnisstandes über die Tätigkeit des privaten Sicherheitsgewerbes und im Hinblick darauf, dass die Novelle zum BDSG (s. o. Nr. 2.1) auch in den für die nicht-öffentlichen Stellen geltenden Abschnitten Verbesserungen mit sich bringen wird, habe ich Forderungen nach zusätzlichen Vorschriften im Rahmen der gesetzlichen Neuregelung des privaten Sicherheitsgewerbes zunächst zurückgestellt. Es muss jedoch gewährleistet werden, dass das BDSG auch dann anwendbar ist, wenn – wie dies offensichtlich der Normalfall ist – personenbezogene Daten von privaten Sicherheitsunternehmen in Akten verarbeitet und genutzt werden. Denn auch nach der geplanten BDSG-Novelle gelten die Vorschriften des dritten Abschnitts für nicht-öffentliche Stellen nur insofern, als die Verarbeitung und Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen oder in Speichermedien erfolgt, die dem Begriff der nicht-automatisierten Datei gem. § 3 Abs. 2 BDSG unterfallen. Da nicht-strukturierte Akten und Aktensammlungen aus dem Anwendungsbereich herausfallen, würden die Verbesserungen der BDSG-Novelle im dritten Abschnitt, wie z. B. die ausdrückliche Regelung der Datenerhebung durch nicht-öffentliche Stellen, die Stärkung des Zweckbindungsprinzips sowie die Ausdehnung der Kontrollbefugnisse der Datenschutz-Aufsichtbehörden, für Bewachungsunternehmen nicht greifen.

Ich habe daher angeregt, im Rahmen der beabsichtigten Änderung der Gewerbeordnung eine Regelung vorzusehen, die sicherstellt, dass die Vorschriften des dritten Abschnitts des BDSG auch dann anzuwenden sind, wenn personenbezogene Daten außerhalb von nicht-automatisierten Dateien erhoben, verarbeitet oder genutzt werden. Ich halte die uneingeschränkte Anwendung dieser Vorschriften für das private Sicherheitsgewerbe auch im Hinblick auf die zunehmende Zusammenarbeit mit Polizeibehörden der Länder im Rahmen von sog. Sicherheitspartnerschaften für geboten, denn für letztere sind Aufgaben und Befugnisse umfassend in den einschlägigen Polizeigesetzen geregelt.

Auch der Geschäftszweck der Bewachungsunternehmen rechtfertigt die Ausdehnung des Anwendungsbereiches des BDSG auf Unternehmen dieses Gewerbes im Verhältnis zu anderen nicht-öffentlichen Stellen. Denn im Rah-

men der Erfüllung der Vertragspflicht geraten nicht nur bescholtene, sondern auch unbeteiligte Bürger in das Visier privater Sicherheitsdienste. Das geschieht zudem in weit größerem Umfang, als dies im Zusammenhang mit der Tätigkeit anderer nicht-öffentlicher Stellen der Fall wäre.

Der von mir dargelegte Regelungsbedarf steht unter der Prämisse der Verwirklichung der BDSG-Novelle, wie sie vom Bundeskabinett in das Gesetzgebungsverfahren eingebracht wurde. Eine andere Beurteilung ergäbe sich auch dann, wenn sich die Bewachungsunternehmen andere Tätigkeitsfelder erschlössen oder mit Aufgaben im hoheitlichen Bereich beauftragt würden und sich damit zwangsläufig auch die Art und Weise sowie der Umfang der personenbezogenen Datenverarbeitung ändern würden.

Ich halte an meiner Auffassung fest, dass „private Sicherheitstätigkeiten", die dadurch gekennzeichnet sind, dass Personen mit oder ohne deren Wissen beobachtet und Daten von ihnen erhoben, verarbeitet und genutzt werden, datenschutzrechtlich problematisch sind. Dies gilt für Bewachungsunternehmen, Detekteien und andere nicht-öffentliche Stellen, die sich mit derartigen Aufgaben befassen. Zwar wird das novellierte BDSG zahlreiche Verbesserungen mit sich bringen, die auch in diesem Bereich wirken werden. Die Vorschriften sind jedoch zu allgemein, um den spezifischen Risiken für das informationelle Selbstbestimmungsrecht Betroffener, die von diesen Tätigkeiten ausgehen, angemessen Rechnung zu tragen. Weitergehende bereichsspezifische Datenschutzregelungen anlässlich der von der Bundesregierung beabsichtigten Neuregelung des Rechtsrahmens für das private Sicherheitsgewerbe zu fordern, hätte jedoch bedeutet, diesen Unternehmenszweig gegenüber anderen Sicherheitsdienstleistern unangemessen zu benachteiligen. Ich behalte mir aber vor, im Rahmen der zweiten Stufe der Novellierung des BDSG (s. o. Nr. 2.1) Verbesserungen insbesondere im Hinblick auf die Rechte der von „privaten Sicherheitstätigkeiten" Betroffenen anzustreben.

32 Internationale Zusammenarbeit und Datenschutz im Ausland

32.1 Datenschutz im Europarat

Dem „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten" – der Europaratskonvention 108 aus dem Jahre 1981 – trat im Berichtszeitraum ein weiterer Mitgliedsstaat des Europarats bei. Im September 2000 ratifizierte die Slowakische Republik die Konvention, die dort zum 1. Januar 2001 in Kraft getreten ist. Damit erhöhte sich die Zahl der Staaten, in denen das Übereinkommen gilt, auf 21. Nach der Aufnahme Georgiens im April 1999 ist die Zahl der Mitglieder des Europarates selbst auf 41 angewachsenen. Litauen hat die Konvention am 11. Februar 2000 gezeichnet, aber bislang nicht ratifiziert.

Das Ministerkomitee verabschiedete am 23. Februar 1999 die Empfehlung zum Schutz personenbezogener Daten im Internet (R(99)5), die im Anhang die „Leitlinien für den Schutz der Privatsphäre im Internet" enthält. Die sog. Internet Guidelines stellen das erste derartige Regelwerk auf internationaler Ebene dar. Die Empfehlung verlangt von den Providern frühzeitige und umfassende Aufklärung über die mit ihren Diensten möglicherweise verbundenen Risiken und appelliert an die Nutzer, alle erreichbaren technischen Vorkehrungen zum Aufbau eines hohen Eigenschutzes zu treffen. Die Guidelines setzen dabei vor allem auf die Eigeninitiative von Providern und Nutzern, die möglichst weit im Vorfeld staatlicher Regulierung ansetzen sollte. Sie eignen sich daher insbesondere als Modell für Verhaltensregeln (sog. codes of conduct) im nicht-öffentlichen Bereich.

Am 15. Juni 1999 nahm das Ministerkomitee eine Änderung der Datenschutzkonvention an, die den Beitritt der Europäischen Gemeinschaften zur Datenschutzkonvention ermöglichen soll, der bisher nur Staaten beitreten konnten. Die Änderung trägt den seit Verabschiedung der EG-Datenschutzrichtlinie erweiterten Zuständigkeiten der Union Rechnung, im Regelungsbereich der Richtlinie mit Drittstaaten und internationalen Organisationen Verpflichtungen einzugehen.

Der Beratende Ausschuss des Europaratsübereinkommens (T-PD) hat am 21. Juni 2000 den Entwurf eines Zusatzprotokolls zum Übereinkommen 108 über Kontrollinstanzen und grenzüberschreitende Datenflüsse angenommen. Zum einen sollen die Vertragsparteien dadurch verpflichtet werden, in Anlehnung an Artikel 28 der EG-Datenschutzrichtlinie eine oder mehrere völlig unabhängig arbeitende Kontrollbehörden einzurichten, die mit der Einhaltung der Beachtung der Datenschutzbestimmungen beauftragt werden und über Ermittlungs- und Interventionsbefugnisse verfügen. Zum anderen soll das künftige Protokoll Regelungen über den grenzüberschreitenden Datenverkehr mit Nicht-Vertragsstaaten einführen, wobei die ins Auge gefassten Bestimmungen nach dem Vorbild der Artikel 25 und 26 der Datenschutzrichtlinie konzipiert sind.

Die Projektgruppe Datenschutz (CJ-PD) verabschiedete einen Empfehlungsentwurf über den Schutz von personenbezogenen Daten, die zu Versicherungszwecken verarbeitet werden (zu den Vorarbeiten s. 16. TB und 17. TB je Nr. 32.1). Im Vordergrund stehen – in Übereinstimmung mit der EG-Datenschutzrichtlinie – die Voraussetzungen der Rechtmäßigkeit der Datenverarbeitung zu Versicherungszwecken sowie Regelungen zu den Betroffenenrechten, zum Rahmen für mögliche automatisierte Einzelentscheidungen, zur Datensicherheit und zum grenzüberschreitenden Datenverkehr.

Bemerkenswert ist die Tatsache, dass die Gremien des Europarates mehr und mehr die Regelungen der **EG-Datenschutzrichtlinie** berücksichtigen, indem sie diese als Orientierung an den Anfang ihrer Überlegungen stellen oder sogar konkret als Richtschnur für zu verabschiedende Rechtstexte nutzen.

32.2 Ein Blick in europäische Länder außerhalb der Union

32.2.1 Der Europäische Wirtschaftsraum und die Schweiz

Als Mitglieder des Europäischen Wirtschaftsraums (EWR), für den die EG-Datenschutzrichtlinie nach Aufnahme in das Abkommen über den EWR volle Wirksamkeit entfaltet (vgl. 17. TB Nr. 32.2.1), haben **Norwegen** und **Island** ihre Datenschutzgesetze aus den Jahren 1978 bzw. 1981 an die Vorgaben der Richtlinie angepasst. Das norwegische Parlament verabschiedete im April 2000 das neue Datenschutzgesetz, das zusammen mit einer Reihe von Rechtsverordnungen zur Konkretisierung einzelner Vorschriften des Gesetzes am 1. Januar 2001 in Kraft trat. Zum selben Zeitpunkt wurde auch das isländische „Gesetz zum Schutz des einzelnen bei der Verarbeitung personenbezogener Daten“ vom 23. Mai 2000 in Kraft gesetzt.

Die revidierte **schweizerische** Bundesverfassung vom 18. April 1999 statuiert in Art. 13 ausdrücklich das Recht auf den Schutz der Privatsphäre sowie einen Anspruch auf Schutz vor Missbrauch personenbezogener Daten. Damit wird das Grundrecht auf Datenschutz, das bisher aus dem ungeschriebenen Recht auf persönliche Freiheit und dem Anspruch auf Achtung des Privatlebens gem. Art. 8 der Europäischen Menschenrechtskonvention (EMRK) hergeleitet wurde, in der Bundesverfassung institutionell verankert. Die Europäische Kommission hat per Entscheidung vom 26. Juli 2000 festgestellt, dass die Schweiz ein angemessenes Datenschutzniveau i. S. von Art. 25 Abs. 2 der europäischen Datenschutzrichtlinie 95/46/EG (s. oben Nr. 2.2.2) gewährleistet.

32.2.2 Die Mittel- und Osteuropäischen Staaten

Wenige Wochen nach Verabschiedung des neuen **tschechischen** Datenschutzgesetzes am 4. April 2000 fand auf Einladung des Innenministers der tschechischen Republik eine Fortsetzung des Gedankenaustauschs (vgl. 17. TB Nr. 32.2.2) über gemeinsam interessierende Datenschutzfragen in Prag statt, an der von tschechischer Seite überwiegend Führungskräfte der Polizei- und Sicherheitsabteilungen des Ministeriums des Innern sowie nachgeordneter Behörden teilnahmen. Neben Fragen der internationalen Zusammenarbeit im Polizeibereich (Schengen, EUROPOL, Interpol) standen Themen im Zusammenhang mit der europäischen Datenschutzrichtlinie, dem Schutz personenbezogener Daten im Fernmeldeverkehr und den Herausforderungen der neuen Informationstechnologien im Vordergrund der Beratungen.

Terminologie und Definitionen des am 1. Juni 2000 in Kraft getretenen Datenschutzgesetzes **Tschechiens** (zum Vorgängergesetz vgl. 17. TB Nr. 32.2.2) wurden in Anlehnung an die EG-Datenschutzrichtlinie entwickelt. Das Gesetz entspricht mit seinen Regelungen in vielem dem deutschen BDSG und dem Novellierungsentwurf dazu (s. o. Nr. 2.1). Es sieht auch die Schaffung einer Datenschutzkontrollinstanz vor. Erster Leiter der Kontrollinstanz ist Dr. Karel Neuwirth, der bereits zu einem Meinungsaustausch in meinem Hause war.

Im April des vergangenen Jahres habe ich gemeinsam mit der Datenschutzbeauftragten **Polens**, Frau Dr. Kulesza, ein dreitägiges Datenschutzseminar in Bonn veranstaltet, an dem über 20 Mitarbeiter unserer beiden Behörden teilnahmen. Zu den Themen von beiderseitigem Interesse gehörten die EG-Datenschutzrichtlinie und ihre Umsetzung in das deutsche Recht sowie die Übereinstimmungen des polnischen Datenschutzgesetzes aus dem Jahre 1997 (vgl. 17. TB Nr. 32.2.2) mit den Anforderungen der Richtlinie. Einen wichtigen Teil des Seminars bildete auch der Erfahrungsaustausch zu Fragen der Beratungs- und Kontrollpraxis, der Behandlung von Eingaben und der Betroffenenrechte. Daneben standen aktuelle Probleme des nicht-öffentlichen Bereichs, Reformfragen wie die Vorabkontrolle und der Datenschutz bei Polizei- und Sicherheitsbehörden sowie in der Telekommunikation auf der Tagesordnung. Teledienste und Internet bildeten weitere Schwerpunkte des Seminars.

Für **Ungarn** hat die Europäische Kommission am 26. Juli 2000 per Entscheidung festgestellt, dass i. S. v. Art. 25 Abs. 2 der europäischen Datenschutzrichtlinie 95/46/EG (s. o. Nr. 2.2.2) ein angemessenes Datenschutzniveau gewährleistet ist.

In den baltischen Staaten gibt es seit 1996 Datenschutzgesetze in **Estland** und **Litauen,** während in **Lettland** dem Parlament ein Regierungsentwurf aus dem Jahre 1998 vorliegt. Das estnische Gesetz sieht ausdrücklich die Einrichtung einer unabhängigen Datenschutzbehörde vor, wohingegen die Kontrollinstanz in Litauen bislang noch vollständig in die staatliche Behördenstruktur eingebunden ist. Auch der lettische Entwurf sieht derzeit nicht vor, die künftige Kontrollinstanz unabhängig zu organisieren.

Die gesetzgeberischen Vorhaben auf Kabinetts- oder Parlamentsebene in **Bulgarien**, **Moldawien** und **Rumänien**, über die ich im 17. TB (Nr. 32.2.2) berichtet habe, sind noch nicht verwirklicht. Dagegen hat **Slowenien**, das bereits seit 1990 über ein Datenschutzgesetz verfügt, 1999 eine umfassende Novellierung auf den Weg gebracht, die sich in zahlreichen Punkten an der EG-Richtlinie orientiert, allerdings keine unabhängige Kontrollinstanz vorsieht.

32.3 Entwicklungen im nicht-europäischen Ausland

Im 17. TB (Nr. 32.3) berichtete ich über erste gesetzgeberische Schritte auf dem Weg zu einem Datenschutzrecht für **Lateinamerika**. Mit dem „Gesetz zum Schutz des Privatlebens“ vom Oktober 1999 regelt **Chile** nunmehr als erstes südamerikanisches Land die Verarbeitung personenbezogener Daten im öffentlichen und privaten Bereich. Das Gesetz sieht allerdings eine Vielzahl von Ausnahmen vor und räumt den Betroffenen neben dem Recht auf Auskunft und Berichtigung lediglich die Möglichkeit gerichtlicher Überprüfung ein, denn eine von sich aus tätige externe Kontrollinstanz ist nicht vorgesehen.

Im Juni 2000 trat das **mexikanische** Gesetz über den E-Commerce in Kraft, das in Form eines Artikelgesetzes das Zivilgesetzbuch, das Handelsgesetzbuch, die Zivilprozessordnung und das Verbraucherschutzgesetz novelliert und datenschutzrechtliche Regelungen sowie Vorschriften über digitale Signaturen und elektronische Dokumente enthält.

Kurz vor dem Abschluss steht ein Datenschutzgesetz für **Argentinien,** nachdem ein entsprechender Entwurf im September 2000 vom Repräsentantenhaus gebilligt wurde. Der Entwurf hat in hohem Maße die EG-Datenschutzrichtlinie zum Vorbild und sieht u. a. eine unabhängige Kontrollinstanz vor.

Im Parlament von **Peru** wurde im Oktober 1999 der Entwurf eines Datenschutzgesetzes eingebracht, der sich neben anderen ausländischen Vorbildern vor allem an den neuen Datenschutzgesetzen Spaniens und Italiens (s. o. Nr. 2.6) sowie an der EG-Datenschutzrichtlinie orientiert und dabei u. a. die Einrichtung eines Datenschutzbeauftragten vorsieht.

Akzeptanzprobleme im Zusammenhang mit dem E-Commerce, schlagzeilenträchtige Missbrauchsfälle und nicht zuletzt Meinungsumfragen haben zu einem stetig wachsenden Datenschutzbewusstsein in den **USA** geführt. So ergab eine von der Zeitschrift Business Week im März 2000 durchgeführte Untersuchung, dass 63 % der Internetsurfer und 41 % der online Einkaufenden sehr beunruhigt über den Schutz ihrer Privatsphäre sind. 57 % aller US-Bürger treten danach grundsätzlich für eine gesetzliche Regelung des Umgangs mit personenbezogenen Daten ein. Mit Blick auf die EG-Datenschutzrichtlinie und die Verhandlungen mit der EU über einen adäquaten Schutz der aus Europa in die USA übermittelten Daten (s. o. Nr. 2.2.2) sieht man sich in den Vereinigten Staaten mehr und mehr zumindest einem indirekten Druck zur Schaffung eines angemessenen Datenschutzniveaus, auch für die US-Bürger selbst, ausgesetzt. Verbunden mit der Andeutung, dass gesetzliche Regelungen unausweichlich werden könnten, hat Präsident Clinton im März 2000 als erste Antwort eine „Information Age Agenda“ vorgestellt, die u. a. eine Aufforderung an Internetbetreiber zur Schaffung von Mindeststandards für den Schutz der Privatsphäre enthält. Außerdem ernannte er einen Chief Counsellor for Privacy, der vom Weißen Haus aus das Bundesrecht für den öffentlichen und privaten Bereich unter Datenschutzgesichtspunkten überprüfen und beobachten soll. Nach der Verabschiedung durch beide Häuser des Kongresses und der – handschriftlichen und elektronischen – Unterzeichnung durch Präsident Clinton trat am 1. Oktober 2000 der „Electronic Signatures in Global and National Commerce Act“ in Kraft, der die rechtliche Gleichstellung der elektronischen mit der eigenhändigen Unterschrift in Papierform regelt. Im Gegensatz zum deutschen Signaturgesetz trifft das amerikanische Pendant keine Aussagen darüber, welche Authentifizierungsverfahren im Einzelnen zugelassen sind. Bedeutende Rechtsgeschäfte, wie z. B. die Erstellung eines Testaments, Kündigungen von Versicherungs- und anderen wichtigen Verträgen oder Willenserklärungen in Familienrechtsstreitigkeiten, bedürfen weiterhin der Unterschrift auf Papier.

Der zum 1. Januar 2001 in Kraft getretene „Personal Information Protection and Electronic Documents Act“ gewährt in umfassender Weise den bislang in **Kanada** durch Bundesrecht nicht geregelten Datenschutz im privaten Bereich. Das Gesetz erstreckt sich auch auf den Arbeitnehmerdatenschutz aller dem Bundesrecht unterfallenden Unternehmen.

Die Bemühungen des **australischen** Bundesgesetzgebers um bislang fehlende Datenschutzregelungen für den nicht-öffentlichen Bereich (vgl. 17. TB Nr. 32.3) sind in ein entscheidendes Stadium getreten, nachdem ein entsprechender Regierungsentwurf demnächst im Repräsentantenhaus und anschließend im Senat zur Beratung ansteht. Allerdings erscheint die Gesetzesvorlage in ihrer derzeitigen Fassung – durch weitgehende Ausnahmeregelungen, zahlreiche Durchbrechungen des Zweckbindungsgedankens und Ausgliederung der Arbeitnehmerdaten – eher weniger geeignet, den Datenschutz im privaten Bereich voranzubringen.

Anlässlich eines weiteren (vgl. 17. TB Nr. 32.3) Besuches einer **japanischen** Regierungsdelegation in meiner Dienststelle im Frühjahr 2000 konnte ich mich wieder aus erster Hand über neueste Entwicklungen in Japan unterrichten. So wurde vom Parlament im Mai 1999 ein Informationsfreiheitsgesetz verabschiedet, das im April 2001 in Kraft tritt. Im Oktober 2000 wurde der Entwurf für ein allgemeines nationales Datenschutzgesetz in das Gesetzgebungsverfahren eingebracht. Das künftige Gesetz soll für den öffentlichen und den bisher weitgehend ungeregelt gebliebenen privaten Bereich gelten und neben grundlegenden Definitionen allgemeine Datenschutzprinzipien enthalten, weshalb es schon jetzt als „Grundgesetz für den Datenschutz“ bezeichnet wird.

Nachdem in **Thailand** bereits Ende 1997 der Official Information Act in Kraft getreten ist, der den Bürgern weitgehenden Zugang zu amtlichen Informationen und die Berichtigung darin enthaltener unrichtiger Daten gewährt, erwägt die Regierung eine Ausweitung seines Anwendungsbereichs auf den privaten Bereich.

32.4 Die Internationale Datenschutzkonferenz

Als Pendant zu den Frühjahrskonferenzen der europäischen Datenschutzbeauftragten (s. o. Nr. 2.5) tagten die 21. und die 22. Internationale Datenschutzkonferenz vom 13. bis zum 15. September 1999 in Hongkong und vom 28. bis 30. September 2000 in Venedig.

In Hongkong standen die Informationstechnologien im Zeitalter der Globalisierung im Mittelpunkt der Beratungen. Themenschwerpunkte bildeten dabei die Vorteile und Risiken der neuen Technologien für die informationelle Selbstbestimmung des Einzelnen und hier vor allem die Gefahrenpotentiale bestehender und künf-

tig denkbarer Überwachungsstrukturen sowie die damit zusammenhängenden Fragen der Garantie einer geschützten Privatsphäre und der Datensicherheit im Rahmen von Datenschutzauditierungen. Die Konferenz befasste sich daneben mit der internationalen Zusammenarbeit im Polizeibereich, mit der Beziehung zwischen Informationsfreiheit und Datenschutz, dem Datenschutz in den neuen Medien, den Implikationen der aufkommenden Cyber-Gesetzgebungen und mit den Verbraucherrechten in bezug auf den E-Commerce.

Auch die Konferenz von Venedig befasste sich in erster Linie mit dem Schutz der Freiheit der Bürger angesichts der rasanten Weiterentwicklung der neuen Technologien. An rechtlichen Themen wurden u. a. Vertragslösungen im grenzüberschreitenden Datenverkehr und Probleme des Umgangs mit personenbezogenen Daten durch die Medien behandelt, während sich die technikorientierten Fragen insbesondere auf die Kosten eines guten Datenschutzes und mögliche Lösungen durch geeignete Software sowie auf den Gebrauch von Chipkarten im Zusammenhang mit zentralisierten Datenbanken konzentrierten. Ich habe zu dem Thema „Neue Herausforderungen“ Probleme der Videoüberwachung, der Chipkarten und des Arbeitnehmerdatenschutzes aufgegriffen und – vor dem Hintergrund der Gesundheitsreform 2000 in Deutschland – die Möglichkeiten der Datensparsamkeit bis hin zur Datenvermeidung durch Anonymisierung und Pseudonymisierung seitens der Krankenkassen deutlich gemacht. Außerdem habe ich auf die weltweiten Lauschaktivitäten des amerikanischen Geheimdienstes National Security Agency (NSA) mit Hilfe des globalen Abhörnetzwerks ECHELON aufmerksam gemacht und in diesem Zusammenhang Regelungen gefordert, die festlegen, was die Nachrichtendienste dürfen und mit welchen Mitteln sie welche Informationen zu welchen Zwecken erheben und verarbeiten (s. o. Nr. 16.4).

Die Konferenz verabschiedete eine Erklärung (s. **Anlage 4**), die angesichts der Zunahme des weltweiten Datenaustauschs durch immer mehr Lebensbereiche erfassende Verarbeitungstechnologien zur Bekräftigung der Einhaltung der allgemeinen Datenschutzprinzipien aufruft, wobei sie insbesondere die Grundsätze der Zweckbindung, der Transparenz der Datenverarbeitung, der Betroffenenrechte und der Einrichtung unabhängiger Datenschutzkontrollinstanzen anspricht. Ziel der Deklaration ist, Überlegungen und ersten Ansätzen zu einer Neudefinition des Datenschutzes entgegenzuwirken, die seine in der Vergangenheit bewährten Instrumente und Schutzmechanismen in Frage stellen wollen.

33 Aus meiner Dienststelle

33.1 Der Datenschutzbeauftragte im Internet

Seit Februar 1999 ist meine Dienststelle mit einem eigenem Angebot im Internet vertreten. Die Homepage meiner Dienstelle (s. Abb. 7) ist unter der Adresse erreichbar.

Im Herbst 2000 hatte ich für zehn Monate ein „Forum des BfD zur EG-Telekommunikations-Datenschutzrichtlinie“ eingerichtet (s. o. Nr. 10.1.1).

Seit der Einrichtung der Homepage im Februar 1999 konnte ich ca. 1,8 Mio. Seitenanfragen verzeichnen. Das entspricht im Durchschnitt etwa 2 600 Seitenanfragen pro Tag. Dabei entwickeln sich die Zugriffszahlen zu meiner Freude kontinuierlich nach oben (s. Abb. 8).

Die meisten Zugriffe entfielen mit ca. 75 % auf die Rubrik „Materialien zum Datenschutz“, die u. a. meinen 16. und 17. Tätigkeitsbericht sowie meine Informationsbroschüren „BfD-Info 1 bis 5“ enthält, aber auch Entschließungen der Datenschutzkonferenzen sowie einschlägige Gesetze und Verordnungen. Anfragen erreichen uns aus allen Ländern der Erde. An der Spitze liegen mit einer Quote von ca. 76 % Anfragen aus Deutschland, gefolgt vom Vereinigten Königreich, Schweiz, Österreich und Niederlande. Aber auch Internetuser von Trinidad/Tobago, Bahamas, Mauritius und Brunei nutzen das Informationsangebot.

Mein Angebot ist auf einem Server beim Competence Center Informationsverbund Berlin-Bonn (CC IVBB) eingerichtet. Das CC betreibt auch eine zentrale Firewall für den Internetzugang aller obersten Bundesbehörden sowie Server für das Intranet-Angebot des Bundes im IVBB (vgl. 17. TB. Nr. 33.2.

33.2 Beteiligung am „Virtuellen Datenschutzbüro“ der Datenschutzbeauftragten

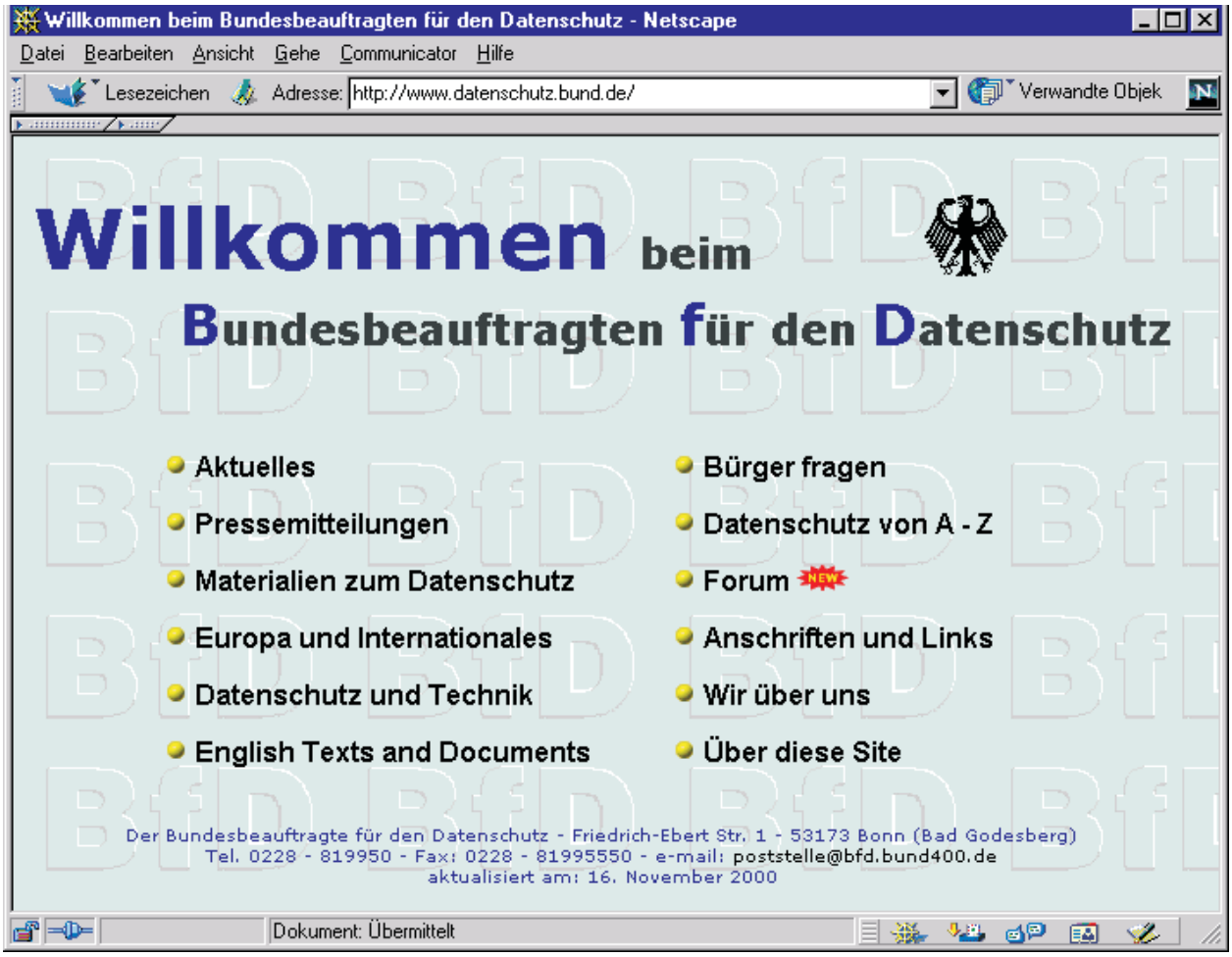
Am 5. Dezember 2000 hat das Virtuelle Datenschutzbüro seinen Betrieb im Internet aufgenommen. Die Idee hierfür wie auch der Aufbau und die momentane Geschäftsführung des Virtuellen Datenschutzbüros sind dem Landesdatenschutzbeauftragten von Schleswig-Holstein zu verdanken. Diese neue Einrichtung bietet unter der Internet-Adresse

- Informationen zu allen Fragen rund um den Datenschutz,
- Diskussionsforen zu aktuellen Datenschutzthemen,
- Antworten zu den häufigsten Fragen von Anwendern

  und
- eine Plattform für die Zusammenarbeit der Datenschützer weltweit.

Das Virtuelle Datenschutzbüro ist Portal und Ansprechstelle im Internet für alle – Bürgerinnen und Bürger, Experten und Datenschutzinstitutionen. Dieser Service wird zur Zeit von folgenden Projektpartnern getragen: Datenschutzbeauftragte des Bundes und der meisten Länder, der Norddeutschen Bistümer der Katholischen Kirche und Datenschutzbeauftragte aus der Schweiz, den Niederlanden und Kanada.

Abbildung 7 (zu Nr. 33.1)



Mit dem Konzept des Virtuellen Datenschutzbüros rücken die Datenschutzbeauftragten noch enger zusammen, zum Vorteil aller. Die wichtigsten Vorteile des Virtuellen Datenschutzbüros sind:

1. Transparenz im Datenschutzbüro

   Das Virtuelle Datenschutzbüro steht für Offenheit der Konzepte, offene Diskussionen und umfassende Informationsangebote. Auch durch den Einsatz von Open-Source-Software (s. o. Nr. 8.8), die ihre Vertrauenswürdigkeit unter Beweis stellt, indem ihr Quellcode offengelegt und damit für jeden einsehbar wird, wird Offenheit praktisch demonstriert.

2. Privacy-Enhancing Technologies

   Im Virtuellen Datenschutzbüro sollen sich auch Teams zusammenfinden, die gemeinsam neue datenschutzfördernde Techniken (Privacy-Enhancing Technologies) für Nutzerinnen und Nutzer fördern und entwickeln. Jede(r) ist eingeladen, dabei mitzuwirken. Durch die offene Gestaltung können nicht nur professionelle Datenschützer, sondern auch alle Experten, interessierte „Freaks“ oder Privacy-Aktivisten mit ihren Kenntnissen das Virtuelle Datenschutzbüro mitgestalten.

3. Technologie des Internets

   Durch die weltweite Vernetzung ist das Global Village zur Realität geworden; Datensicherheit und Datenschutz werden damit zu einer weltweiten Angelegenheit. Die beteiligten Datenschutzinstitutionen betrachten das Virtuelle Datenschutzbüro als ihre Antwort auf die Herausforderungen für die Privatsphäre, die das grenzüberschreitende Internet mit sich bringt. Es klingt trivial, aber im „Global Village“ muss der Datenschutz auch global und mit der adäquaten Technologie des Internets angegangen werden. Besonders zu diesen Themen wird das Virtuelle Datenschutzbüro praktische Hilfestellungen geben.

Zugleich wird erwartet, dass die Projektpartner mit der Kooperation im Virtuellen Datenschutzbüro durch Arbeitsteilung, Spezialisierung und systematische Bündelung ihrer Ressourcen ihre Effizienz steigern. Mit Beginn des Wirkbetriebs sind die bislang noch nicht am Projekt beteiligten Datenschutzbeauftragten in Europa und in aller Welt zur Mitarbeit eingeladen – eine wichtige Auf-

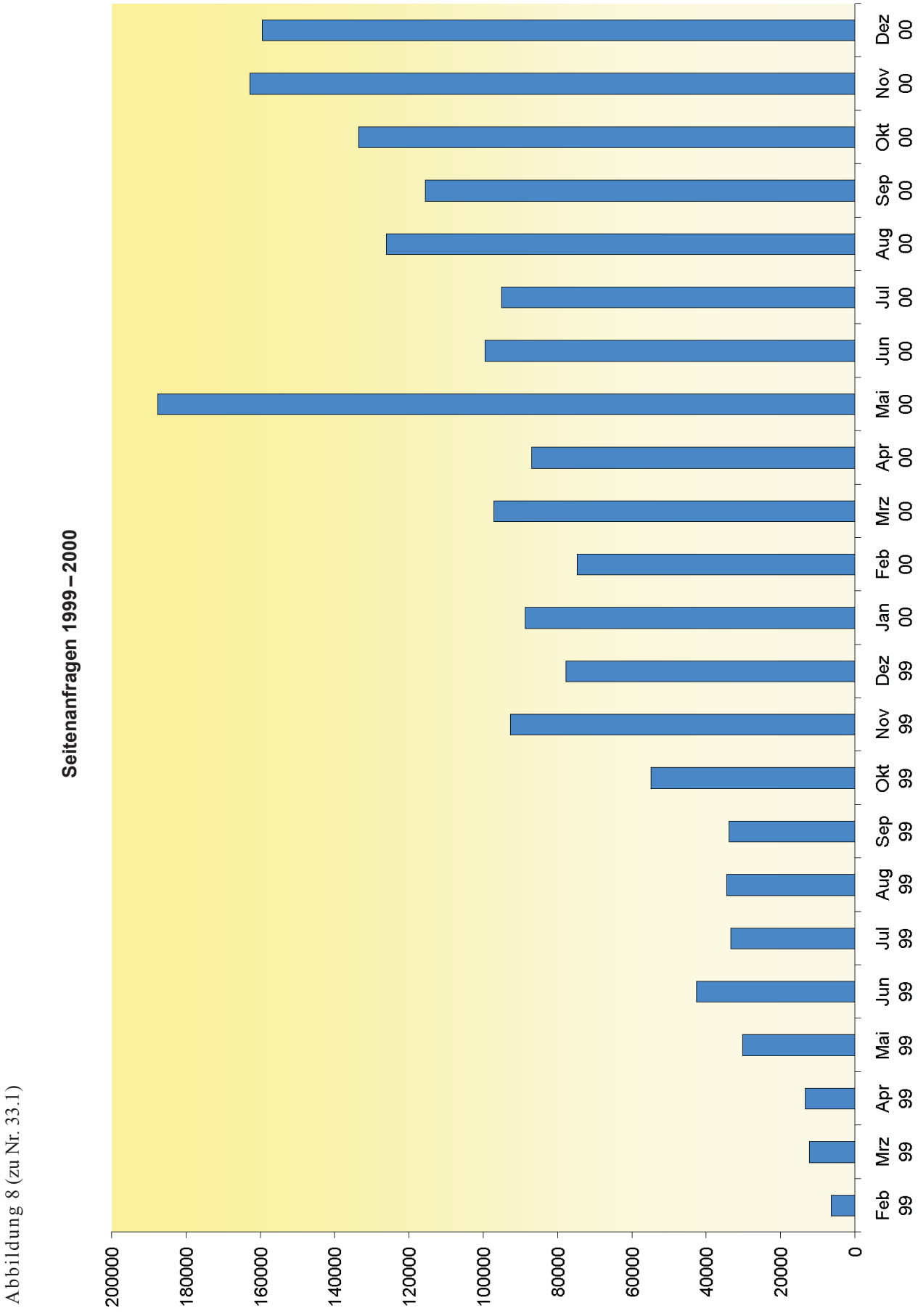


Abbildung 8 (zu Nr. 33.1)

gabe von uns allen zum Schutze jedes Einzelnen, denn im globalen Informationszeitalter hat der Schutz des Persönlichkeitsrechts eines jeden Einzelnen eine neue tragende Bedeutung.

Im Virtuellen Datenschutzbüro sind Teile meines Internetangebotes, wie Informationen zum Datenschutz auf europäischer Ebene, Rechtsgrundlagen des Bundes, Bürgerfragen, Tätigkeitsberichte, Bürgerbroschüren oder aktuelle Mitteilungen verfügbar. Auch bei der Moderation von Themen, wie beispielsweise zum Datenschutz in der Europäischen Union, zur Telekommunikation, Tele- und Mediendiensten, Chipkarten oder Firewalls beteiligt sich meine Dienststelle.

33.3 Berlin und Bonn: IT überbrückt die Entfernung

33.3.1 Einander näher sein mit Videokonferenzen

Die Aufteilung der Regierungsarbeit zwischen Berlin und Bonn wird in meiner Dienststelle durch den Einsatz innovativer Kommunikationstechnik unterstützt. So kommt im Rahmen des IVBB (Informationsverbund Berlin-Bonn) seit 1999 eine Videokonferenzanlage zum Einsatz (s. Abb. 9).

Ein für zehn Personen ausgelegter Videokonferenzraum ist mit einem Gruppenvideokonferenzsystem, bestehend aus

– 27“-TV-Monitor,

– schwenkbarer, fernsteuerbarer Farbkamera,

– PC-basierter Video-Einheit,

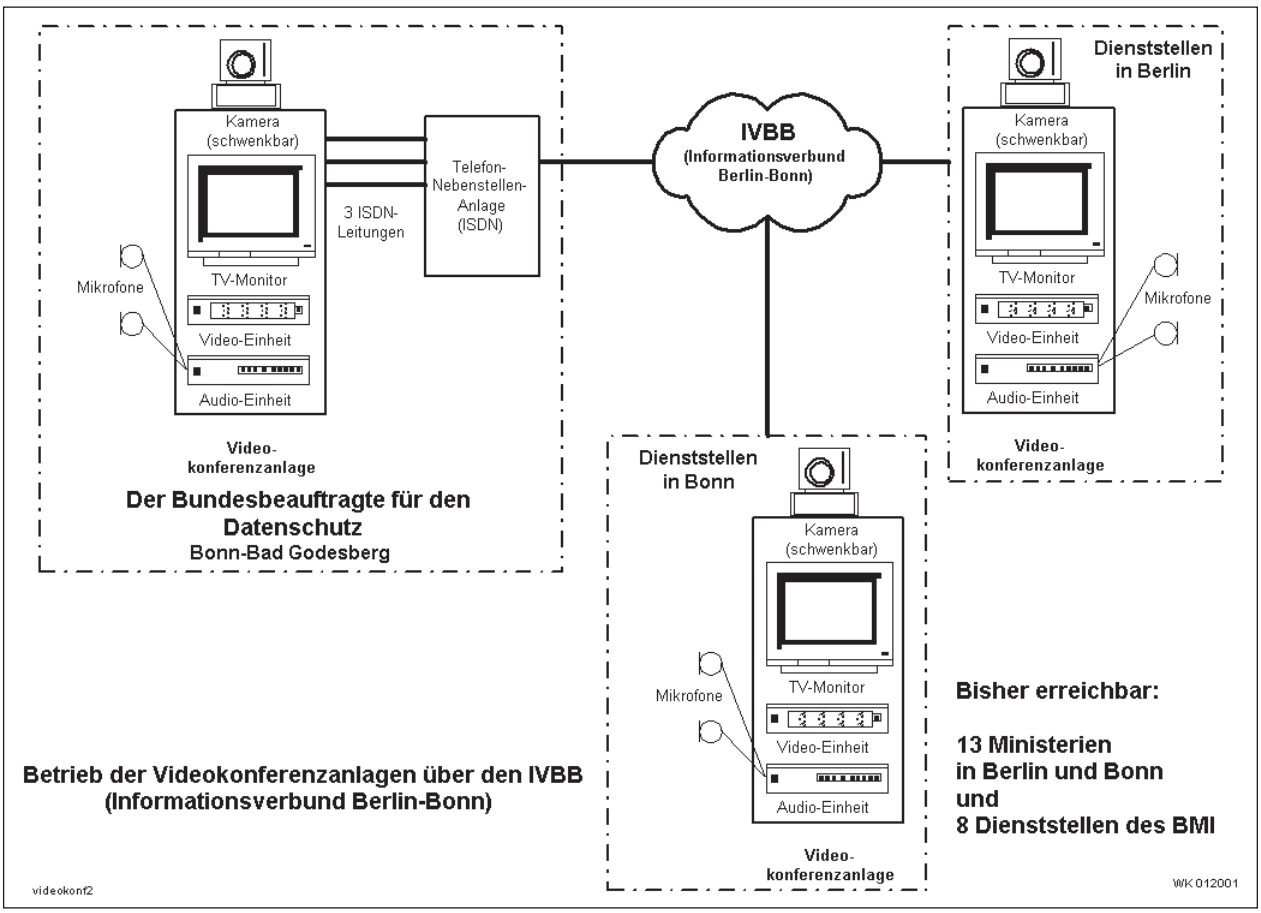
– Audio-Einheit und

– Tischmikrofonen

ausgestattet und kann von jedem Mitarbeiter genutzt werden.

Die Verbindung zu den Konferenzpartnern über drei gebündelte ISDN-Leitungen erfolgt über meine Telefonanlage. Sind die Teilnehmer über den IVBB zu erreichen, entstehen keine Verbindungskosten. Für die Kommunikation innerhalb und außerhalb des IVBB werden standardisierte Protokolle (H.320 (ISDN) und H.323 (IP-LAN)) genutzt. Aus Sicherheitsgründen ist diese Anlage nicht mit meinem PC-Netz verbunden; für den Dokumentenaustausch soll deshalb zukünftig eine Dokumentenkamera eingesetzt werden.

Abbildung 9 (zu Nr. 33.3.1)



Durch die Kanalbündelung ist eine qualitativ hochwertige Video- und Audioübertragung möglich. Über einen bei der Koordinierungs- und Beratungsstelle für den Einsatz der Informationstechnik der Bundesregierung (KBSt) zentral geführten Verteiler sind z. Z. 13 Ministerien in Berlin und Bonn sowie acht nachgeordnete Dienststellen des Bundesministerium des Innern erreichbar, was zu Zeitersparnissen durch die Einschränkung von Dienstreisen führt. Nach der geplanten Einbindung des Bundestages kann auch die Kommunikation mit den Ausschüssen durch diese Technik wirkungsvoll unterstützt werden.

33.3.2 Dem Parlament bei der Plenararbeit zusehen

Mit dem Umzug des Bundestages nach Berlin wurde das bisherige, auf Basis analoger Breitbandkabel betriebene Parlamentsfernsehen-Ressortnetz durch ein digitales System mit neuer Qualität abgelöst. Wie im Konzept des Informationsverbundes Berlin-Bonn (IVBB) vorgesehen, wird für die digitale Übertragung eine kryptierte Satelliten-Strecke (IntelSat 7) zur Verteilung der Audio- und Videodaten des „Parlamentsfernsehens“ in Berlin und Bonn genutzt. Im Rahmen dieses Projektes wurde auch meine Dienststelle mit den notwendigen Empfangsgeräten ausgestattet.

Folgende Kanäle können empfangen werden:

a. Bundestag:
Aus dem Reichstagsgebäude in Berlin werden alle Sitzungen des Deutschen Bundestages übertragen. In der sitzungsfreien Zeit werden Programminformationen eingeblendet.

b. Bundesrat:
Hier wird nur während der Sitzungszeit übertragen.

c. Bundespressekonferenz
Dieser Kanal überträgt Pressekonferenzen der Bundespressekonferenz Bonn bzw. Berlin e.V.

d. MAZ-Kanal
Auf diesem Kanal werden vom BPA Aufzeichnungen eingespielt, die von einzelnen Nutzern des IVBB liegenschaftsbezogen angefordert werden können. Durch ein spezielles Verschlüsselungsverfahren wird sichergestellt, dass angeforderte Aufzeichnungen nur in den gewünschten Liegenschaften empfangen werden können. Dieser Kanal kann auch wahlweise zur Einspeisung von lokalen MAZ-Aufzeichnungen über einen Video-Recorder genutzt werden.

e. Kanzleramt
Bis zur Fertigstellung des neuen Kanzleramtes im Berliner Spreebogen wird lediglich ein Tonsignal ausgestrahlt. Es sollen Pressekonferenzen und Erklärungen, die z. B. im Rahmen von Staatsbesuchen abgegeben werden, übertragen werden.

33.4 Das „noch-nicht-ganz-papierarme“ Büro

33.4.1 Einführung von elektronischen Akten auch beim BfD

Die öffentliche Verwaltung steht – wie die Wirtschaft – zunehmend unter Kosten- und Leistungsdruck. Zugleich gilt es, in einem permanenten Prozess Potenziale, Ressourcen und Motivation der Angehörigen im Bereich der öffentlichen Verwaltung zu fördern und zu nutzen. Wesentliches Ziel ist die Steigerung der Effizienz des Verwaltungshandelns. Eine bedeutende Rolle bei der Effizienzsteigerung kommt der Informations- und Kommunikationstechnik zu. Die rasanten Entwicklungen in diesem Bereich hin zu immer komplexeren, aber auch bedienungsfreundlicheren Anwendungen wirken mittlerweile wie ein Motor für die Veränderung, Anpassung und Erleichterung vielfältigster Arbeitsabläufe.

Besonders betroffen ist hiervon einer der Kernbereiche öffentlichen Verwaltungshandelns: der Umgang mit Papier. Geradezu geprägt von diesem Medium wendet die Verwaltung einen erheblichen Teil ihrer Ressourcen auf, Dokumente entgegenzunehmen, zu erfassen, zu erstellen, zu bearbeiten, weiterzuleiten, abzusenden und zu archivieren. Diese Arbeitsvorgänge erfordern Zeit und Aufwand; Güter, die die Verwaltung mit dem Ziel der Effizienzsteigerung vor Augen kritisch betrachten und optimieren muss. Vor diesem Hintergrund werden erhebliche Rationalisierungspotenziale erwartet, wenn herkömmliche papierbezogene Verfahren durch elektronische Verfahren abgelöst werden. Die damit verbundene Änderung der Arbeitsweisen und Regelwerke wird langfristig zu einschneidenden Veränderungen in der öffentlichen Verwaltung führen. Nach meiner Überzeugung ist die Arbeit mit elektronischen Akten mittelfristig unvermeidbar und die flächendeckende Einführung in der öffentlichen Verwaltung somit nur noch eine Frage der Zeit.

Bereits mit Kabinettsbeschluß vom 7. Februar 1996 zur „Verringerung und Straffung der Bundesbehörden“ wurde eine Standardisierung der IT-Verfahren in den Bereichen Organisation und Personal angestrebt. Eine wesentliche konzeptionelle Grundidee ist dabei die ganzheitliche IT-Unterstützung des Geschäftsganges. Das BMI, verfahrensverantwortliches Ressort für die Verwaltungsorganisation, hat sich mit zwei Projekten auseinander gesetzt, um diese Rationalisierungspotenziale abzuklären. Im zweiten Halbjahr 1999 hat das BMI im Rahmen des Pilotprojektes „Papierarmes Büro (PARO)“ nach dem „Einer-für-alle-Prinzip“ verschiedene, auf die Anforderungen der öffentlichen Verwaltung ausgerichtete Workflow- und Dokumentenmanagementsysteme getestet und auf ihre Einsatztauglichkeit im Bereich der öffentlichen Verwaltung untersucht. An diesem Pilotprojekt war auch mein Haus beteiligt.

Im Ergebnis erwies sich das in meinem Hause getestete Produkt für die Arbeit mit den für die planende und aus-

führende Verwaltung typischen Vorgängen als geeignet. Einer Beibehaltung dieses Produktes zur dauerhaften Nutzung steht somit nichts entgegen; nach entsprechenden Vorbereitungsarbeiten im Verlauf des Jahres 2000 soll mit der flächendeckenden Einführung in 2001 begonnen werden.

Die Einführung eines Vorgangsbearbeitungssystems in seiner vollen Ausprägung stellt aber wegen der zwangsläufigen Auswirkungen auf bisher gewohnte Arbeitsweisen für alle Beteiligten eine enorme Herausforderung dar. Diese Erkenntnis hat mich bewogen, eine Entscheidung zugunsten einer stufenweisen Einführung zu treffen. Zur Gewährleistung einer akzeptanzfördernden Arbeitsweise wird das System entsprechend dem DOMEA-Stufenkonzept zunächst als Elektronische Aktenablage genutzt, erst zu einem späteren Zeitpunkt werden die Arbeitseinheiten sukzessive auf das Arbeiten mit dem Vorgangsbearbeitungssystem umgestellt. Diese Vorgehensweise bietet den wesentlichen Vorteil, dass für alle Arbeitsbereiche vorerst weiterhin die gewohnte papiergebundene Bearbeitung erhalten bleibt; daneben wird aber der Aufbau der Elektronischen Aktenablage mit der Möglichkeit betrieben, von allen Arbeitsplätzen des Hauses auf alle aktenrelevante Dokumente zuzugreifen. Hierdurch wird die Informationsgewinnung durch den Bearbeiter deutlich verbessert und zugleich werden die Registratoren bei der Informationsbeschaffung und -aufbereitung entlastet. Die vorläufige Nutzung des Systems als Elektronische Aktenablage soll den Mitarbeitern den späteren Wechsel in die Elektronische Vorgangsbearbeitung erleichtern. Schliesslich sollen die mit der praktischen Nutzung gewonnenen Erkenntnisse und Erfahrungen den „sanften“ Übergang von der papiergebundenen zur elektronischen Akten- und Vorgangsbearbeitung vorbereiten.

Die datenschutzrechtliche Bedeutung der automatisierten Vorgangsbearbeitungssysteme hängt vor allem damit zusammen, dass die elektronische Akte – so wie die auf Papier – jeden Beitrag eines Bearbeiters ausweist; nur das ist nach beinahe beliebigen Kriterien auswertbar. Die elektronische Akte ist deshalb zu einer weitgehenden lückenlosen Leistungskontrolle geeignet, die weit über das hinausgeht, was rechtlich und auch unter dem Aspekt moderner Personalführung akzeptabel ist. Ein solches System kann nur eingeführt werden, wenn der Personal- bzw. Betriebsrat zugestimmt hat. In den zu treffenden Vereinbarungen ist präzise festzulegen, wie mit diesen Daten und mit den Daten aus eventuellen Protokollierungen einzelner Arbeitsschritte umzugehen ist. Zur Wahrung der berechtigten Interessen meiner Mitarbeiter und Mitarbeiterinnen habe ich dafür Sorge getragen, dass der Personalrat frühzeitig in das Vorhaben einbezogen wurde.

33.4.2 Elektronische Korrespondenz nimmt zu: „Dienstanweisung E-Mail“

Die Verbreitung der Informationstechnik im beruflichen wie im privaten Leben und die Möglichkeiten der elektronischen Datenübermittlung haben auch für die Korrespondenz Zeichen gesetzt. Zwar liegt der Schwerpunkt der Korrespondenz auch in meiner Dienststelle noch immer bei der „guten alten“ Briefpost und beim Fax, der Trend geht heute aber unübersehbar zum elektronischen Dokumentenaustausch (E-Mail). Nicht allein aus wirtschaftlichen Überlegungen, sondern auch weil E-Mail die Übermittlung und weitere Bearbeitung von Dokumenten vereinfacht sowie die kurzen Laufzeiten der Nachrichten die Arbeit effektiver machen, setze auch ich immer stärker auf E-Mail (derzeit ca. 4 000 E-Mail-Eingänge pro Monat). Dies gilt für die Kommunikation innerhalb der Dienststelle, aber auch mit externen Kommunikationspartnern, wie beispielsweise Bundesbehörden, den Landesbeauftragten für den Datenschutz oder Petenten.

Damit aber kein „Durcheinander“ bei der Handhabung der unterschiedlichen Verfahren (Briefpost, Fax, E-Mail) entsteht, habe ich für mein Haus eine Dienstanweisung E-Mail erlassen, die den Umgang und den Geschäftsgang innerhalb meiner Dienststelle regelt (s. **Anlage 28**). Der „Dienstanweisung E-Mail“ hat die Personalvertretung zugestimmt. Sie wird auch in Zukunft immer wieder überarbeitet werden müssen, weil technische Entwicklungen, aber auch praktische Erfordernisse dies notwendig machen.

33.5 Neues von SPHINX – Ausstattung im Hause –

Die Sicherheit der Vorgänge im elektronischen Rechts- und Geschäftsverkehr ist eine wichtige Voraussetzung für die erfolgreiche Weiterentwicklung unserer Informationsgesellschaft. Problematisch ist in diesem Zusammenhang die Vertraulichkeit einer Kommunikationsverbindung zu gewährleisten und die Kommunikationspartner sicher zu authentifizieren.

Die rechtliche Voraussetzung hierfür ist das Signaturgesetz (SigG), in Kraft getreten am 1. August 1997, das gerade aufgrund der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 überarbeitet wird. Es fehlt in der Praxis aber noch an nutzerfreundlicher Technik und an der Infrastruktur, die zum alltäglichen Gebrauch elektronischer Signaturen gehört. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit seinem Pilotversuch „SPHINX – sichere E-Mail“ dieses Anliegen aufgegriffen (s. 17. TB Nr. 8.8). In dem bundesweit betriebenen Projekt werden bei unterschiedlichen Behörden und Unternehmen verschiedene Produkte im Projekt SPHINX eingesetzt, die auf Basis internationaler Standards die verschlüsselte und signierte Übertragung von Dokumenten über das Internet ermöglichen. Projektziel der Stufen 1 und 2 war die flächendeckende Einführung einer Ende-zu-Ende-Verschlüsselung einschließlich der Nutzung der digitalen Signatur für elektronische Post (E-Mail). Hierzu wurden Erfahrungen gesammelt, ausgewertet und bei Bedarf direkt in geeignete technische oder organisatorische Änderungen umgesetzt. Zum Abschluss seiner dritten und letzten Stufe hat

das Projekt dann das Ziel erreicht, interoperable Technologien für Verschlüsselung und digitale Signatur in heterogenen Umgebungen bereit zu stellen.

Im Nachfolgeprojekt SPHINX-PKI wird bereits am Aufbau der für Signatur und Verschlüsselung erforderlichen Public-Key-Infrastruktur (PKI) gearbeitet. SPHINX ist mit dem SigG konform, doch werden z. Zt. noch keine qualifizierten Signaturen unterstützt. Das BSI forciert die Weiterentwicklung hin zur Unterstützung dieser Signaturen. Informationen hierzu enthält das Internetangebot des BSI unter der Adresse http://www.bsi.bund.de/aufgaben/projekte/sphinx.

Seit dem Herbst 2000 beteilige ich mich am Pilotprojekt. Die in meiner Dienststelle installierte Softwarelösung bietet auch die Möglichkeit, Smartcard-Terminals und Chipkarten einzusetzen. Mit der Verfügbarkeit qualifizierter Signaturen nach dem SigG beabsichtige ich, die Chipkartentechnik zur Speicherung der persönlichen Sicherheitsumgebung einzuführen.

33.6 Die Informationstechnik in meiner Dienststelle

Eine effiziente und wirtschaftliche Aufgabenerfüllung ist heute ohne IT-Einsatz nicht mehr denkbar. Auch meine vielfältigen Kommunikationsbeziehungen zu den Behörden und Wirtschaftsunternehmen meines Zuständigkeitsbereiches machen eine sachgerechte, zeitgemäße IT-Ausstattung unerlässlich. Auch teilen mir mittlerweile viele Bürger ihre Sorgen und Beschwerden „elektronisch" – z. B. per E-Mail – mit. Ich bin daher ständig bemüht, die IT- und TK-Systeme meiner Dienststelle der Entwicklung anzupassen.

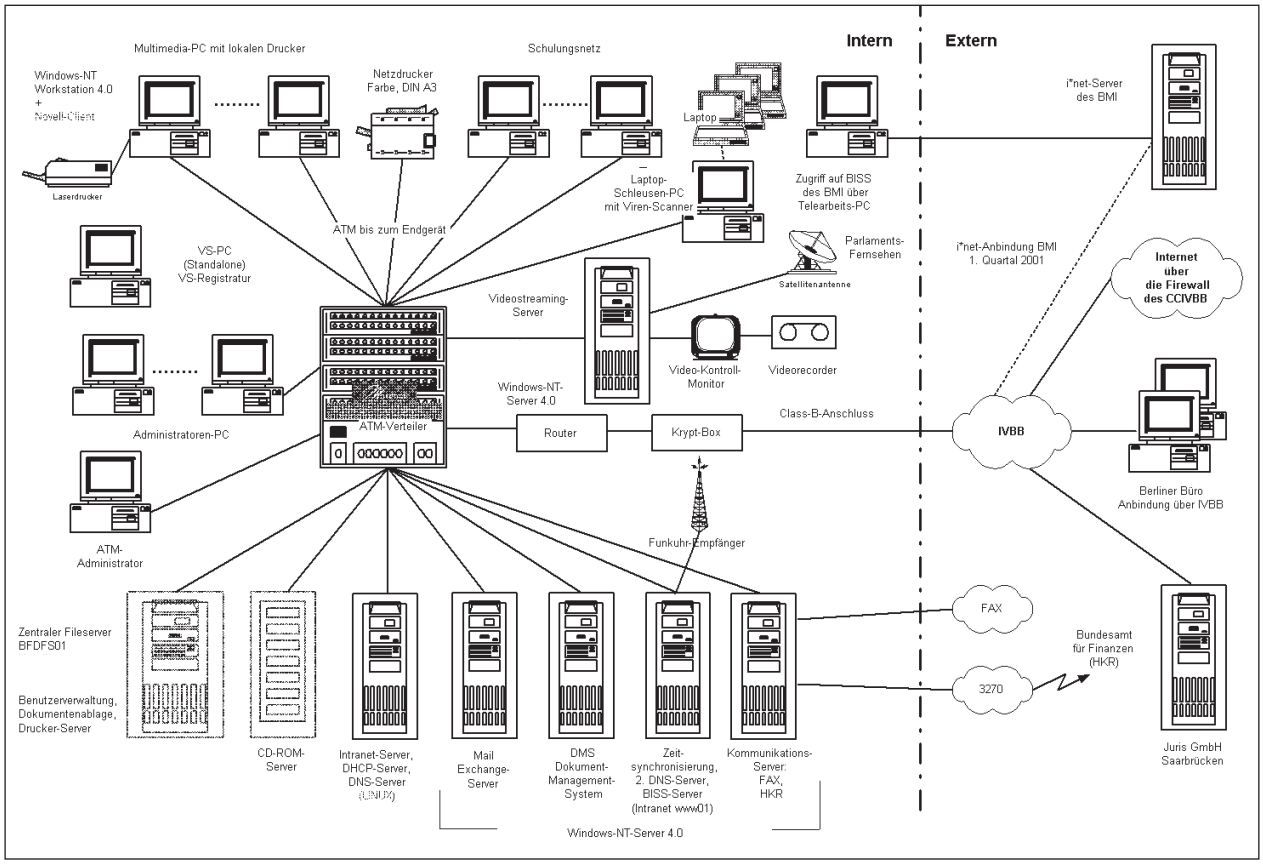
In den vergangenen Jahren wurde die Ausstattung meiner Dienststelle mit informationstechnischen Geräten weiter verbessert. So verfügen jetzt alle Mitarbeiter über einen PC (Pentium II/III Prozessoren, 128 MB RAM) mit einem Laserdrucker (Ausstattungsgrad 100 %). Die PC und die acht zentralen Server sind alle an einem LAN (Local Area Network) angeschlossen. Dieses Netz hat über den IVBB (s. o. Nr. 33.1) auch Zugang zum Internet und weiteren Diensten (s. Abb. 10).

Im Zuge der Modernisierung wurden alle PC auf das Betriebssystem Windows-NT-Workstation umgestellt. Die Sicherheitsmechanismen dieses Betriebssystems werden durch zusätzliche Sicherheitsmaßnahmen, wie z. B. Kartenleser in der PC-Tastatur, worüber sich der Mitarbeiter gegenüber „seinem PC" identifiziert, unterstützt.

Als Bürokommunikationssoftware wird einheitlich das Büro-Software-Paket „MS-Office" mit Textverarbei-

Abbildung 10 (zu Nr. 33.6)

Die IT-Konfiguration meiner Dienststelle



tung, Tabellenkalkulation, Geschäftsgrafikprogramm und elektronischer Post eingesetzt. So sind meine Mitarbeiter und ich weltweit unter der E-Mail-Kennung **poststelle@bfd.bund400.de** erreichbar.

Alle PC sind sternförmig über ein **ATM-Netz** (Asynchronous Tranfer Mode) mit dem zentralen Fileserver verbunden. Diese sternförmige Vernetzung mit verbindungsorientierte Technologie hat sich auch aus Sicht der IT-Sicherheit bewährt, da sich ein Fehler an einem PC nicht auf das ganze Netz auswirken kann. Das ATM-Netz erlaubt über Kupferkabel Übertragungsgeschwindigkeiten bis zu 155 Mbit/s.

Der zentrale **Fileserver** mit dem Betriebssystem „Novell NetWare 5“ verwaltet den Zugang zum **LAN** und speichert die von den Nutzern erstellten und bearbeiteten Dokumente. Neben dem eigentlichen File- und Anmeldeserver sind zusätzlich noch sieben Dienstleistungs-Server installiert: Ein Server mit **DNS** (Domain Name Service) und DHCP (Dynamic Host Configuration Protocol) verwaltet Namen und IP-Nummern der PC in meinem Netzwerk. Dieser Server läuft unter dem Betriebsystem LINUX und ist auch die Plattform für mein hausinternes Informationssystem auf Basis eines Intranet (s. auch Nr. 8.8). Ein weitere Server dient als DNS-Ausfallserver. Er enthält das bisherige BMI-Informationssystem (BISS) und ist Zeitsynchronisierungs-Server für mein LAN. Der **Mail-Server** realisiert den Mail-Zugang zum IVBB und in das Internet. Im **CD-ROM-Server** mit acht CD-ROM-Laufwerken werden allen PC-Benutzern zentrale Informationsangebote zur Verfügung gestellt, wie z. B. die Gesetzessammlungen „Schönfelder“ und „Satorius“ oder das „Bundesgesetzblatt“. Der Server für das **Dokument-Management-System** unterstützt im Rahmen des Pilotprojektes „Papierarmes Büro“ meine Registratur und die beteiligten Mitarbeiter. Da sich diese Lösung bewährt hat, wird im Jahr 2001 der Ausbau elektronischer Akten verstärkt werden (s. o. Nr. 33.4.1).

Der **Kommunikations-Server** ermöglicht das Versenden von Dokumenten als FAX vom PC aus. Gleichzeitig wird über diesen Server der Zugang (3270-Emulation) meiner Dienststelle zum Bundesamt für Finanzen realisiert. Der **Video-Server** verteilt das über Satellitenschüssel empfangene Parlamentsfernsehen auf die PC (s. o. Nr. 33.3.2).

33.7 Sonstiges

Zwischen dem BMI und dem BfD besteht ein Personalverbund. Dieser führte im Berichtszeitraum durch den Umzug von Parlament und Teilen der Bundesregierung nach Berlin zu einer besonders starken Personalfluktuation, von der mehr als die Hälfte meiner Mitarbeiter betroffen waren. Angehörige meiner Dienststelle, die sich für eine Fortsetzung ihrer beruflichen Tätigkeit in Berlin entschieden, wechselten ins BMI, andere kamen im Gegenzug zum BfD und mussten in ihre neuen Aufgaben eingearbeitet werden.

Die durch den Aufgabenzuwachs meiner Dienststelle in den letzten Jahren bedingten personellen Verstärkungen machten den Umzug in eine größere Liegenschaft notwendig. Der Umzug in die Friedrich-Ebert-Straße in Bonn-Bad Godesberg konnte im September 1999 abgeschlossen werden.

In Berlin stehen meinen Mitarbeitern, die sich zur Beratung von Ausschüssen des Deutschen Bundestages dort aufhalten, im gemeinsamen Behördenhaus Bundesallee 216–218 Büroräume zur Verfügung, die durch moderne Informationstechnik mit der Dienststelle in Bonn verbunden sind.

Unverändert groß ist das Interesse an meinen Veröffentlichungen: Insgesamt wurden von Privatpersonen, Organisationen und Firmen annähernd 60 000 Publikationen pro Jahr angefordert und versandt.

34 Am Schluss noch einiges Wichtige aus zurückliegenden Tätigkeitsberichten

1. Über die Fertigstellung einer **„Machbarkeitsstudie zum Einsatz einer Smart-Card im Asylverfahren“** habe ich im 17. TB (Nr. 5.3) berichtet. Auf Beschluss der Innenministerkonferenz vom 18./19. November 1999 wurde inzwischen eine Bund-Länder-Arbeitsgruppe gebildet, die die Modalitäten eines Pilotversuchs erarbeiten soll. Neben dem Bund nehmen daran Vertreter der Länder Baden-Württemberg, Brandenburg, Bayern, Mecklenburg-Vorpommern, Niedersachsen und Nordrhein-Westfalen teil. Diese Länder haben sich grundsätzlich bereit erklärt, einen Pilotversuch durchzuführen, der jedoch noch nicht begonnen hat. Derzeit wird ein Stufenplan diskutiert, der vier Ausbaustufen vorsieht. Eine abschließende Meinungsbildung lag bei Redaktionsschluss noch nicht vor.

2. In meinem 17. TB (Nr. 5.4.4) habe ich über den **deutsch-türkischen Briefwechsel** berichtet. Wie ich anlässlich eines Kontrollbesuches erfahren habe, fanden im November 1999 Konsultationen zwischen Vertretern der beiden Innenministerien zu diesem Thema statt, die zum Ergebnis hatten, den Briefwechsel beizubehalten. Für die Anwendung dieses Verfahrens bestand von Ende 1998 bis Frühjahr 2000 kein Anlass. Danach sind zwei Anfragen gestellt worden. Im Zusammenhang mit dem Briefwechsel steht noch eine abschließende Stellungnahme des BMI zu der Frage aus, mit welcher Erforderlichkeit und für welchen Zeitraum auszugsweise Unterlagen aus diesen Verfahren aufbewahrt werden.

3. Über den **Einsatz ausländischen Liaisonpersonals im BAFl** habe ich in meinem 17. TB (Nr. 5.4.5.2) ausführlich berichtet und die damit verbundenen Probleme dargestellt. Die seinerzeit noch nicht vorliegende Stellungnahme des BMI ist mir in der Zwischenzeit zwar zugegangen, jedoch bestehen zwischen dem BMI und mir zur Frage der Anwend-

barkeit der Funktionsdoppelungstheorie auf das ausländische Liaisonpersonal nach wie vor unterschiedliche Auffassungen. Ich habe daher das BMI gebeten, diese Frage auch unter Einbeziehung der für das Dienstrecht zuständigen Fachabteilung nochmals zu prüfen. Da mir bei Redaktionsschluss die erbetene Stellungnahme noch nicht vorlag, werde ich erneut berichten.

4. In meinem 17. TB (Nr. 5.5) habe ich über den Entwurf eines Artikelgesetzes zur Änderung des AZR-Gesetzes und zur Einrichtung einer **Warndatei** berichtet und Kritik an einzelnen Vorschriften des geplanten Warndateigesetzes geübt. Der Gesetzentwurf wurde in der vergangenen Legislaturperiode nicht weiterverfolgt. In dieser Legislaturperiode hat die CDU/CSU-Fraktion einen Gesetzentwurf zur Änderung des Ausländerzentralregisters und zur Einrichtung einer Warndatei eingebracht, der am 11. Mai 2000 im Deutschen Bundestag abgelehnt worden ist.

5. Seit meinem 17. TB (Nr. 5.12) ist keine Änderung der rechtlichen Situation oder der Praxis zum Ablauf der Datenerhebung und Recherche im Zusammenhang mit der **Verleihung des Verdienstordens der Bundesrepublik Deutschland** eingetreten. Im Hinblick auf die Deregulierungsbestrebungen der Bundesregierung habe ich in der Zwischenzeit gegenüber dem BMI mein Verständnis signalisiert, in dieser Frage auf eine normative Regelung zu verzichten. Gleichzeitig habe ich jedoch klargestellt, dass es aus meiner Sicht erforderlich erscheint, zumindest eine abgestimmte und verbindliche Verfahrensregelung mit den Ländern zu treffen, um eine Datenbeschaffung auf Vorrat zu unterbinden. Die bisherige Verfahrensweise der parallelen Prüfung von „Verdiensten“ und „Würdigkeit“ führt nämlich unweigerlich zu Datensammlungen, die zunächst nicht benötigt werden. Es werden Daten zur Würdigkeit eines zur Ordensverleihung Vorgeschlagenen bis hin zu einer Abfrage bei der BStU gesammelt, ohne zu diesem Zeitpunkt zu wissen, ob dessen Verdienste den Anforderungen für die beabsichtigte Ehrung genügen. Das BMI hat mir inzwischen mitgeteilt, dass es in Absprache mit dem Bundespräsidialamt die Frage einer Systematisierung und Stufung der Prüfung aufgreifen will.

6. In meinem 17. TB (Nr. 7.4) habe ich nach dem damaligen Sachstand die Erwartung geäußert, dass die **Steuerdaten-Abruf-Verordnung** in absehbarer Zeit erlassen wird. Zu einem im September 1999 vorgelegten Entwurf habe ich dem BMF einige Änderungsvorschläge unterbreitet. Das BMF hat mir jedoch nunmehr mitgeteilt, dass aufgrund eingegangener Stellungnahmen der Länder und Gemeinden und insbesondere im Hinblick auf die unterschiedliche Handhabung der bisherigen Verwaltungsregelung zum Abruf der Steuerdaten in den Ländern eine erneute Überarbeitung des Entwurfs erforderlich sei. Ab Beginn des Jahres 2001 werde sich eine Arbeitsgruppe hiermit beschäftigen. Der Erlass der Steuerdaten-Abruf-Verordnung verzögert sich somit leider weiterhin.

7. In meinem 17. TB (Nr. 7.6.2) habe ich über Probleme berichtet, die sich aus der Umsetzung der „**Schwarze Liste-Verordnung**“ für Marktbeteiligte ergeben, auf die diese Verordnung (noch) nicht anzuwenden ist, weil zwar Unregelmäßigkeiten festgestellt wurden, diese aber den Schwellenwert von 100 000 EURO zumindest zunächst nicht überschreiten. Die datenverarbeitungstechnischen Probleme einer entsprechenden Datei sind mit dem BMF erörtert und überwiegend geklärt. Keine Einigung konnte jedoch bisher in der Frage erzielt werden, ob ein direkter Zugriff auf die Daten dieser Marktbeteiligten auch notwendig ist, solange diese nicht wegen Erreichens des Schwellenwertes in die „Schwarze Liste“ übernommen worden sind. Die vom BMF vorgetragenen Gründe sind weiterhin nicht überzeugend. Die Erörterung mit dem BMF wird fortgesetzt.

8. Die Privatsphäre – auch das Post-, Brief- und Fernmeldegeheimnis – lässt sich allein durch Rechtsvorschriften nicht ausreichend schützen. Daher habe ich wiederholt auf die Notwendigkeit hingewiesen, **Kryptographie** als „Schlüsseltechnik“ für die Informationstechnik einzusetzen (s. 17. TB Nr. 8.10).

   Damals musste befürchtet werden, dass auf Betreiben staatlicher Sicherheitsbehörden in Deutschland das Recht auf freie Verfügbarkeit von Verschlüsselungsprodukten eingeschränkt würde. Inzwischen hat die Bundesregierung jedoch mit dem **Eckpunktepapier vom 2. Juni 1999** dargelegt, dass auch künftig Verschlüsselungsverfahren und -produkte ohne Restriktion entwickelt, hergestellt, vermarktet und genutzt werden dürfen. Das Papier ist unter http://www.bmwi.de/Homepage/Presseforum/pressemitteilungen/1999/0602prm1.jsp nachzulesen.

   Das war ein erster Schritt in die richtige Richtung, der auch in einer Entschließung zu den Eckpunkten der deutschen Kryptopolitik auf der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 7./8. Oktober 1999 ausdrücklich begrüßt wurde (s. **Anlage 18**).

9. In meinem 17. TB (Nr. 10.1.5.3) habe ich über das **automatisierte Auskunftsverfahren nach § 90 TKG** berichtet und Bedenken gegen die zu weite Festlegung des Kreises der Verpflichteten geltend gemacht. Insbesondere habe ich kritisiert, dass nach dem Gesetzeswortlaut auch sämtliche Betreiber von **Corporate Networks** betroffen sind, zu denen u. a. Nebenstellenanlagen in Krankenhäusern und Betrieben zählen, soweit sie ihre Anschlüsse den Patienten bzw. Mitarbeitern für eine private Nutzung zur Verfügung stellen. Auf meinen Vorschlag, die Vorschrift des § 90 TKG insoweit einengend zu ändern, hatte mir das BMWi seinerzeit mitgeteilt, über die Einbezie-

hung von Nebenstellenanlagen könne erst entschieden werden, wenn ausreichende Erfahrungen über das neue Verfahren vorlägen.

Da das automatisierte Auskunftsverfahren von der RegTP bislang nur für Telekommunikationsdiensteanbieter, die ihre Leistungen der Öffentlichkeit gegenüber anbieten, aufgenommen worden ist (s. o. Nr. 10.3), war der Problematik zunächst die Dringlichkeit genommen. Erste Erfahrungen liegen nunmehr vor. Die Frage der Ausweitung des Verfahrens auch auf Nebenstellenanlagen drängt sich daher wieder auf und bedarf nunmehr einer Klärung. Ich werde dem BMWI meine unverändert fortbestehenden Bedenken erneut vortragen und auf eine rechtliche Klarstellung hinsichtlich des Kreises der Verpflichteten nach § 90 TKG hinwirken.

10. Würden die Strafverfolgungs- und Sicherheitsbehörden im Rahmen des automatisierten Auskunftsverfahrens nach § 90 TKG (vgl. Nr. 10.3) Anfragen mit unvollständigen Namens- bzw. Adressangaben sog. **Jokerabfragen** (vgl. 17. TB Nr. 10.1.5.3) stellen, müssten ihnen regelmäßig auch Daten Unbeteiligter bekannt gegeben werden. Da das Telekommunikationsgesetz solche uneindeutigen und nicht für die Aufgabenerledigung der Behörden erforderlichen Abfragen nicht zulässt, hat die RegTP diese Anfragen nicht in das Auskunftsverfahren nach § 90 TKG aufgenommen.

    Es wird jedoch die Ansicht vertreten, dass die Jokerabfrage ohne ausdrückliche gesetzliche Regelung möglich sein müsste. Diese Meinung teile ich nicht. Auch das BMJ rät weiterhin zu einer gesetzlichen Klarstellung. Das BMWi hat daher erfreulicherweise deutlich gemacht, dass eine Umsetzung dieser Abfragemöglichkeit erst erfolgen kann, wenn eine eindeutige Rechtsgrundlage in § 90 TKG geschaffen worden ist. Diese liegt bis heute nicht vor.

11. In meinem 17. TB (Nr. 10.1.6) hatte ich bereits darauf hingewiesen, dass ich eine konzeptionelle und inhaltliche Überarbeitung des **Kataloges für Sicherheitsanforderungen** nach § 87 TKG für notwendig erachte. Dabei handelt es sich um technische und organisatorische Vorgaben, die auch dem Schutz des Fernmeldegeheimnisses und personenbezogener Daten dienen. Diese sind von den Betreibern von Telekommunikationsanlagen in ein Sicherheitskonzept einzustellen und entsprechend zu realisieren. Wegen des von mir angemeldeten Änderungsbedarfs hat die RegTP in der Vergangenheit unter anderem darauf verwiesen, dass sie noch keine praktischen Erfahrungen in bezug auf die Umsetzung des Sicherheitskataloges durch die Telekommunikationsunternehmen habe sammeln können. Inzwischen wurden von der RegTP entsprechende Kontrollen bei Unternehmen durchgeführt. Dabei wurde u. a. festgestellt, dass die Sicherheitskonzepte oft nicht aktualisiert werden und dass die Unternehmen noch bezüglich der Maßnahmen zum Schutz des Fernmeldegeheimnisses und der personenbezogenen Daten sensibilisiert werden müssen.

    Ich werde mich weiterhin dafür einsetzen, dass der Katalog für Sicherheitsanforderungen überarbeitet und fortgeschrieben wird.

12. In meinem 17. TB (Nr. 20.4) habe ich berichtet, dass das **psychologische Gutachten** eines Petenten aus dem Jahre 1988, das längst hätte vernichtet sein müssen, weiterhin in der **Leistungsakte des** für ihn zuständigen **Arbeitsamts** aufbewahrt wurde und dass dieses darüber hinaus Mitte der neunziger Jahre eine Reha-Akte angelegt hatte, die mit diesem Gutachten begann. Beides hatte ich wegen Verstoßes gegen die §§ 67b Abs. 1, 67c Abs. 1 und 2 SGB X gegenüber der BA beanstandet und diese aufgefordert, das fragliche Gutachten und dessen Kopien zu vernichten. Die BA hat mir inzwischen mitgeteilt, dass das Arbeitsamt das Gutachten und die Kopien mittlerweile vernichtet hat.

13. In meinem 17. TB (Nr. 34, dort Nr. 9) habe ich berichtet, dass mir seit März 1999 ein vom BMF überarbeiteter Entwurf einer „ **Dienstanweisung für den Einsatz des IT-Verfahrens AVS – APC bei den Vollstreckungsstellen der Hauptzollämter**“ vorliegt. Hierzu habe ich gegenüber dem BMF geringfügige inhaltliche Änderungen angeregt. Da das IT – Verfahren AVS im Jahre 1999 zunächst auf Client/Server-Architektur und anschließend auf Windows NT umgestellt worden ist, muss nun der mir im März 1999 vom BMF übersandte Entwurf wieder entsprechend angepasst werden. Diese Überarbeitung durch das BMF war bei Redaktionsschluss noch nicht abgeschlossen.

14. Gegen Ende des Berichtszeitraums hat das BMVg einen Entwurf eines Zweiten **Gesetzes zur Neuordnung des Wehrdisziplinarrechts** in die parlamentarische Beratung eingebracht. Erfreulich war für mich, dass eine Reihe der von mir anlässlich von Truppenbesuchen gemachten Bedenken berücksichtigt wurden (vgl. auch 16. TB Nr. 26.2).

Dr. Joachim Jacob

Der Bundesbeauftragte für den Datenschutz

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:

Auswärtiger Ausschuss	2; 4; 32
Innenausschuss	2; 5; 6.1 bis 6.4; 8.1.2; 8.5; 8.9; 8.11; 9; 10.1.3; 10.2; 10.3; 10.4; 11; 12; 14; 15; 16; 17; 18; 28.1.1f; 28.5.3; 29.5; 30.1; 33.1; 33.3, 34 dort Nrn. 1 bis 5, 8 bis 11
Rechtsausschuss	2.7; 5.1.1; 5.2.3; 5.7; 5.10.1; 6; 8.6; 10.1.3; 10.2; 10.3; 10.4; 29.2.3; 29.5; 32; 34 dort Nrn. 8 bis 11
Finanzausschuss	7; 8.5; 9.2; 13
Haushaltsausschuss	8.6; 8.8; 33.3
Ausschuss für Wirtschaft und Technologie	2.7; 8.1.2; 8.3; 8.5; 8.6; 8.7; 8.9; 8.10; 10.1; 10.1.2; 10.1.3; 10.2; 10.3; 10.4; 17.1; 29.2; 29.3; 31.8; 33; 34 dort Nrn. 8 bis 11
Ausschuss für Arbeit und Sozialordnung	8.5; 8.6; 18.3; 19; 20; 22; 23
Verteidigungsausschuss	8.5; 8.6; 15; 26; 33.5
Ausschuss für Familie, Senioren, Frauen und Jugend	19; 24; 27
Ausschuss für Gesundheit	8.5; 9.1; 19; 21; 24; 25
Ausschuss für Verkehr, Bau- und Wohnungswesen	8.6; 28; 29.3
Ausschuss für Bildung, Forschung und Technikfolgenabschätzung	2.7; 8.5; 8.7; 8.9; 8.10; 8.11; 33; 34 dort Nr. 8
Ausschuss für die Angelegenheiten der Europäischen Union	2; 8.5; 11.9; 11.10; 32
Ausschuss für Kultur und Medien	8.9; 33.2; 33.3

Anlage 2 (zu Nr. 1.12)

Übersicht über die durchgeführten Kontrollen, Beratungen und Informationsbesuche

Bundeskanzleramt

- Beauftragter der Bundesregierung für Angelegenheiten der Kultur und der Medien
  Bundesarchiv
  Kunst- und Ausstellungshalle der Bundesrepublik Deutschland
- Bundesnachrichtendienst

Auswärtiges Amt

- 3 Botschaften
- 1 Ständige Vertretung
- 1 Generalkonsulat

Bundesministerium des Innern

- Statistisches Bundesamt
- Bundesamt für die Anerkennung ausländischer Flüchtlinge:
  Zentrale Nürnberg und 3 Außenstellen
- Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR:

  Zentrale und 2 Außenstellen
- Bundesverwaltungsamt
- Bundesgrenzschutz mit Grenzschutzdirektion, einem Grenzschutzpräsidium und mehreren Grenzschutzämtern
- Bundeskriminalamt
- Deutsche Verbindungsbeamte bei EUROPOL/EDS
- Bundesamt für Verfassungsschutz
- Bundeszentrale für politische Bildung
- Technisches Hilfswerk:

  Zentrale Bonn, 1 Landesverband und 1 Ortsverband

Bundesministerium der Justiz

- Generalbundesanwalt beim Bundesgerichtshof
- Bundeszentralregister
- Zentrales Staatsanwaltschaftliches Verfahrensregister
- Deutsches Patentamt

Bundesministerium der Finanzen

- Bundesamt für Finanzen
- 1 Bundesvermögensamt
- Zollkriminalamt
- 1 Hauptzollamt
- 1 Zollfahndungszweigstelle

Bundesministerium für Wirtschaft und Technologie

- Physikalisch-Technische Bundesanstalt

Bundesministerium für Arbeit und Soziales

- Hauptstelle und Zentralamt der Bundesanstalt für Arbeit
- 4 Arbeitsämter

Bundesministerium der Verteidigung

- Militärischer Abschirmdienst
- 1 Wehrbereichsverwaltung
- 1 Kreiswehrersatzamt
- Universität der Bundeswehr München
- 1 Bundeswehrkrankenhaus
- TK-Anlage eines Bundeswehrkrankenhauses

Bundesministerium für Gesundheit

- Robert-Koch-Institut

Bundesministerium für Verkehr, Bau- und Wohnungswesen

- Luftfahrt-Bundesamt
- Kraftfahrt-Bundesamt
- Bundesamt für Güterverkehr
- Wasser- und Schifffahrtsdirektion Ost

Presse- und Informationsamt der Bundesregierung

Deutsche Bundesbank

Deutsche Post AG

- Zentrale
- Frachtpostermittlungsstelle Bamberg
- 1 Frachtpostzentrum
- Niederlassung Postphilatelie Frankfurt

- Niederlassung Internationale Post Frankfurt
- 1 Postfiliale
- 1 Briefzentrum
- 1 Niederlassung Software-Entwicklung

Neue Postdienstunternehmen: 6

Telekommunikationsunternehmen: 11

Bundesversicherungsanstalt für Angestellte

- Hauptstelle
- 1 Auskunfts- und Beratungsstelle
- 1 Rehabilitationsklinik

Künstlersozialkasse

Deutsches Rotes Kreuz

- Suchdienst Hamburg
- Suchdienst München

Berufsgenossenschaften und Krankenkassen

- Hauptverband der gewerblichen Berufsgenossenschaften
- Großhandels- und Lagerei-Berufsgenossenschaft
- Holzberufsgenossenschaft – Hauptverwaltung
- Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege – 1 Bezirksverwaltung
- Barmer Ersatzkasse–Zentrale Wuppertal
- Deutsche Angestellten Krankenkasse – 2 Außenstellen

Sonstige

- Bundesdruckerei GmbH Berlin
- 2 Heimatortskarteien des kirchlichen Suchdienstes
- Stiftung für ehemalige politische Häftlinge
- Wirtschaftsunternehmen u. a. wegen Verfahren zur Sicherheitsüberprüfung
- 1 überregionales Corporate Network
- 1 lokales Corporate Network
- Vertragshändler für TK-Dienstleistungen

Anlage 3 (zu Nr. 1.12)

Übersicht über Beanstandungen nach § 25 BDSG

Auswärtiges Amt

- Verstoß gegen § 9 BDSG durch unzureichende Sicherungsmaßnahmen bei der Verarbeitung personenbezogener Daten durch eine Auslandsvertretung (s. Nr. 4.3.2).

Bundesministerium des Innern

- Verstoß des BAFl gegen § 9 sowie Anlage zu § 9 Satz 1 BDSG wegen Mängel im Bereich der Datensicherheit bei dem Personalaktengeheimnis unterliegenden Mitarbeitern (s. Nr. 18.6.2).
- Verstoß des BAFl gegen die Regelungen der §§ 90 ff BBG beim Umgang mit Personalaktendaten (s. Nr. 18.6.2).
- Verstoß des BGS gegen § 32 Abs. 3 i. V. m. § 33 Abs. 6 BGSG wegen unzulässiger Übermittlung personenbezogener Daten an eine öffentliche Stelle eines anderen Staates, wegen unterlassener Hinweise auf die zweckgebundene Verwendung personenbezogener Daten sowie auf den beim BGS vorgesehenen Löschungszeitpunkt anlässlich der Übermittlung personenbezogener Daten an eine öffentliche Stelle eines anderen Staates (s. Nr. 12.4).
- Verstoß des BGS gegen die Polizeidienstvorschrift (PDV) 384.1 wegen Ausschreibung zur Aufenthaltsermittlung in einem Verfahren nach dem Ordnungswidrigkeitsgesetz (s. Nr. 12.2.2).
- Verstoß des BGS gegen § 35 Abs. 2 Nr. 2 und Abs. 5 Satz 2 BGSG wegen unterlassener Löschung von beim BGS gespeicherten personenbezogen Daten und unterlassener Vernichtung der entsprechenden Aktenvorgänge (s. Nr. 12.2.1).
- Verstoß des BGS gegen § 11 Abs. 2, 13 i. V. m. § 12 Abs. 2 BKAG wegen unzulässiger Eingabe personenbezogener Daten in das beim BKA geführte polizeiliche Informationssystem des Bundes und der Länder (s. Nr. 12.2.1).
- Verstöße gegen § 32 Abs. 1 Nr. 3 i. V. m. §§ 33 und 34 StUG durch Herausgabe von Stasi-Abhörprotokollen über eine Person der Zeitgeschichte an Journalisten (s. Nr. 5.8.1).

Bundesministerium der Finanzen

- Verstoß gegen § 18 Abs. 2 Satz 3 BDSG durch fehlerhafte Verarbeitung von FSA-Daten durch die BSV (s. Nr. 7.6.2).
- Verstoß gegen §§ 304 SGB III, 107 SGB IV wegen unzulässiger Verarbeitung personenbezogener Daten durch ein Hauptzollamt (s. Nr. 7.8).
- Verstoß eines Bundesvermögensamtes gegen die Regelungen der §§ 90 ff BBG beim Umgang mit besonders schützenswerten Daten – Personalaktendaten (s. Nr. 18.3.2).
- Verstoß eines Hauptzollamtes gegen die Regelungen der §§ 90 ff BBG beim Umgang mit Personalaktendaten (s. Nr. 18.3.2).

Bundesanstalt für Arbeit

- Zahlreiche Verstöße gegen gesetzliche Vorgaben der §§ 90 bis 90f BBG wegen Mängeln bei der Anlage und Führung von Personalakten (s. Nr. 18.3.1).

Berufsgenossenschaften

- Verstöße gegen § 200 Abs. 2 SGB VII wegen Nichtgewährung des Gutachterauswahlrechts und wegen fehlenden Hinweises auf ein Widerspruchsrecht hinsichtlich der Übermittlung medizinischer Daten sowie Verstöße gegen § 199 Abs. 3 und § 200 Abs. 2 SGB VII wegen Nichtgewährung des Gutachterauswahlrechts (s. Nr. 23.1).

Anlage 4 (zu Nr. 32.4)

Erklärung der 22. Internationalen Datenschutzkonferenz vom 29. September 2000: VENICE DECLARATION

The data protection commissioners from the countries convened in Venice on the occasion of the 22nd International Conference on Privacy and Personal Data Protection agree on the need for reaffirming common data protection principles and standards in the face of the increasingly pervasive data processing technologies, the growing number of users of such technologies and the intensification of data exchanges worldwide.

Many international instruments are already available in this sector: from OECD Privacy Guidelines up to Council of Europe Convention no. 108, EU directives, resolutions and recommendations from international organizations.

These instruments already represent the significant core of reference principles supported by wideranging consensus; they are the basis of a common exercise with a view to securing their worldwide application taking due account of the many technological and social changes.

In the light of the recognition of privacy as a fundamental personal right and as a constitutive element of citizens' freedom, our work should aim at a global recognition of guidelines for the processing of personal data

– reaffirming the binding nature of these principles, with particular regard to the purposes of data collection, the need for fair, transparent processing operations (especially in respect of the socalled invisible processing operations), proportionality, quality of data, time for which the data can be kept, access and the other data subjects' rights;

– providing data subjects with more effective protection via the independent supervision of processing operations and the availability of user-friendly remedies;

– strengthening the safeguards applying to the processing of certain categories of data such as genetic data or data related to the various types of electronic surveillance.

This would allow citizens worldwide to attain an adequate, more widely shared level of protection regardless of the place where the processing is performed and irrespective of the instruments used for implementing protection in national and international fora.

Data Protection and Privacy Commissioners will work with others to elaborate and implement the globally recognised principles.

Anlage 5 (zu Nr. 2.2.1)

Datenschutzgruppe nach Artikel 29 der EG-Datenschutzrichtlinie Von der Arbeitsgruppe angenommene Dokumente

WP 1 (5012/97) bis WP 15 (5092/98)	s. 17. TB, Anlage 18 (zu Nr. 2.2.1)
WP 16 (5013/99)	Arbeitsunterlage: Die Verarbeitung personenbezogener Daten im Internet Angenommen am 23. Februar 1999
WP 17 (5093/98)	Empfehlung 1/99 über die unsichtbare und automatische Verarbeitung personenbezogener Daten im Internet durch Software und Hardware Angenommen am 23. Februar 1999
WP 18 (5005/99)	Empfehlung 2/99 zur Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs Angenommen am 3. Mai 1999
WP 19 (5047/99)	Stellungnahme 2/99 zur Angemessenheit der „Internationalen Grundsätze des sicheren Hafens“, ausgegeben vom Wirtschaftsministerium der USA am 19. April 1999 Angenommen am 3. Mai 1999
WP 20 (5055/99)	Stellungnahme 3/99 betreffend die Informationen des öffentlichen Sektors und Schutz personenbezogener Daten – Beitrag zu der mit dem Grünbuch der Europäischen Kommission unter dem Titel „Informationen des öffentlichen Sektors – eine Schlüsselrolle für Europa“ begonnenen Anhörung (KOM [1998] 585) Angenommen am 3. Mai 1999
WP 21 (5066/99)	Stellungnahme 4/99 zu den Häufig Gestellten Fragen (Frequently Asked Questions), vorgelegt vom US-Handelsministerium im Zusammenhang mit den vorgeschlagenen „Grundsätzen des sicheren Hafens“ Angenommen am 7. Juni 1999
WP 22 (5054/99)	Stellungnahme 5/99 zum Schutzniveau personenbezogener Daten in der Schweiz Angenommen am 7. Juni 1999
WP 23 (5075/99)	Arbeitsunterlage zum gegenwärtigen Stand der Diskussion zwischen der Europäischen Kommission und der Regierung der Vereinigten Staaten über die „Internationalen Grundsätze des Sicheren Hafens“ Angenommen am 7. Juli 1999
WP 24 (5070/99)	Stellungnahme 6/99 zum Schutzniveau personenbezogener Daten in Ungarn Angenommen am 7. September 1999
WP 25 (5085/99)	Empfehlung 3/99 zur Aufbewahrung von Verkehrsdaten durch Internet-Dienstanbieter für Strafverfolgungszwecke Angenommen am 7. September 1999
WP 26 (5143/99)	Empfehlung 4/99 über die Aufnahme des Grundrechts auf Datenschutz in den Europäischen Grundrechtekatalog Angenommen am 7. September 1999

WP 27 (5146/99)	Stellungnahme 7/99 zum Datenschutzniveau, das die Grundsätze des sicheren Hafens in ihrer veröffentlichten Form, die dazu gehörigen Häufig Gestellten Fragen (FAQ) und andere vom US-Handelsministerium am 15./16. November 1999 veröffentlichte Dokumente gewährleisten Angenommen am 3. Dezember 1999
WP 28 (5007/00)	Stellungnahme 1/2000 zu bestimmten Datenschutzaspekten des elektronischen Geschäftsverkehrs Vorgelegt von der Internet-Task Force Angenommen am 3. Februar 2000
WP 29 (5009/00)	Stellungnahme 2/2000 zur allgemeinen Neugestaltung des Rechtsrahmens für den Telekommunikationssektor Vorgelegt von der Internet-Task Force Angenommen am 3. Februar 2000
WP 30 (5139/99)	Empfehlung 1/2000 zur Umsetzung der Richtlinie 95/46/EG Angenommen am 3. Februar 2000
WP 31 (5019/00)	Stellungnahme 3/2000 zum Dialog EU-USA betreffend die Vereinbarung über den sicheren Hafen Angenommen am 16. März 2000
WP 32 (CA07/434/00)	Stellungnahme 4/2000 über das Datenschutzniveau, das die Grundsätze des sicheren Hafens bieten Angenommen am 16. Mai 2000
WP 33 (5058/00)	Stellungnahme 5/2000 Nutzung von öffentlichen Verzeichnissen für Invert- oder Multikriterien-Suchdienste (Inverse Verzeichnisse) Angenommen am 13. Juli 2000
WP 34 (5062/00)	Stellungnahme 6/2000 zur Genomproblematik Angenommen am 13. Juli 2000
WP 35 (5066/00)	Dritter Jahresbericht über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten und des Schutzes der Privatsphäre in der Gemeinschaft und in Drittländern Berichtsjahr 1998 Angenommen am 22. Dezember 1999
WP 36 (5042/00)	Stellungnahme 7/2000 zum Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privat-sphäre in der elektronischen Kommunikation vom 12. Juli 2000 – KOM (2000) 385 Angenommen am 2. November 2000
WP 37 (5063/00)	Privatsphäre im Internet – Ein integrierter EU-Ansatz zum Online-Datenschutz Angenommen am 21. November 2000

Die genannten Papiere sind unter folgenden Internetadressen zu finden:
http:\\www.europa.eu.int/comm/dg15 („Eingang“) und von dort weiter verlinken

oder direkt:

http://europa.eu.int/comm/internal_market/de/media/dataprot/wpdocs/index.htm

Anlage 6 (zu Nr. 2.2.2)

Grundsätze des „Sicheren Hafens“ zum Datenschutz

vorgelegt vom amerikanischen Handelsministerium am 21. Juli 2000
(abgedruckt im Amtsblatt der Europäischen Gemeinschaften Nr. L 215 vom 25. August 2000, 11f.)

Informationspflicht

Die Organisation muss Privatpersonen darüber informieren, zu welchem Zweck sie die Daten über sie erhebt und verwendet, wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe der Daten einzuschränken. Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig gebeten werden, der Organisation personenbezogene Daten zu liefern, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben oder verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt*).

Wahlmöglichkeit

Die Organisation muss Privatpersonen die Möglichkeit geben zu wählen („opt out“), ob ihre personenbezogenen Daten

a) an Dritte weitergegeben werden sollen oder

b) für einen Zweck verwendet werden sollen, der mit dem ursprünglichen oder dem nachträglich von der betreffenden Person genehmigten Erhebungszweck unvereinbar ist.

Der betroffenen Person muss die Ausübung ihres Wahlrechts durch leicht erkennbare und verständliche, leicht zugängliche und kostengünstige Verfahren ermöglicht werden.

Bei sensiblen Daten (wie z. B. Angaben über den Gesundheitszustand, über Rassen- oder ethnische Zugehörigkeit, über politische, religiöse oder philosophische Überzeugungen, über die Mitgliedschaft in einer Gewerkschaft oder über das Sexualleben) benötigen die Organisationen die ausdrückliche Zustimmung („opt in“) der betroffenen Personen, wenn die Daten an Dritte weitergegeben oder für einen anderen als den ursprünglichen Erhebungszweck oder den Zweck verwendet werden sollen, dem die betroffene Person nachträglich durch Ausübung des Wahlrechts zugestimmt hat. In jedem Fall sollen die Organisationen alle ihnen von Dritten übermittelten Informationen als sensibel behandeln, die der Übermittler als sensibel einstuft und behandelt.

Weitergabe

Eine Organisation darf Daten nur dann an Dritte weitergeben, wenn sie die Grundsätze der Informationspflicht und der Wahlmöglichkeit anwendet. Möchte eine Organisation Daten an einen Dritten weitergeben, der in ihrem Auftrag und auf ihre Anweisung tätig ist (vergleiche Fußnote), kann sie dies tun, sofern der Dritte entweder dem „sicheren Hafen“ angehört oder der Richtlinie unterliegt, oder von einer anderen Feststellung angemessenen Schutzniveaus erfasst wird oder sich schriftlich in einer Vereinbarung mit der Organisation dazu verpflichtet, zumindest das Maß an Schutz personenbezogener Daten zu gewährleisten, das in den entsprechenden Grundsätzen des „sicheren Hafens“ gefordert wird. Eine Organisation, die diese Forderungen erfüllt, kann nicht haftbar gemacht werden (sofern sie nichts anderes vereinbart hat), wenn ein Dritter, an den sie Daten übermittelt hat, Beschränkungen der Verarbeitung dieser Daten missachtet oder sie in einer Weise verarbeitet, die seinen Erklärungen widerspricht, es sei denn, die Organisation wusste oder konnte wissen, dass der Dritte die Daten in unzulässiger Weise verarbeiten würde, und hat keine angemessenen Schritte unternommen, um das zu unterbinden.

Sicherheit

Organisationen, die personenbezogene Daten erstellen, verwalten, verwenden oder verbreiten, müssen angemessene Sicherheitsvorkehrungen treffen, um sie vor Verlust, Missbrauch und unbefugtem Zugriff, Weitergabe, Änderung und Zerstörung zu schützen.

Datenintegrität

In Übereinstimmung mit den Grundsätzen müssen personenbezogene Daten für den beabsichtigten Verwendungszweck erheblich sein. Eine Organisation darf personenbezogene Daten nicht in einer Weise verarbeiten, die mit dem ursprünglichen Erhebungszweck oder mit dem Zweck unvereinbar ist, dem der Betroffene nachträglich zugestimmt hat. In dem für diese Zwecke notwendigen Umfang muss die Organisation durch angemessene Maßnahmen gewährleisten, dass die Daten für den vorgesehenen Zweck hinreichend zuverlässig, genau, vollständig und aktuell sind.

Auskunftsrecht

Privatpersonen müssen Zugang zu den personenbezogenen Daten haben, die eine Organisation über sie besitzt,

*) Die Übermittlung solcher Daten an einen Dritten ist nicht mitteilungspflichtig bzw. unterliegt nicht dem Grundsatz der Wahlmöglichkeit, wenn dieser im Auftrag oder auf Anweisung der Organisation tätig ist. Der Grundsatz der Weitergabe gilt jedoch auch in solchen Fällen.

und sie müssen die Möglichkeit haben, diese zu korrigieren, zu ändern oder zu löschen, wenn sie falsch sind, es sei denn, die Belastung oder die Kosten für die Gewährung des Zugangs würden in dem jeweiligen Fall in einem Missverhältnis zu den Nachteilen für den Betroffenen stehen, oder Rechte anderer Personen als des Betroffenen würden verletzt.

Durchsetzung

Für einen effektiven Schutz der Privatsphäre müssen Mechanismen geschaffen werden, die die Einhaltung der Grundsätze des „sicheren Hafens“ gewährleisten, Rechtsbehelfe für Betroffene vorsehen, bei deren Daten die Grundsätze nicht eingehalten wurden, sowie Sanktionen für die Organisation, die die Grundsätze nicht befolgt. Diese Mechanismen müssen mindestens folgendes umfassen: a) leicht zugängliche, erschwingliche und von unabhängigen Stellen durchgeführte Verfahren, nach denen Beschwerden, die betroffene Personen unter Berufung auf die Grundsätze erhoben haben, behandelt werden und nach denen Schadensersatz geleistet wird, wenn das geltende Recht oder private Regelungen dies vorsehen; b) Kontrollmaßnahmen, um zu überprüfen, ob die Bescheinigungen und Behauptungen der Unternehmen über ihre Datenschutzmaßnahmen der Wahrheit entsprechen und ob diese Maßnahmen wie angegeben durchgeführt werden; c) Verpflichtungen zur Lösung von Problemen, die daraus resultieren, dass Organisationen die Einhaltung der Grundsätze zwar erklärt, sich aber trotzdem nicht daran gehalten haben, sowie entsprechende Sanktionen für diese Organisationen. Die Sanktionen müssen hinreichend streng sein, um sicherzustellen, dass die Organisationen die Grundsätze einhalten.

Anlage 7 (zu Nr. 2.5)

Die Konferenz der Europäischen Datenschutzbeauftragten

– ist sich der raschen Entwicklung der Informationstechnologien bewusst,

– stellt die bedeutsamen sozialen Auswirkungen dieser Entwicklung fest

– und betont die Notwendigkeit, die Achtung des Rechts auf Privatleben bei der Anwendung dieser Technologien sicherzustellen.

Sie **bekräftigt** die Bedeutung der Rolle der Datenschutzbeauftragten für die Förderung guter Datenschutzpraxis und bei der Unterrichtung der Öffentlichkeit hierüber, wenn und soweit diese es für angebracht halten, über Datenschutzangelegenheiten und insbesondere über gute Praxis und Übereinstimmung mit den Datenschutzgesetzen, der Richtlinie 95/46/EG und der Europaratskonvention 108 zu informieren.

Helsinki 15./16. April 1999

Anlage 8 (zu Nr. 2.5)

Konferenz der Europäischen Datenschutzbeauftragten vom 6. bis 7. April 2000 in Stockholm: Aufbewahrung von Verkehrsdaten durch Internet Service Provider (ISP)

Die Frühjahrskonferenz 2000 der europäischen Datenschutzbeauftragten stellt mit Besorgnis fest, dass es Vorschläge gibt, laut welchen ISP routinemäßig Verkehrsdaten aufbewahren sollen über die Erfordernisse der Gebührenabrechnung hinaus, um den rechtspflegenden Behörden Zugang zu denselben zu ermöglichen.

Die Konferenz betont, dass eine derartige Aufbewahrung eine unzulässige Beeinträchtigung der Grundrechte darstellt, die Personen durch Artikel 8 der Europäischen Konvention über Menschenrechte zugesichert ist.

Wenn in besonderen Fällen Verkehrsdaten aufbewahrt werden sollen, muss eine beweisbare Notwendigkeit vorliegen und die Zeitdauer der Aufbewahrung muss so kurz wie möglich sein; weiterhin muss die diesbezügliche Praxis klar gesetzlich geregelt sein.

Englischsprachige Version

„Retention of Traffic Data by Internet Service Providers (ISPs)

The Spring 2000 Conference of European Data Protection Commissioners notes with concern proposals that ISPs should routinely retain traffic data beyond the requirements of billing purposes in order to permit possible access by law enforcement bodies.

The Conference emphasises that such retention would be an improper invasion of the fundamental rights guaranteed to individuals by Article 8 of the European Convention on Human Rights. Where traffic data are to be retained in specific cases, there must be a demonstrable need, the period of retention must be as short as possible and the practice must be clearly regulated by law.“

Anlage 9 (zu Nr. 2.1.1)

Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999 zu: Modernisierung des Datenschutzrechts jetzt – umfassende Novellierung des BDSG nicht aufschieben

Die deutschen Datenschutzbeauftragten haben bereits früh gefordert, die Novellierung des BDSG zur Umsetzung der EG-Datenschutzrichtlinie zu einer gründlichen Modernisierung des veralteten deutschen Datenschutzrechts zu nutzen. Da die dreijährige Anpassungsfrist im Oktober 1998 verstrichen ist, besteht jetzt ein erheblicher Zeitdruck. Für die Neuregelung, die derzeit in der Bundesregierung und in Koalitionsgremien vorbereitet wird, ist daher ein „Zwei-Stufen-Konzept“ vorgesehen. Einem ersten, in Kürze vorzulegenden Novellierungsgesetz soll zu einem späteren Zeitpunkt eine zweite Änderung folgen, die weitere Verbesserungen enthalten soll. Die Konferenz geht davon aus, dass das Zweistufenkonzept von dem festen politischen Willen getragen wird, die zweite Stufe nach Einbringung des ersten Gesetzentwurfes zügig in Angriff zu nehmen und noch in dieser Legislaturperiode abzuschließen. Auch der in dieser Stufe bestehende Handlungsbedarf duldet keinen Aufschub.

Die Konferenz begrüßt, dass jetzt mit Hochdruck an der BDSG-Novellierung gearbeitet wird und Verantwortliche in Regierung und Fraktionen zugesagt haben, die erste Stufe der Neuregelung werde sich nicht auf das von der Richtlinie geforderte Minimum beschränken. Sie unterstützt die Vorschläge, Regelungen zur Videoüberwachung, zu Chipkarten und zum Datenschutzaudit aufzunehmen. Gleiches gilt für die Übernahme der zukunftsweisenden Bestimmungen zur Datenvermeidung sowie zur anonymen bzw. pseudonymen Nutzung von Telediensten aus dem Multimediarecht. Diese sind wichtige und dringend notwendige Regelungen zur Modernisierung des Datenschutzrechts. Die Konferenz drückt daher ihre Erwartung darüber aus, dass diese Vorschriften in der ersten Stufe des Gesetzgebungsverfahrens zügig verabschiedet werden.

Zu den Punkten, die keinen Aufschub dulden, gehört auch die Verbesserung der Voraussetzungen für eine effektive Datenschutzkontrolle. Die völlig unabhängige Gestaltung der Kontrolle im nichtöffentlichen Bereich muss institutionell sichergestellt und durch eine sachgerechte finanzielle und personelle Ausstattung unterstützt werden. Gegenwärtig noch bestehende Einschränkungen der Kontrollkompetenzen im öffentlichen Bereich müssen abgebaut, den Aufsichtsbehörden müssen wirksamere Befugnisse an die Hand gegeben werden.

Zum Schutz der Bürgerinnen und Bürger sind bei massenhaften Datenerhebungen mit unkalkulierbaren Datenverarbeitungsrisiken oder ungeklärter Zweckbestimmung klare materielle Grenzen durch den Gesetzgeber zu ziehen.

Die bereichsspezifischen Gesetze, z. B. die Sicherheitsgesetze, dürfen nicht vom Bundesdatenschutzgesetz mit den dort zu erwartenden substantiellen Fortschritten für die Bürgerinnen und Bürger, wie beispielsweise einem verbesserten Auskunftsrecht, abgekoppelt werden.

Notwendig ist nach Auffassung der Konferenz, dass das Datenschutzrecht auch in Zukunft bürgerfreundlich und gut lesbar formuliert ist. Dies ist eine unverzichtbare Akzeptanzvoraussetzung für den Datenschutz bei Bürgern, Wirtschaft und Verwaltung.

Anlage 10 (zu Nr. 8.8)

Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999 zu: Transparente Hard- und Software

Die Datenschutzbeauftragten des Bundes und der Länder haben sich wiederholt für die Nutzung datenschutzfreundlicher Technologien eingesetzt. Sie sehen jedoch mit Sorge die Entwicklung im Bereich der Informationstechnik, die zu neuen Industriestandards und Produkten führt, die für die Benutzerinnen und Benutzer kaum durchschaubar und selbst für Fachleute nur noch eingeschränkt revisionsfähig sind.

Beispielsweise sind seit kurzem mit dem Intel Pentium III-Prozessor bestückte PCs auf dem Markt, deren Prozessor bei der Herstellung mit einer eindeutigen Nummer (Processor Serial Number – PSN) versehen wurde. Intel sieht vor, das Auslesen der PSN durch die Nutzerinnen und Nutzer kontrollieren zu lassen. Die mittlerweile bekannt gewordenen Manipulationsmöglichkeiten der dafür erforderlichen Software machen deutlich, dass die Existenz einer solchen eindeutigen Kennung kaum kontrollierbare Nutzungsmöglichkeiten eröffnet, die dem Datenschutz diametral zuwider laufen.

Die durch den Intel Pentium III initiierte Debatte um eindeutige Kennungen brachte ans Tageslicht, dass Softwarehersteller Nutzern neuerer Office-Produkte ohne deren Wissen eindeutige Kennungen zuordnen. Diese Kennungen können in Dokumenten versteckt sein und bei der Nutzung des Internets von Softwareherstellern verdeckt abgefragt werden.

Werden Daten der Nutzerinnen und Nutzer übermittelt, ohne dass sie dies bemerken, kann deren missbräuchliche Verwendung die Anonymität der Anwender von Informationstechnik weiter aushöhlen. Den Erfordernissen des Datenschutzes wird aber nur dann ausreichend Rechnung getragen, wenn zum Schutz der Privatheit transparente und von den Nutzerinnen und Nutzern in eigener Verantwortung bedienbare Sicherheitsfunktionen zur Verfügung stehen.

Deshalb erwarten die Datenschutzbeauftragten des Bundes und der Länder von Herstellern von Informations- und Kommunikationstechnik, Hard- und Software so zu entwickeln und herzustellen, dass Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen überzeugen können.

Den Anwendern moderner Technik empfehlen die Datenschutzbeauftragten, nur solche Produkte einzusetzen, welche auch eine Transparenz der Verfahrensabläufe gewährleisten.

Anlage 11 (zu Nr. 16.3)

Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999 zu: Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation (ENFOPOL '98) *)

Gegenwärtig berät der Rat der EU über den Entwurf einer Entschließung zur grenzüberschreitenden Überwachung der Telekommunikation und der Internet-Nutzung (ENFOPOL '98).

Die Konferenz der Datenschutzbeauftragten hält es für inakzeptabel, dass der entsprechende Entwurf bisher geheimgehalten und ohne Einbeziehung der Datenschutzbeauftragten beraten wird.

Sie fordert die Bundesregierung auf, der Schaffung gemeinsamer Standards zur grenzüberschreitenden Überwachung der Telekommunikation nur insoweit zuzustimmen, als damit nicht zusätzliche Eingriffe in das Grundrecht auf unbeobachtete Kommunikation und das Fernmeldegeheimnis verbunden sind und die Nutzung datenschutzfreundlicher Technologien (z. B. prepaid cards) nicht konterkariert wird.

*) Bei Redaktionsschluss: ENFOPOL 19

Anlage 12 (zu Nr. 6.6)

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16. August 1999 zu: Angemessener Datenschutz auch für Untersuchungsgefangene

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass die Bundesregierung den Entwurf eines Gesetzes zur Regelung des Vollzuges der Untersuchungshaft vorgelegt hat. Damit wird die seit Jahren erhobene Forderung der Datenschutzbeauftragten nach einer bereichsspezifischen gesetzlichen Regelung aufgegriffen.

Diese Regelung muss das Strafverfolgungs- und Sicherheitsinteresse des Staates im Rahmen des gesetzlichen Zwecks der Untersuchungshaft berücksichtigen. Gleichzeitig sind jedoch das Persönlichkeitsrecht der Gefangenen sowie die Unschuldsvermutung und der Anspruch auf wirksame Verteidigung im Strafverfahren angemessen zur Geltung zu bringen.

Der Gesetzentwurf der Bundesregierung trägt diesem Anliegen durch differenzierende Vorschriften teilweise Rechnung, läßt allerdings noch Raum für datenschutzrechtliche Verbesserungen. Die Stellungnahme des Bundesrates betont demgegenüber einseitig das staatliche Vollzugsinteresse und entfernt sich damit deutlich vom Ziel einer sorgfältigen Güterabwägung.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder muss die gesetzliche Regelung insbesondere folgenden Anforderungen genügen:

– Entgegen dem Vorschlag des Bundesrates, von einer inhaltlichen Überwachung nur ausnahmsweise nach dem Ermessen des Gerichts abzusehen, sollte im weiteren Gesetzgebungsverfahren an der Konzeption der Bundesregierung festgehalten werden. Der Gesetzentwurf der Bundesregierung differenziert bei der Überwachung der Unterhaltung mit Besucherinnen und Besuchern sowie bei der Kontrolle des Textes von Schriftstücken sachgerecht nach Haftgründen. Nur im Falle der Untersuchungshaft wegen Verdunkelungsgefahr sollten diese Maßnahmen unmittelbar und generell durch Gesetz vorgeschrieben werden, während sie bei Vorliegen anderer Haftgründe (z. B. Fluchtgefahr) nur im Einzelfall aufgrund richterlicher Anordnung erfolgen dürfen. Darüber hinaus sollte im weiteren Gesetzgebungsverfahren die Möglichkeit unüberwachter Kontakte der Gefangenen zu nahen Angehörigen mit Zustimmung der Staatsanwaltschaft auch in Fällen der Untersuchungshaft wegen Verdunkelungsgefahr erwogen werden. Stichprobenartige Überprüfungen von Schriftstücken durch die Vollzugsanstalt anstelle einer Textkontrolle sollten nicht den gesamten Schriftverkehr einzelner Gefangener umfassen. Dies könnte sich im Ergebnis als verdachtsunabhängige Totalkontrolle ohne richterliche Entscheidung auswirken.

– Das Recht auf ungehinderten und unüberwachten telefonischen Kontakt zwischen Verteidigung und Beschuldigten muss auch in der Untersuchungshaft gewährleistet sein. Mit dem rechtsstaatlichen Gebot wirksamer Strafverteidigung wäre es nicht vereinbar, diesen Kontakt von einer besonderen Erlaubnis des Gerichts abhängig zu machen, wie vom Bundesrat befürwortet.

– Bei Datenübermittlungen an öffentliche Stellen außerhalb der Vollzugsanstalt (z. B. Sozialleistungsträger, Ausländerbehörden) und an Forschungseinrichtungen müssen die schutzwürdigen Interessen der Betroffenen im Rahmen einer Abwägung berücksichtigt werden. Auch die Erteilung von Auskünften an die Verletzten der Straftat sollte der Gesetzgeber unter Beachtung der Unschuldsvermutung regeln.

– Die vom Bundesrat vorgeschlagene erhebliche Einschränkung des Auskunfts- und Akteneinsichtsrechts von Gefangenen im Hinblick auf den Zweck der Untersuchungshaft würde wesentliche Datenschutzrechte in einem besonders sensiblen Bereich weitgehend entwerten und ist daher abzulehnen.

Anlage 13 (zu Nr. 2.4)

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 zum Beschluss des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union

Der Europäische Rat hat anlässlich seiner Zusammenkunft am 4. Juni 1999 in Köln die Ausarbeitung einer Charta der Grundrechte der Europäischen Union beschlossen. In dem Ratsbeschluss heißt es: „Im gegenwärtigen Entwicklungszustand der Union ist es erforderlich, eine Charta dieser Rechte zu erstellen, um die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern“.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen nachhaltig die Initiative des Europäischen Rates zur Ausarbeitung einer europäischen Grundrechtscharta. Sie fordern Bundesregierung, Bundestag und Bundesrat auf, sich für die Einfügung eines Grundrechts auf Datenschutz in den zu schaffenden Katalog europäischer Grundrechte und dessen Verankerung in den Verträgen der Europäischen Union einzusetzen. Damit würde der herausragenden Bedeutung des Datenschutzes in der Informationsgesellschaft Rechnung getragen.

Die europäische Datenschutzrichtlinie verpflichtet die Mitgliedstaaten zur Gewährleistung des Schutzes der Grundrechte und Grundfreiheiten und insbesondere des Schutzes der Privatsphäre (Art. 1 Abs. 1). Die Datenschutzbeauftragten weisen darauf hin, dass einige europäische Länder ein Datenschutzgrundrecht in ihre Verfassung aufgenommen haben; in einigen anderen Ländern wurde ihm durch die Rechtsprechung Grundrechtsgeltung zuerkannt. In Deutschland wird das vom Bundesverfassungsgericht aus dem Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) abgeleitete Grundrecht auf Datenschutz als solches von zahlreichen Landesverfassungen ausdrücklich erwähnt.

Anlage 14 (zu Nr. 6.4.1)

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 zu: Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation

Die Ausbreitung moderner Telekommunikationsnetze und die Fortentwicklung der Informationstechnologie erfolgen in großen Schritten. Dieser technische Fortschritt hat einerseits zu einer massenhaften Nutzung der neuen Möglichkeiten der Telekommunikation und damit zu einer grundlegenden Veränderung des Kommunikationsverhaltens der Bevölkerung geführt. Andererseits erhalten dadurch die herkömmlichen Befugnisse der Strafverfolgungsbehörden zur Überwachung des Fernmeldeverkehrs eine neue Dimension, weil aufgrund der weitreichenden Digitalisierung immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden.

Die bei der Telekommunikation anfallenden Daten können mit geringem Aufwand in großem Umfang kontrolliert und ausgewertet werden. Anhand von Verbindungsdaten lässt sich nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Bereits auf der Ebene der bloßen Verbindungsdaten können so Verhaltensprofile erstellt werden, die die Aussagekraft von Inhaltsdaten erreichen oder im Einzelfall sogar übertreffen. Eine staatliche Überwachung dieser Vorgänge greift daher tief in das Telekommunikationsgeheimnis der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse.

Die bisherige rechtliche Grundlage für den Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in § 12 des Fernmeldeanlagengesetzes (FAG) stammt noch aus einer Zeit, in der die analoge Vermittlungstechnik vorherrschte, nicht für jedes Gespräch personenbezogene Verbindungsdaten erzeugt wurden und die Telekommunikationsdienste in wesentlich geringerem Maße als heute genutzt wurden. Die Vorschrift erlaubt auch Zugriffe auf Verbindungsdaten wegen unbedeutenden Straftaten, bei denen eine inhaltliche Überwachung der Telekommunikation unzulässig wäre. Unter Berücksichtigung der Digitaltechnik, der vollständigen Datenerfassung und der Möglichkeit zur Bildung von Verhaltensprofilen verstößt § 12 FAG daher gegen den Verhältnismäßigkeitsgrundsatz und ist somit nicht mehr geeignet, Eingriffe in das Telekommunikationsgeheimnis zu rechtfertigen.

In einem früheren Gesetzesentwurf war vorgesehen, den Zugriff auf Verbindungsdaten grundsätzlich auf nicht unerhebliche Straftaten zu beschränken. Beschlossen wurde aber lediglich die unveränderte Fortgeltung des § 12 FAG, zuletzt befristet bis zum 31. Dezember 1999. Nunmehr wollen der Bundesrat und die Justizministerkonferenz die Befristung für die Weitergeltung dieser Vorschrift aufheben und es damit beim bisherigen, verfassungsrechtlich bedenklichen Rechtszustand belassen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen eine Verlängerung der Geltungsdauer des § 12 FAG und fordern statt dessen eine Neufassung der Eingriffsbefugnis unter Beachtung der grundrechtlichen Bindungen und Anforderungen, die sich aus dem von Art. 10 Grundgesetz geschützten Telekommunikationsgeheimnis ergeben.

Die gesetzliche Ermächtigung für den Zugriff auf Verbindungsdaten gehört sachlich in die Strafprozessordnung. Die gesetzlichen Zugriffsvoraussetzungen sollten in Abstimmung mit § 100a StPO neu geregelt werden.

Anlage 15 (zu Nr. 6.5)

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 zu: Täter-Opfer-Ausgleich und Datenschutz

Kernstück datenschutzrechtlicher Überlegungen zum Täter-Opfer-Ausgleich ist die Frage, ob Institutionen zur Durchführung des Ausgleichsverfahrens umfassende Informationen insbesondere über Opfer von Straftaten erhalten dürfen, ohne dass diese davon Kenntnis erlangt und eingewilligt haben.

Darin wäre ein unverhältnismäßiger Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen zu sehen. Dies ist nach geltendem Recht unzulässig.

Der nunmehr vorliegende Gesetzentwurf der Bundesregierung (BR-Drs. 325/99 vom 28.Mai 1999) sieht in § 155a Satz 3 StPO-Entwurf vor, dass nur der ausdrücklich geäußerte entgegenstehende Wille der oder des Verletzten dazu führt, dass keine Datenübermittlungen an Schlichtungsstellen erfolgen sollen. Das bedeutet, dass solche im Einzelfall gleichwohl möglich sind. Dies halten die Datenschutzbeauftragten nicht für ausreichend.

Der Bundesrat ist sogar dem Gesetzentwurf der Bundesregierung nicht gefolgt; er hat vielmehr angeregt, im Gesetz klarzustellen, dass es für solche Datenübermittlungen auf den Willen der Opfer nicht ankommen soll. Folgende Argumente werden dafür genannt: Eine vor der Einschaltung von Schlichtungsstellen durch die Justiz einzuholende Einwilligung führe dazu, dass das kriminalpolitisch wichtige Institut des „Täter-Opfer-Ausgleichs“ nicht ausreichend genutzt werde. Erst die professionelle Tätigkeit der Schlichtungsstellen mit ihrem Selbstverständnis als „objektive Dritte mit dem Gebot der Unterstützung jeder Partei“ könnte wirksame Überzeugungsarbeit leisten; nur dann könne der Rechtsfriede dauerhafter als bei herkömmlichen Verfahren sichergestellt werden, wenn durch die „fachlich geleitete Auseinandersetzung“ der „am strafrechtlich relevanten Konflikt beteiligten Parteien im Idealfall Verständnis und wechselseitige Toleranz geweckt werden“.

Dieser Argumentation widersprechen die Datenschutzbeauftragten entschieden: Die Achtung und wirksame Unterstützung der Opfer ist ein wesentliches Anliegen des Strafverfahrens. Rechtsfriede und Toleranz können nur verwirklicht werden, wenn die Strafverfolgungsbehörden bei Datenübermittlungen an Schlichtungsstellen (z. B. in der Rechtsform von Vereinen) den Willen und die Eigenverantwortung der Opfer uneingeschränkt respektieren. Auch die Sicht der Beschuldigten, ohne deren Mitwirkung der Täter-Opfer-Ausgleich nicht durchgeführt werden kann, sollte von den Strafverfolgungsbehörden dabei berücksichtigt werden. Die Konferenz der Datenschutzbeauftragten fordert deshalb, dass an der Voraussetzung der unzweifelhaften Einwilligung vor solchen Datenübermittlungen festgehalten wird.

Ferner sollte der Gesetzgeber festlegen, dass die Berichte der Schlichtungsstellen an Staatsanwaltschaft und Gericht nur für Zwecke der Rechtspflege verwendet werden dürfen. Das besondere Vertrauensverhältnis zwischen den Schlichtungsstellen und den am „Täter-Opfer-Ausgleich“ Beteiligten muss gesetzlich geschützt werden.

Anlage 16 (zu Nr. 6.15)

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 zu: Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich am 9./10. März 1995 gefordert, dass insbesondere die Dauer der Aufbewahrung von Strafakten nach rechtskräftigem Abschluss eines Strafverfahrens, ihre Aussonderung und Vernichtung einer Regelung durch formelles, den Grundsätzen des Volkszählungsurteils entsprechendes Gesetz bedarf.

Mit Beschluss vom 16. August 1998 hat das Oberlandesgericht Frankfurt am Main festgestellt, dass der derzeitige Zustand zwar für eine Übergangsfrist noch hinzunehmen sei, dass die Schaffung einer gesetzlichen Grundlage für die Aufbewahrung von Akten jedoch nicht als nur mittelfristige Aufgabenstellung des Gesetzgebers betrachtet werden dürfe, sondern alsbald in Angriff zu nehmen sei. In gleicher Weise hat auch das OLG Hamm mit Beschluss von 17. September 1998 darauf hingewiesen, dass die Aufbewahrung von Strafakten einer gesetzlichen Grundlage bedarf. Auch der Entwurf des Strafverfahrensänderungsgesetzes 1999 enthält insoweit keine Regelung.

Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für dringend geboten, dass unverzüglich mit der Umsetzung dieser Aufgabe begonnen wird. Sie weisen ferner darauf hin, dass auch für die Aufbewahrung von Zivilprozessakten und Akten im Bereich der freiwilligen Gerichtsbarkeit umgehend gesetzliche Regelungen zu schaffen sind, die die Dauer der Aufbewahrung auf das erforderliche Maß festlegen.

Anlage 17 (zu Nr. 21.1)

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 zu: Patientenschutz durch Pseudonymisierung

Im Gesundheitsausschuss des Deutschen Bundestages wird derzeit der vom Bundesministerium für Gesundheit vorgelegte Gesetzesentwurf zur Gesundheitsreform 2000 dahingehend geändert, dass die Krankenkassen künftig von den Leistungserbringern (z. B. Ärztinnen und Ärzte, Krankenhäuser, Apotheken) die Patientendaten nicht in personenbezogener, sondern in pseudonymisierter Form erhalten. Dieses neue Modell nimmt eine zentrale Forderung der Datenschutzbeauftragten auf, für die Verarbeitung von Patientendaten solche technischen Verfahren zu nutzen, die die Persönlichkeitsrechte der Betroffenen wahren und so die Entstehung des „gläsernen Patienten“ verhindern.

Auch anhand von pseudonymisierten Daten können die Krankenkassen ihre Aufgaben der Prüfung der Richtigkeit der Abrechnungen sowie der Wirtschaftlichkeit und der Qualität der Leistungen erfüllen.

Die Konferenz unterstützt den Bundesbeauftragten für den Datenschutz dabei, dass in den Ausschussberatungen die Wirksamkeit der Pseudonymisierung, die gesetzliche Festlegung von Voraussetzungen für die Identifizierung der Versicherten zu bestimmten Zwecken und die Definition strikter Zweckbindung dieser Daten durchgesetzt werden.

Anlage 18 (zu Nr. 34 dort Nr. 8)

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08. Oktober 1999 zu: Eckpunkte der deutschen Kryptopolitik – ein Schritt in die richtige Richtung

Das Brief-, Post- und Fernmeldegeheimnis zählt zu den traditionellen und wichtigsten Garantien einer freiheitlichen Verfassung. Artikel 10 Grundgesetz gewährleistet deshalb die freie Entfaltung der Persönlichkeit durch einen privaten, vor Dritten verborgenen Austausch von Nachrichten, Gedanken und Informationen. Deshalb darf nur in Ausnahmefällen im überwiegenden Allgemeininteresse auf gesetzlicher Grundlage in dieses Grundrecht eingegriffen werden.

Im Zuge der Privatisierung der Telekom hat der Staat sein Post- und Fernmeldemonopol verloren, so dass zum Grundrechtsschutz die bloße Abwehr unrechtmäßiger staatlicher Eingriffe nicht mehr genügt. Darüber hinaus bestehen die Möglichkeiten der staatlichen Datenschutzkontrolle in offenen Netzen nur in eingeschränktem Maße. Der Schutz personenbezogener Daten während der Verarbeitung und Übertragung ist häufig nicht ausreichend gewährleistet. Deshalb sind ergänzende staatliche Maßnahmen zum Schutz Aller gegen neugierige Dritte (z. B. Systembetreiber, Unternehmen mit wirtschaftlichen Interessen, Hacker und Hackerinnen, ausländische Geheimdienste) erforderlich.

Die Privatsphäre lässt sich jedoch nur mit Rechtsvorschriften nicht ausreichend schützen. Neben bestehenden Ge- und Verboten sind wirksame technische Vorkehrungen nötig. Systemdatenschutz und datenschutzfreundliche Technologien sind unverzichtbar. Den Bürgerinnen und Bürgern müssen effektive Instrumente zum Selbstschutz an die Hand gegeben werden. Der Datenverschlüsselung kommt deshalb in einem modernen Datenschutzkonzept eine herausragende Bedeutung zu.

Bislang musste befürchtet werden, dass auf Betreiben der staatlichen Sicherheitsbehörden in Deutschland das Recht auf Verschlüsselung eingeschränkt würde. Jetzt jedoch hat die Bundesregierung mit dem Eckpunktepapier vom 2. Juni 1999 die Diskussion auf eine völlig neue Basis gestellt. Richtigerweise wird darin die Kryptographie als „eine entscheidende Voraussetzung für den Datenschutz der Bürger“ besonders hervorgehoben.

Die Position der Bundesregierung, die freie Verfügbarkeit von Verschlüsselungsprodukten nicht einschränken zu wollen, wird von den Datenschutzbeauftragten des Bundes und der Länder ausdrücklich begrüßt. Damit wurde ein erster wichtiger Schritt in die richtige Richtung getan, dem jedoch weitere folgen müssen. Der im Sinne des Artikels 10 des Grundgesetzes legitime und grundrechtlich geschützte Anspruch Aller auf unbeobachtete Telekommunikation und auf den Schutz ihrer personenbezogenen Daten sollte von der Bundesregierung noch stärker unterstützt werden. Um der Bedeutung geschützter Telekommunikation unter den Bedingungen der Informationsgesellschaft gerecht zu werden, sind konkrete Maßnahmen notwendig. Vorrangig sind zu nennen:

- Aktive Förderung des Einsatzes von Verschlüsselungstechniken in der öffentlichen Verwaltung, bei Privatpersonen und in Wirtschaftsunternehmen,
- Erbringung von Serviceleistungen, die den Gebrauch von effektiven Verschlüsselungsprogrammen für jedermann erleichtern,
- Maßnahmen zum besonderen Schutz der Telekommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte und Ärztinnen, Anwälte und Anwältinnen, Psychologen und Psychologinnen),
- Unterstützung von Wirtschaftsunternehmen beim Schutz ihrer geschäftlichen Telekommunikation,
- Förderung einer neutralen Bewertung von Verschlüsselungsprodukten mit dem Ziel, den Verbrauchern Empfehlungen für ihren Gebrauch zu geben,
- Förderung der Entwicklung europäischer Verschlüsselungsprodukte mit offengelegten Algorithmen.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten die öffentlichen Stellen auf, mit gutem Beispiel voranzugehen. Sie sollten vorbehaltlos die technischen Möglichkeiten des Einsatzes kryptographischer Verfahren zum Schutz personenbezogener Daten prüfen und derartige Lösungen häufiger als bisher einsetzen. Künftig muss Kryptographie der Standard in der Informations- und Kommunikationstechnik werden, auf deren Einsatz nur dann verzichtet wird, wenn wichtige Gründe dagegen sprechen.

Hersteller von Produkten der Informations- und Telekommunikationstechnik werden aufgefordert, die guten Voraussetzungen zur Entwicklung von Verschlüsselungsprodukten in Deutschland zu nutzen, um sichere, leicht bedienbare und interoperable Produkte zu entwickeln und den Anwendern kostengünstig anzubieten. Die Datenschutzbeauftragten des Bundes und der Länder bieten hierfür ihre Kooperation an.

Anlage 19 (zu Nr. 11.2)

Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 zu: Unzulässiger Speicherungsumfang in „INPOL-neu“ geplant

Das Bundeskriminalamt und die Polizeien der Bundesländer konzipieren seit geraumer Zeit unter der Bezeichnung „INPOL-neu“ eine Fortentwicklung des gemeinsamen Informationssystems. Inzwischen steht der Beginn der schrittweisen Einführung des neuen Datenaustauschsystems kurz bevor.

Das Informationssystem INPOL wirft in vielfacher Hinsicht datenschutzrechtliche Probleme auf. Die Datenschutzbeauftragten des Bundes und der Länder haben mehrfach aus konkretem Anlass darauf hingewiesen, dass nicht jede mit den heutigen technischen Möglichkeiten realisierbare oder mit polizeifachlicher Erforderlichkeit begründete Verarbeitung personenbezogener Daten zulässig ist. Bereits bei der Konzeption des INPOL-Systems muss vielmehr dafür Sorge getragen werden, dass in das Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung nur soweit eingegriffen wird, wie dies im Rahmen der Erforderlichkeit für die polizeiliche Aufgabenerfüllung durch Rechtsvorschriften erlaubt wird.

Es besteht jedoch Grund zu der Sorge, dass es bei der Neugestaltung des INPOL-Systems zu falschen Weichenstellungen mit der Folge unzulässiger Verarbeitung personenbezogener Daten kommt. Die zu befürchtende Fehlentwicklung liegt darin, dass das Bundeskriminalamt und die Landeskriminalämter planen, künftig im Bundes–Kriminalaktennachweis (KAN) die „gesamte kriminelle Karriere“ jeder Person abzubilden, die aus Anlass eines INPOL-relevanten Delikts erfasst ist. Es sollen in diesen Fällen auch Daten über solche Straftaten gespeichert und zum Abruf bereit gehalten werden, die weder von länderübergreifender oder internationaler noch von besonderer Bedeutung sind.

§ 2 Abs. 1 BKAG beschränkt die Zuständigkeit des BKA (als Zentralstelle des polizeilichen Informationssystems) sowohl im präventiven als auch im repressiven Bereich auf „Straftaten mit länderübergreifender, internationaler oder erheblichen Bedeutung“. Der Wortlaut ist eindeutig. Anknüpfungspunkt und Gegenstand der Einteilung in INPOL-relevante Informationen einerseits und INPOL-irrelevante Informationen andererseits sind die „Straftaten“, nicht die einzelne Person und auch nicht das „Gesamtbild einer Person“. Der Gesetzeswortlaut bildet die Grenze der Auslegung; eine über den Wortsinn hinausgehende Anwendung verstößt gegen das Gesetz. Daher ist es unzulässig, die Frage der INPOL-Relevanz unabhängig von der konkreten einzelnen Straftat zu beurteilen. Vielmehr dürfen im Bundes-KAN nur Informationen zu solchen Straftaten verarbeitet werden, die im Einzelfall die in § 2 Abs. 1 BKAG aufgestellte Bedeutungsschwelle überschreiten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern das Bundesinnenministerium und die Innenministerien der Länder auf, von der geschilderten KAN-Erweiterung abzusehen.

Anlage 20 (zu Nrn. 1.5, 12.3)

Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 zu: Risiken und Grenzen der Videoüberwachung

Immer häufiger werden Videokameras eingesetzt, die für Zwecke der Überwachung genutzt werden können. Ob auf Flughäfen, Bahnhöfen, in Ladenpassagen, Kaufhäusern oder Schalterhallen von Banken oder anderen der Öffentlichkeit zugänglichen Einrichtungen, überall müssen Bürgerinnen und Bürger damit rechnen, dass sie auf Schritt und Tritt offen oder heimlich von einer Videokamera aufgenommen werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht darin die Gefahr, dass diese Entwicklung zu einer Überwachungsinfrastruktur führt.

Mit der Videoüberwachung sind besondere Risiken für das Recht auf informationelle Selbstbestimmung verbunden. Weil eine Videokamera alle Personen erfasst, die in ihren Bereich kommen, werden von der Videoüberwachung unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen betroffen. Erfassung, Aufzeichnung und Übertragung von Bildern sind für die Einzelnen in aller Regel nicht durchschaubar. Schon gar nicht können sie die durch die fortschreitende Technik geschaffenen Bearbeitungs- und Verwendungsmöglichkeiten abschätzen und überblicken. Die daraus resultierende Ungewissheit, ob und von wem sie beobachtet werden und zu welchen Zwecken dies geschieht, erzeugt einen latenten Anpassungsdruck. Dies beeinträchtigt nicht nur die grundrechtlich garantierten individuellen Entfaltungsmöglichkeiten, sondern auch das gesellschaftliche Klima in unserem freiheitlichen und demokratischen Gemeinwesen insgesamt. Alle Menschen haben das Grundrecht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird.

Daher müssen

- eine strenge Zweckbindung,
- eine differenzierte Abstufung zwischen Übersichtsaufnahmen, dem gezielten Beobachten einzelner Personen, dem Aufzeichnen von Bilddaten und dem Zuordnen dieser Daten zu bestimmten Personen,
- die deutliche Erkennbarkeit der Videoüberwachung für die betroffenen Personen,
- die Unterrichtung identifizierter Personen über die Verarbeitung ihrer Daten
- sowie die Löschung der Daten binnen kurzer Fristen

strikt sichergestellt werden.

Jede Einrichtung einer Videoüberwachung sollte der datenschutzrechtlichen Vorabkontrolle unterzogen werden. Das heimliche Beobachten und Aufzeichnen, die gezielte Überwachung bestimmter Personen sowie die Suche nach Personen mit bestimmten Verhaltensmustern müssen grundsätzlich verboten sein. Ausnahmen müssen im Strafprozessrecht und im Polizeirecht präzise geregelt werden. Videoüberwachung darf nicht großflächig oder flächendeckend installiert werden, selbst wenn jeder Einsatz für sich gesehen gerechtfertigt wäre. Auch ein zeitlich unbegrenzter Einsatz ohne regelmäßige Erforderlichkeitsprüfung ist abzulehnen. Der Schutz der Freiheitsrechte erfordert überdies, dass heimliches Aufzeichnen und unbefugte Weitergabe oder Verbreitung von Aufnahmen ebenso strafbewehrt sein müssen wie der Missbrauch videotechnisch gewonnener – insbesondere biometrischer – Daten und deren Abgleiche.

Dies bedeutet:

1. Bei einer gesetzlichen Regelung der Videoüberwachung durch **öffentliche Stellen** dürfen Einschränkungen nur aufgrund einer klaren Rechtsgrundlage erfolgen, die dem Grundsatz der Verhältnismäßigkeit Rechnung trägt.

– Die Voraussetzungen einer Videoüberwachung und der mit ihr verfolgte Zweck müssen eindeutig bestimmt werden. Dafür kommen **– soweit nicht überwiegende schutzwürdige Belange von Betroffenen entgegenstehen –** unter Anderem in Betracht:*)

  - *die Beobachtung einzelner öffentlicher Straßen und Plätze oder anderer öffentlich zugänglicher Orte, auf denen wiederholt Straftaten begangen worden sind, solange tatsächliche Anhaltspunkte dafür bestehen, dass dort weitere Straftaten begangen werden (Kriminalitätsschwerpunkte) und mit der Beobachtung neben der Sicherung von Beweisen eine Präventionswirkung erreicht werden kann; der Grundsatz der Verhältnismäßigkeit ist dabei strikt zu beachten. Ungezielte Verlagerungsprozesse sollten vermieden werden.*
  - *für die Verkehrslenkung nur Übersichtsaufnahmen,*
  - *der Schutz öffentlicher Einrichtungen im Rahmen der ordnungsbehördlichen Gefahrenabwehr, solange eine besondere Gefahrenlage besteht.*

– Maßnahmen im Rahmen des Hausrechts dürfen den grundsätzlich unbeobachteten Besuch öffentlicher Gebäude nicht unverhältnismäßig einschränken.

*) Die kursiv gedruckte Passage wurde bei Stimmenthaltung der Datenschutzbeauftragten der Länder Brandenburg, Bremen, Mecklenburg-Vorpommern und Nordrhein-Westfalen angenommen.

- Die Videoüberwachung ist für die Betroffenen durch entsprechende Hinweise erkennbar zu machen.
- Bildaufzeichnungen sind nur zulässig, wenn und solange sie zum Erreichen des verfolgten Zweckes unverzichtbar sind. Die Anlässe, aus denen eine Bildaufzeichnung ausnahmsweise zulässig sein soll, sind im einzelnen zu bezeichnen. Die Aufzeichnungen sind unverzüglich zu löschen, wenn sie hierzu nicht mehr erforderlich sind oder überwiegende schutzwürdige Belange von Betroffenen entgegenstehen.
- Werden die Aufnahmen einer bestimmten Person zugeordnet, ist diese zu benachrichtigen, sobald der Zweck der Speicherung dadurch nicht gefährdet wird.
- Zur Prüfung der Normeffizienz ist festzulegen, dass das jeweils zuständige Parlament jährlich über die angeordneten Maßnahmen, soweit sie mit einer Speicherung der erhobenen Daten verbunden sind, und die mit ihnen erreichten Ergebnisse unterrichtet wird.

Bei der Videoüberwachung muss in besonderer Weise den Grundsätzen der Datensparsamkeit und Datenvermeidung Rechnung getragen werden. Die Chancen, die die modernen Technologien für die Umsetzung dieser Grundsätze, insbesondere für die Reduzierung auf tatsächlich erforderliche Daten bieten, sind zu nutzen.

2. Der Gesetzgeber ist auch aufgefordert, für die Videoüberwachung **durch Private** Regelungen zu schaffen, die den für die optisch-elektronische Beobachtung durch öffentliche Stellen geltenden Grundsätzen entsprechen. Dabei muss sichergestellt werden, dass optisch-elektronische Systeme, die die Identifizierung einzelner Personen ermöglichen, nur zur Abwehr von Gefahren für Personen und zum Schutz gewichtiger privater Rechte eingesetzt werden dürfen. Die privatrechtlichen Regelungen zum Schutz des eigenen Bildes durch das Vertragsrecht, das Deliktsrecht, das Besitz- und Eigentumsrecht, das Kunsturheberrecht und die dazu ergangene Rechtsprechung reichen nicht aus.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, dass die Gesetzgeber bei der Novellierung der Datenschutzgesetze und anderer Gesetze diese Grundsätze berücksichtigen.

Anlage 21 (zu Nr. 6.2)

Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 zu: Strafverfahrensänderungsgesetz 1999 (StVÄG 1999)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen es, dass mit dem Entwurf für ein Strafverfahrensänderungsgesetz 1999 die Strafprozessordnung endlich die seit fast zwei Jahrzehnten überfälligen datenschutzrechtlichen Regelungen erhalten soll. Sie stellen jedoch fest, dass der nunmehr vorliegende Gesetzesbeschluss des Bundestages nicht alle wichtigen Forderungen des Datenschutzes erfüllt.

Darüber hinaus will der Bundesrat das Datenschutzniveau weiter absenken und hat auch zu diesem Zweck den Vermittlungsausschuss angerufen. Zu kritisieren ist, dass

- Zeuginnen und Zeugen auch bei Straftaten ohne erhebliche Bedeutung durch Öffentlichkeitsfahndung im Fernsehen oder Internet gesucht werden können,
- Zweckbindungen präventivpolizeilicher Daten, darunter auch der Erkenntnisse aus verdeckten Datenerhebungsmaßnahmen, wie z. B. einem Großen Lauschangriff oder einem Einsatz verdeckter Ermittler, völlig aufgehoben werden, so dass sie uneingeschränkt zur Strafverfolgung genutzt werden können,
- umgekehrt aber auch Informationen aus Strafverfahren über die Gefahrenabwehr hinaus uneingeschränkt zur Gefahrenvorsorge genutzt werden können,
- nicht am Verfahren beteiligte Dritte schon bei „berechtigtem Interesse“ Einsicht in Strafverfahrensakten bekommen können.

Die Datenschutzbeauftragten des Bundes und der Länder sehen den verfassungsrechtlich gebotenen Ausgleich zwischen Persönlichkeitsschutz und Interessen der Strafverfolgungsbehörden nicht mehr als gewährleistet an, falls die Vorschläge des Bundesrates Eingang in die Strafprozessordnung finden sollten. Die Datenschutzbeauftragten fordern daher den Vermittlungsausschuss auf, die Änderungsanträge zurückzuweisen. Stattdessen sind Regelungen in der Strafprozessordnung vorzusehen, die geeignet sind, bei einer effektiven Strafverfolgung die Persönlichkeitsrechte der Betroffenen angemessen zu gewährleisten.

Anlage 22 (zu Nrn. 6.1. 16.1.2)

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 26. Juni 2000 zu: Effektive parlamentarische Kontrolle von Lauschangriffen durch aussagekräftige jährliche Berichte der Bundesregierung

Die Bundesregierung hat den Bundestag jährlich über die nach Art. 13 Abs. 3 GG zur Strafverfolgung eingesetzten „Großen Lauschangriffe“ zu unterrichten. § 100e StPO konkretisiert die Berichtspflicht dahingehend, dass die Bundesregierung aufgrund von Mitteilungen der Staatsanwaltschaften der Länder den Bundestag über Anlass, Umfang, Dauer, Ergebnis und Kosten der Maßnahmen zu unterrichten hat.

Diese Berichte sollen eine laufenden parlamentarische Kontrolle dieser mit intensiven Grundrechtseingriffen verbundenen Maßnahmen ermöglichen. Der Bundestag soll aufgrund der Berichte in die Lage versetzt werden, die Angemessenheit und Eignung der Maßnahme zu überprüfen.

Diesen Anforderungen wird der erste von der Bundesregierung vorgelegte Bericht nicht in vollem Umfang gerecht. So wurde nur die Gesamtzahl der von der Anordnung Betroffenen erfasst, wobei zwischen beschuldigten und nicht beschuldigten Wohnungsinhabern unterschieden wird.

Nach § 100e Abs. 1 StPO muss über den Umfang der Maßnahme berichtet werden. Hierzu zählt die Angabe über die Anzahl aller von der Maßnahme betroffenen Personen, nicht nur der in der gerichtlichen Anordnung genannten. Von dem „Großen Lauschangriff“ ist jeder betroffen, dessen gesprochenes Wort in der Wohnung abgehört wird. Er greift auch in die grundrechtlich geschützten Rechte der am Verfahren Unbeteiligten, wie z. B. unverdächtige Familienangehörige, Bekannte, Besucherinnen und Besucher sowie sonstige Personen, die nicht selbst Wohnungsinhaber sind, ein. Dem wollte der Gesetzgeber mit der Einführung der Berichtspflicht Rechnung tragen.

Die Beschränkung der Berichtspflicht auf Wohnungsinhaber und Beschuldigte gibt nicht den wirklichen Umfang der von der Maßnahme betroffenen Personen wieder. Somit erfüllt sie den Zweck der im Grundgesetz vorgesehenen Berichtspflicht nicht.

Darüber hinaus wäre es wünschenswert, wenn – wie in den „Wire-tap-Reports“ der USA – die Anzahl der abgehörten Gespräche und die Anzahl der Gespräche, die mit dem Ermittlungsverfahren in Zusammenhang stehen, die Art der betroffenen Räume (Geschäftsräume, Wohnung, Restaurant etc.), die Anzahl und Dauer der angeordneten Verlängerungen der Maßnahme, die Zahl der Verhaftungen, Anklageerhebungen und Verurteilungen, zu denen die Maßnahme beigetragen hat, angegeben werden.

Die Länder haben nach Art. 13 Abs. 6 Satz 3 GG eine gleichwertige parlamentarische Kontrolle zu gewährleisten. Die oben genannten Forderungen gelten deshalb gleichermaßen bzw. in entsprechender Weise für die den Landesparlamenten vorzulegenden jährlichen Berichte über die nach § 100c Abs. 1 Nr. 3 StPO durchgeführten Maßnahmen bzw. über die von der Polizei zur Gefahrenabwehr veranlassten „Großen Lauschangriffe“.

Anlage 23 (zu Nr. 11.2)

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 10. Oktober 2000 zur Auftragsdatenverarbeitung durch das Bundeskriminalamt

Im Rahmen der Neukonzeption des polizeilichen Informationssystems INPOL ist geplant, neben bundesweit verfügbaren Verbunddaten auch Landesdatenbestände im Wege der Auftragsdatenverarbeitung logisch getrennt in der INPOL-Datenbank zu speichern. Zudem sollen aufgrund bilateraler Absprachen landesspezifische Informationen in bestimmtem Umfang gespeichert werden können und ebenso gegenseitige Zugriffe einzelner Länder auf die Datenbestände ermöglicht werden.

§ 2 Abs. 5 des Bundeskriminalamtgesetzes lässt grundsätzlich eine Unterstützung der Länder bei deren Datenverarbeitung auf Ersuchen, also in Einzelfällen, zu. Diese Vorschrift kann auch herangezogen werden, wenn aufgrund besonderer Dringlichkeit, wie gegenwärtig bei der Realisierung von INPOL-neu, eine zeitlich befristete Auftragsdatenverarbeitung von Landesdaten geplant ist. Hierzu sind Ende vergangenen Jahres entsprechende Beschlüsse des Arbeitskreises II und der Innenministerkonferenz gefasst worden.

Diese Entwicklung birgt aus der Sicht der Datenschutzbeauftragten die Gefahr, dass weitere Beschlüsse folgen werden, die die dauerhafte Speicherung von Landesdaten beim BKA begründen; bereits jetzt sind Tendenzen deutlich, die zentralisierte Speicherung der Daten auch zur Erleichterung der gegenseitigen Zugriffe auf Landesdaten zu nutzen.

Die Notwendigkeit der zentralen Datenspeicherung beim Bundeskriminalamt wird im wesentlichen mit Kosten- und Zeitargumenten begründet. Diese sind jedoch aus datenschutzrechtlicher Sicht nicht geeignet, eine Erweiterung der zentralen Datenverarbeitung beim Bundeskriminalamt zu begründen.

Die dauerhafte zentrale Datenhaltung beim BKA würde die informationelle Trennung von Landesdaten und Verbunddaten aufweichen; die in § 2 Abs. 1 BKA-Gesetz statuierte Schwelle, dass nur Daten über Straftaten von länderübergreifender, internationaler oder sonst erheblicher Bedeutung beim BKA verarbeitet werden dürfen, würde schleichend umgangen.

Eine dauerhafte zentrale Landesdatenhaltung beim Bundeskriminalamt beinhaltet eine neue, bei der augenblicklichen Rechtslage unakzeptable Qualität polizeilicher Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern dazu auf, die für die Datenverarbeitung beim Bundeskriminalamt gesetzlich gezogenen Grenzen strikt zu beachten. Sie appellieren an die Innenminister/-senatoren von Bund und Ländern, an den bisherigen Beschlüssen festzuhalten und die Polizeien der Länder, wie ursprünglich geplant, aufzufordern, unverzüglich eigene Datenverarbeitungsverfahren zu entwickeln. Bis zur Realisierung dieser Verfahren könnte allenfalls eine übergangsweise Lösung als Auftragsdatenverarbeitung unter Wahrung datenschutzrechtlicher Anforderungen ermöglicht werden. Daneben steht das Angebot des Bundeskriminalamtes, kostenlos Software von INPOL-neu zur Verfügung zu stellen. Diese Lösung würde auch das vorgetragene Kostenargument entkräften.

Anlage 24 (zu Nr. 2.1.1)

Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000 zu: Novellierung des BDSG

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an Bundestag und Bundesrat, das Gesetzgebungsverfahren eines novellierten Bundesdatenschutzgesetzes zügig und ohne Abstriche zum Abschluss zu bringen. Damit wird die längst überfällige Anpassung des deutschen Datenschutzrechts an die Vorgaben der EG-Richtlinie vorgenommen. Die Novelle enthält verschiedene innovative Ansätze, insbesondere das Gebot zur Datenvermeidung und Datensparsamkeit bei der Systemgestaltung (Systemdatenschutz – § 3a E-BDSG) und die Einführung des Datenschutzaudits (§ 9a), die von den Datenschutzbeauftragten schon seit langem befürwortet werden.

Sowohl der Systemdatenschutz als auch das Datenschutzaudit werden die Durchsetzung datenschutzfreundlicher Lösungen im Wettbewerb erleichtern und tragen auf diese Weise zur Selbstregulierung des Marktes bei. Das Datenschutzaudit fügt sich in die bewährten Strukturen des betrieblichen Datenschutzes ein und ermöglicht es den Unternehmen, datenschutzkonforme Angebote und Verhaltens- weisen nachprüfbar zu dokumentieren und damit einen Wettbewerbsvorsprung zu gewinnen.

Die Konferenz fordert den Bundesrat auf, die Aufnahme des Datenschutzaudit in das BDSG nicht zu blockieren. Sie geht weiter davon aus, dass die angekündigte zweite Stufe der Novellierung des BDSG noch in dieser Legislaturperiode realisiert wird, und erklärt ihre Bereitschaft, hieran konstruktiv mitzuwirken.

Anlage 25 (zu Nr. 6.3)

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 zu: DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen

In der Strafprozessordnung ist der Einsatz der DNA-Analyse zur vorbeugenden Verbrechensbekämpfung nur mit richterlicher Anordnung vorgesehen.

In einigen deutschen Ländern werden DNA-Analysen ohne richterliche Anordnung gestützt allein auf die Einwilligung der Betroffenen durchgeführt. Soweit die dabei erhobenen Daten zum Zweck der Identitätsfeststellung in künftigen Strafverfahren genutzt werden sollen, bedürfen DNA-Analysen nach der klaren gesetzlichen Regelung des DNA-Identitätsfeststellungsgesetzes jedoch einer richterlichen Anordnung. Der Richter oder die Richterin hat u. a. die Prognose zu treffen, ob Grund zur Annahme besteht, dass gegen Betroffene künftig erneut Strafverfahren wegen des Verdachts erheblicher Straftaten zu führen sind. Wenn nunmehr auch DNA-Analysen gespeichert und zum Zweck der zukünftigen Strafverfolgung genutzt werden dürfen, die auf freiwilliger Basis – also ohne richterliche Anordnung – erstellt worden sind, und dies sogar durch die Errichtungsanordnung für die DNA-Analyse-Datei beim BKA festgeschrieben werden soll, werden damit die eindeutigen gesetzlichen Vorgaben des DNA-Identitätsfeststellungsgesetzes unterlaufen.

Die von Strafgefangenen erteilte Einwilligung zur Entnahme, Analyse und Speicherung kann keine Grundlage für einen derartigen Eingriff sein. Eine wirksame Einwilligung setzt voraus, dass sie frei von psychischem Zwang freiwillig erfolgt. Da Strafgefangene annehmen können, dass die Verweigerung der Einwilligung Auswirkungen z. B. auf die Gewährung von Vollzugslockerungen hat, kann hier von Freiwilligkeit keine Rede sein. Ausschlaggebend für die Beurteilung der Freiwilligkeit einer Einwilligung ist die subjektive Einschätzung des Betroffenen. Auch wenn im Einzelfall die Weigerung von Strafgefangenen, sich einer DNA-Analyse zu unterziehen, die Entscheidung über Vollzugslockerungen nicht beeinflusst, ist dennoch davon auszugehen, dass die Befürchtung, die Verweigerung habe negative Folgen, die freie Willensentscheidung beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder halten deshalb die Praxis einiger Länder, DNA-Analysen – abweichend von den gesetzlich vorgesehenen Verfahren – systematisch auf der Grundlage von Einwilligungen durchzuführen, für eine Umgehung der gesetzlichen Reglung und damit für unzulässig. Die möglicherweise mit der Beantragung richterlicher Anordnungen verbundene Mehrarbeit ist im Interesse der Rechtmäßigkeit der Eingriffsmaßnahmen hinzunehmen. Die Datenschutzbeauftragten fordern daher, DNA-Analysen zum Zweck der Identitätsfeststellung in künftigen Strafverfahren nur noch auf der Grundlage richterlicher Anordnungen durchzuführen.

Anlage 26 (zu Nrn. 25.2.1, 25.2.2)

Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 12./13. Oktober 2000 zu: Datenschutzrechtliche Konsequenzen aus der Entschlüsselung des menschlichen Genoms

Bei der Entschlüsselung des menschlichen Genoms sind in den letzten Monaten wohl entscheidende Durchbrüche gelungen. Für mehr als 20, oft vererbliche Krankheiten sind bereits Gentests zu erwerben, mit denen in Labors analysiert werden kann, ob eine Erkrankung vorliegt bzw. in welchem Umfang ein Erkrankungsrisiko besteht. Viele dieser Krankheiten sind allerdings bisher nicht heil- oder behandelbar.

Gentechnische Untersuchungen beim Menschen eröffnen den Zugang zu höchstpersönlichen und hochsensiblen Informationen in einem Maße, das die Intensität bisheriger personenbezogener Informationen ganz erheblich übersteigt. Durch den genetischen Einblick in den Kernbereich der Privatsphäre, etwa in Gesundheitsdisposition, Anlagen der Persönlichkeitsstruktur oder den voraussichtlichen Lebensverlauf, entsteht eine ganz neue Qualität des Wissens und des Offenlegens von persönlichsten Daten. Sowohl für die Betroffenen als auch für dritte Personen, insbesondere Familienangehörige, ist es von entscheidender Bedeutung, ob und inwieweit sie selbst und wer außer ihnen von den Ergebnissen Kenntnis bekommt. Davor steht die Frage, ob und aus welchen Anlässen überhaupt genetische Untersuchungen am Menschen vorgenommen werden dürfen. Zur informationellen Selbstbestimmung gehört auch das Recht auf Nichtwissen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass für die Zulässigkeit gentechnischer Untersuchungen beim Menschen und für den Umgang mit den dabei gewonnenen Informationen sehr schnell klare und verbindliche Prinzipien entwickelt werden, um auch die informationelle Selbstbestimmung in diesem Kernbereich zu sichern und zugleich eine „genetische Diskriminierung“ bei der Gewinnung oder Verwendung genetischer Informationen, etwa im Arbeitsverhältnis oder beim Abschluss von Versicherungsverträgen zu verhindern. Auf der Grundlage dieser und in der „Entschließung über Genomanalyse und informationelle Selbstbestimmung“ vom 26. Oktober 1989 formulierten Grundsätze wird die Konferenz an der Ausgestaltung mitwirken.

Die Datenschutzbeauftragten erinnern an ihre Grundsätze aus der Entschließung von 1989 bezüglich der Genomanalyse:

1. Die Genomanalyse darf grundsätzlich nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden; ausgenommen sind Straf- und Abstammungsverfahren.

2. Die jederzeit widerrufliche Einwilligung muss sich auch auf die weitere Verwendung der gentechnischen Informationen erstrecken. Im Falle eines Widerrufs sind die gewonnnen Informationen zu löschen oder an den Betroffenen herauszugeben.

3. Jede Genomanalyse muss zweckorientiert vorgenommen werden. Es ist diejenige genomanalytische Methode zu wählen, die keine oder die geringste Menge an Überschussinformationen bringt. Überschussinformationen sind unverzüglich zu vernichten.

4. Es ist zu prüfen, inwieweit genomanalytische Untersuchungsmethoden einer staatlichen Zulassung bedürfen. Für DNA-Sonden ist dies jedenfalls zu bejahen.

5. Die Genomanalyse im gerichtlichen Verfahren muss auf die reine Identitätsfeststellung beschränkt werden; es dürfen keine genomanalytischen Methoden angewandt werden, die Überschussinformationen zur Person liefern. Die Nutzung der Genomanalyse im Strafverfahren setzt eine normenklare gesetzliche Ermächtigung voraus. Präzise Regelungen müssen u. a. sicherstellen, dass genomanalytische Befunde einer strengen Zweckbindung unterworfen werden.

6. Im Arbeitsverhältnis sind die Anordnung von Genomanalysen oder die Verwendung ihrer Ergebnisse grundsätzlich zu verbieten. Ausnahmen bedürfen der gesetzlichen Regelung. Eine bloße Einwilligung des Arbeitnehmers ist wegen der faktischen Zwangssituation, der er im Arbeitsleben häufig unterliegt, nicht ausreichend.

7. Genomanalysen im Versicherungswesen sind grundsätzlich nicht erforderlich und mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschließen, unvereinbar. Dies sollte durch eine Klarstellung im Versicherungsvertragsgesetz deutlich gemacht werden.

8. Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, bei denen eine Schädigung heilbar ist oder die zu einer so schwerwiegenden Gesundheitsschädigung des Kindes führen würden, dass ein Schwangerschaftsabbruch straffrei bliebe. Reihenuntersuchungen an Neugeborenen dürfen sich nur auf solche Erbkrankheiten erstrecken, die bei frühzeitiger Erkennung eines genetischen Defekts geheilt oder zumindest spürbar therapeutisch begleitet werden können. Die Eltern müssen nach umfassender fachkundiger Beratung in voller Freiheit über die Anwendung genomanalytischer Methoden entscheiden

können. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck, muss vermieden werden. Die informationelle Selbstbestimmung Dritter, zu der auch das Recht auf Nichtwissen gehört, muss berücksichtigt werden.

Demnächst werden nicht nur – wie bisher – Gensequenzen aufgedeckt und verglichen, sondern auch die mit dem Genom verbundenen Wirkungszusammenhänge für die menschliche Gesundheit und für die Persönlichkeitsstruktur entschlüsselt werden können.

Anlage 27 (zu Nr. 31.4)

Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 zu: Data Warehouse, Data Mining und Datenschutz

Mit der ständig zunehmenden Leistungsfähigkeit der Informations- und Kommunikationstechnik wächst die Menge gespeicherter personenbezogener Daten in Wirtschaft und Verwaltung weiter an. Zunehmend kommen automatisierte Verfahren zum Einsatz, die das gesammelte Datenmaterial effektiv verwalten und analysieren. Im „Data Warehouse“ werden alle verwendbaren Daten in einem einheitlichen Datenpool losgelöst von ihrer ursprünglichen Verwendung zusammengeführt. „Data Mining“ bietet Werkzeuge, die die scheinbar zusammenhanglosen Daten nach noch nicht bekannten, wissenswerten Zusammenhängen durchsuchen, Daten aufspüren, kombinieren und neue Informationen zur Verfügung stellen.

Diese Entwicklung schafft neben Vorteilen neue Gefahren und Risiken für das Grundrecht auf informationelle Selbstbestimmung und für den Schutz der Privatheit: Persönlichkeitsprofile, automatisierte Vorhersagen von Verhaltens- und Handlungsweisen, Manipulationsmöglichkeiten und zu lange Speicherung sind befürchtete Gefahren.

Die Konferenz der Datenschutzbeauftragten weist auf Folgendes hin:

- Nach dem grundrechtlichen Gebot der Zweckbindung dürfen personenbezogene Daten nur im Rahmen der gesetzlich zugelassenen Zwecke oder der gegenseitigen Vereinbarungen verwendet werden. Eine personenbezogene Speicherung in einem allgemein verwendbaren Data Warehouse entfernt sich vom ursprünglichen Verwendungszweck und stellt eine Speicherung auf Vorrat ohne Zweckbindung dar. Personenbezogene Daten, die bei der öffentlichen Verwaltung vorhanden sind, sind in ihrer Zweckbestimmung grundrechtlich geschützt und dürfen nicht für unbestimmte Zwecke in einem „Daten-Lagerhaus“ gesammelt werden.
- Eine Zweckänderung ist nur mit Einwilligung der Betroffenen zulässig, nachdem diese über die Tragweite der Einwilligung aufgeklärt worden sind. Eine Einwilligung in unbestimmte und zeitlich unbegrenzte Zweckänderungen ist deswegen unwirksam.
- Gestaltung und Auswahl von Datenverarbeitungs-Systemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Anonyme und pseudonyme Verfahren sind datenschutzrechtlich unbedenklich.
- Verfahren sind so zu gestalten, dass die Betroffenen hinreichend unterrichtet werden, damit sie jederzeit die Risiken abschätzen und ihre Rechte wahrnehmen können. Sie haben insbesondere das Recht, eine erteilte Einwilligung jederzeit zurückzuziehen.
- Die gesetzlichen Speicherfristen, nach deren Ablauf die Daten zwingend archiviert oder gelöscht werden müssen, sind strikt zu beachten. Deswegen ist die Einrichtung von permanenten „Daten-Lagerhäusern“ rechtswidrig.
- Die Europäische Datenschutzrichtlinie spricht grundsätzlich jeder Person das Recht zu, keiner belastenden automatisierten Einzelentscheidung unterworfen zu werden (Art. 15). „Data Mining“ ist ein Instrument, das für solche Entscheidungen herangezogen werden kann.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ruft die Hersteller und Anwender von „Data Warehouse“- und „Data Mining“-Verfahren dazu auf, solchen Programmen den Vorzug zu geben, die unter Einsatz von datenschutzfreundlichen Technologien die Speicherung von personenbezogenen Daten durch Anonymisierung oder Pseudonymisierung vermeiden.

Anlage 28 (zu Nr. 33.4.2)

Dienstanweisung zum elektronischen Dokumentenaustausch in der Dienststelle des Bundesbeauftragten für den Datenschutz (DA-E-Mail)

Inhalt

1. Nutzung des E-Mail-Systems

1.1 Zielvorstellung

Es wird erwartet, dass anstelle des papiergebundenen Schriftverkehrs der „elektronische" Dokumentenaustausch innerhalb der Dienststelle des BfD und auch zwischen BfD und externen Stellen wegen der damit verbundenen Qualitätsverbesserung und des Zeitgewinns bei der Zustellung der Dokumente stärker genutzt wird; damit wird immer mehr auf den Versand von Papierdokumenten verzichtet werden.

1. 2 Sicherheit bei der Übertragung

Die Nutzung des E-Mail-Systems wirft auch Sicherheitsprobleme auf.

Bei Sendungen, die den IVBB verlassen – insbesondere solchen ins **Internet** – besteht ein erhöhtes Risiko, dass die adressierte **Stelle** (oder **Person**!) die E-Mail nicht erhält, dass unbefugte Dritte Kenntnis von deren Inhalt erlangen, und dass der Mailinhalt verändert wird. Besonders problematisch sind die mit der Mail versandten Anlagen, da hier leicht Computer-Viren versteckt sein können.

Hinreichende Sicherheit besteht insoweit lediglich dann, wenn der Übertragungsweg vom Absender zum Empfänger ausschließlich im IVBB erfolgt; hier werden die Daten zwischen den entsprechenden Mailservern verschlüsselt übertragen. Innerhalb des jeweiligen lokalen Netzwerkes werden die Daten in der Regel unverschlüsselt verarbeitet (d. h. es liegt keine Ende-zu-Ende-Verschlüsselung vor).

Darüber hinaus treten Sicherheitsprobleme grundsätzlicher Art auf, die durch eine ordnungsgemäße Handhabung des Systems minimiert werden können.

Die elektronische Kommunikation wird für Zwecke der Datensicherheit und der Datenschutzkontrolle protokolliert. Eine Nutzung der Daten für andere Zwecke erfolgt nicht.

1.3 Netz

Alle PC-Arbeitsplätze der Dienststelle sind über ein Netzwerk in die Kommunikationsinfrastruktur eingebunden und über die elektronische Post erreichbar. Damit kann elektronische Post von allen Bearbeitern/-innen

→ intern über das hauseigene Netzwerk und

→ extern über den IVBB

versendet und empfangen werden.

1.4 Informationsverbund Berlin-Bonn (IVBB)

Durch die Anbindung an den IVBB können alle Ressorts, einzelne Behörden des Geschäftsbereichs und eine Vielzahl weiterer externer Kommunikationspartner erreicht werden. Eine Zusammenstellung der Teilnehmer am IVBB befindet sich auf der Web–Site des IVBB (http://service.ivbb.bund.de/ivbb/aktuelles/rufnummern.html). Eine Auswahl von dienstlichen Kommunikationsadressen steht im Globalen Adressbuch des Mail-Systems (MS-Outlook) zur Verfügung und wird ständig aktualisiert und erweitert. Zur Sicherstellung der direkten Erreichbarkeit durch Externe werden Kommunikationsadressen im IVBB veröffentlicht.

1.5 Dokumentenformate

Das für Anlagen verwendete Dokumentenformat (z. B. MS-Word, RTF*)-Format) ist ggf. mit dem Empfänger abzustimmen bzw. ihm in der E-Mail mitzuteilen. Dabei ist grundsätzlich das RTF-Format zu verwenden (Empfehlung des BSI).

2. Versand elektronischer Dokumente

2.1 Allgemeines

Elektronisch gespeicherte Dokumente können an alle mit E-Mail erreichbaren Empfänger versendet werden.

Das genutzte Dokumentenformat der Anlagen (soweit nicht das RTF-Format verwendet wird) ist dem Empfänger in der E-Mail mitzuteilen.

Bei externer Versendung ist – soweit im Einzelfall geboten – eine „Empfangsbestätigung" anzufordern, auszudrucken und mit zur Akte zu nehmen.

Soll ein Dokument, das mit der E-Mail versandt wurde, zusätzlich per Post versandt werden, ist dies dem Empfänger mitzuteilen.

2.2 Zulässigkeit

Es ist grundsätzlich zulässig, Dokumente mit Hilfe der elektronischen Post an interne und externe Empfänger als E-Mail zu versenden. Die Verantwortung für den ordnungsgemäßen Versand obliegt dem/der zuständigen Bearbeiter(in).

Dokumente mit der Einstufung VS-NfD dürfen nur innerhalb des IVBB versendet werden. Dies gilt auch für die Versendung sonstiger besonders schutzwürdiger oder personenbezogener Daten

Soweit nicht vom Einverständnis des Empfängers ausgegangen werden kann, dürfen an Ziele außerhalb des IVBB nur E-Mails gesendet werden, deren Inhalt so wenig sensibel ist, dass das Risiko einer Kenntnisnahme durch Dritte in Kauf genommen werden könnte. Dies kann beispielhaft für den **Zwischenbescheid** an einen Petenten gelten, der sich per E-Mail an die Dienststelle gewandt hat; soweit im Einzelfall geboten, erhält er den Schlussbescheid – mit Details in seiner Angelegenheit – dann mit der Briefpost.

*) RTF = Rich Text Format

Unzulässig ist:

a) Die elektronische Versendung von Informationen und Dokumenten an Behörden und Dritte,

– die höher als VS-NfD eingestuft sind (dies gilt auch bei einer Versendung innerhalb des IVBB),

– welche **außerhalb des IVBB** versandt werden sollen und gemäß VS-Anweisung eingestuft sind oder einem besonderen Schutz unterliegen (z. B. sensible Personal- und Sozialdaten).

b) Die Versendung von Programmen sowie die Ausführung empfangener Programme, soweit diese als solche erkennbar sind.

2.3 Adressierung

2.3.1 Organisations-/Funktionsbezogene Adressierung

Im behördlichen Dokumentenverkehr ist grundsätzlich die Adresse der federführenden Organisationseinheit zu verwenden. Ist diese nicht bekannt, ist die Behörde/Organisation allgemein zu adressieren. Eine personenbezogene Adressierung sollte nur in Ausnahmefällen erfolgen.

2.3.2 X.400-Mailadressen

Verfügt ein Adressat sowohl über eine X.400-Mailadresse als auch über eine Internet-Adresse, ist grundsätzlich die X.400-Mailadresse zu verwenden.

Die Aufnahme von X.400-Mailadressen im globalen Adressbuch erfolgt nur auf Antrag an die Anwenderberatung. Die Aufnahme und Pflege von X.400-Mailadressen im persönlichen Adressbuch obliegt dem Anwender.

2.3.3 Internet-Mailadressen

Die Aufnahme von Internet-Mailadressen im globalen Adressbuch erfolgt nur auf Antrag an die Anwenderberatung. Die Aufnahme und Pflege von Internet-Mailadressen im persönlichen Adressbuch obliegt dem Anwender.

2.4 Behandlung elektronischer Postausgänge

2.4.1 Dokumentangaben

Elektronische Dokumente enthalten grundsätzlich folgende Angaben:

→ Behörden-/Organisationsname,

→ Anschrift,

→ Geschäftszeichen,

→ Datum,

→ Bearbeitername(n),

→ Adressen/Rufnummern für Telekommunikationsdienste.

2.4.2 Sachgerechter Betreff

Im Betreffsfeld der elektronischen Post ist ein sachgerechter Betreff einzutragen, ggf. der des zu versendenden Anlagedokuments.

2.4.3 Behandlung von als Anlage beigefügter Word-Dokumente

Bei der Versendung von Dokumenten (sowohl Word- als auch RTF-Format) ist zu beachten, dass diese unsichtbare Zeichen – z. B. vorige Textversionen oder Verfügungspunkte – enthalten können. Sollen diese nicht übertragen werden, sind die Dokumente vor dem Versand entsprechend zu prüfen und zu überarbeiten

2.4.4 Schlusszeichnung

Bis zur Einführung der elektronischen Unterschrift ersetzt der Zusatz „gez.“ vor der Namensangabe des Schlusszeichnenden in der elektronischen Reinschrift die Unterschrift/Beglaubigung. Falls aus Lesbarkeitsgründen erforderlich, ist das Reinschriftdokument nach der „Schlusszeichnung“ und dem Versand mit der Absendemaske (Versandinformationen) auszudrucken und zu den Akten zu nehmen.

3 Eingang elektronischer Dokumente

3.1 Zustellung von Posteingängen

Elektronische Post kann von allen vernetzten IT–Nutzern/Nutzerinnen empfangen werden. Für jede(n) IT-Nutzer(in) ist ein persönliches Benutzerpostfach, für jede Arbeitseinheit ein „Referatspostfach“ eingerichtet. Die Bezeichnung für das Referatspostfach bildet sich nach der Regel „refX@bfd.bund400.de“ (z. B.ref3@bfd.bund400.de). Zugriffsberechtigt auf die Referatspostfächer sind alle Referatsangehörigen.

Ankommende Dokumente gehen der Adressierung entsprechend unmittelbar bei dem Empfänger ein.

Die Kommunikationspartner sind dahingehend zu informieren, dass E-Mails grundsätzlich an das Referatspostfach zu schicken sind.

Für alle elektronisch eingehenden Dokumente, die vom Mail-System nicht automatisch an einen definierten Adressaten weitervermittelt werden können, z. B. wegen fehlerhafter Namensschreibweise oder weil der Adressat aus der Dienststelle ausgeschieden ist, ist eine zentrale Posteingangsstelle für elektronische Post („Poststelle“) eingerichtet.

3.2 Eingangsüberwachung

Die elektronischen Postfächer sind mehrfach täglich auf Eingänge zu überprüfen. Fehladressierte elektronische

Post ist, soweit das zuständige Referat ersichtlich ist oder nach dem Geschäftsverteilungsplan ermittelt werden kann, unverzüglich an das betreffende Referatspostfach weiterzuleiten; andernfalls ist sie an die Poststelle zur Zuständigkeitsermittlung weiterzuleiten.

3.3 Weiterleitung bei Abwesenheit

Auch bei Abwesenheit ist sicherzustellen, dass eine eingegangene E-Mail entsprechend der Wichtigkeit ihres Inhaltes bearbeitet werden kann. Dazu ist ein(e) Vertreter(in) zu benennen und die Funktion der automatischen Weiterleitung („Abwesenheitsassistent“) zu aktivieren. Die elektronische Post wird dann **zusätzlich** an den/die jeweilige(n) Vertreter(in) weitergeleitet.

Alternativ kann der Absender durch eine automatische Antwort mit Hilfe des Abwesenheitsassistenten aufgefordert werden, die Mitteilung erneut an das Referatspostfach zu senden.

Im Falle nicht vorhersehbarer Abwesenheit, z. B. wegen Krankheit, richtet die Systemverwaltung bei unabweisbarem Bedarf dem/der Vertreter(in) für den PC des Abwesenden ein neues Passwort ein; mit dessen Hilfe sichtet der Vertreter bereits eingegangene E-Mails und aktiviert den Abwesenheitsassistenten.

3.4 Behandlung elektronischer Posteingänge

Der/die zuständige Bearbeiter(in) ist für die ordnungsgemäße Behandlung elektronischer Posteingänge verantwortlich.

Können Dokumente nicht mit den am Arbeitsplatz zur Verfügung stehenden Hilfsmitteln geöffnet und gelesen werden, so sind sie zur Prüfung an die Systemverwaltung zu leiten.

Eingänge bei der Poststelle sowie bei den persönlichen Bearbeiterpostfächern werden an das Referatspostfach des zuständigen Referates weitergeleitet.

3.4.1 Eingangsempfänger; Vorlage an die Hausleitung

Eingangsempfänger i. S. v. § 17 GGO I ist der/die Referatsleiter/-in. Damit ist er/sie u. a. verantwortlich, dass wichtige Eingänge rechtzeitig dem Geschäftsgang zugeführt werden.

Er/Sie sichtet mehrmals täglich die Eingänge im Referatspostfach, druckt alle Eingänge, deren Kenntnis für die Aufgabenerfüllung des BfD relevant ist, aus und lässt sie mit Geschäftsgangvermerk „GG“ unverzüglich der Eingangsmappe der Hausleitung beifügen („Geschäftsgang“); ausgenommen sind Eingänge von geringer Bedeutung (z. B. Druckschriftenanforderungen, Werbung usw.). Bei umfangreichen Eingängen druckt er/sie nur diejenigen Seiten aus, die der Leitung das Erkennen des Sachverhaltes ermöglichen, z. B. die Eingangsseite der E-Mail und das Titelblatt des Anlagedokumentes.

Mit der Sichtung und dem Ausdruck der Eingänge kann der/die Referatsleiter/-in eine(n) Mitarbeiter(in) des Referates beauftragen.

3.4.2 Speicherung im elektronischen Postsystem

E-Mails dürfen im elektronischen Postsystem nur solange gespeichert werden, wie dies für die Aufgabenerfüllung erforderlich ist. Die Notwendigkeit der Speicherung ist regelmäßig zu prüfen. Nicht mehr benötigte E-Mails sind zu löschen.

3.5 Sicherheitsrisiken; Computer-Viren

Ist einer eingehenden E-Mail ein Computer-Virus anhängig, wird dieser in den meisten Fällen durch den Virenscanner des lokalen E-Mail-Rechners erkannt. Die E-Mail wird in ein temporäres Verzeichnis gespeichert und kann vom Nutzer nicht mehr geöffnet werden. Gleichzeitig erfolgt rechnerseitig eine Alarmmeldung an die Systemverwaltung. Die Systemverwaltung ist dann in der Lage, die „verseuchte“ Mail zu löschen.

Zwecks Erhöhung der Sicherheit wird die eingehende Mail ein weiteres Mal durch den zentralen Server auf Computer-Viren überprüft. Bei einem erkannten Computer-Virus wird die Systemverwaltung auch hier unterrichtet. Der Ablauf erfolgt wie oben beschrieben.

Der Absender der virenbehafteten Mail sollte über den gefundenen Computer-Virus informiert werden. Die Antwortfunktion darf dabei nicht genutzt werden.

Mit der elektronischen Post (E-Mail) übersandte Programme dürfen nicht zur Ausführung gebracht werden. Die Anwenderberatung ist unverzüglich über entsprechende Eingänge zu unterrichten. Dies gilt auch bei sonstigen ungewöhnlichen Vorgängen die auf ein IT-Sicherheitsproblem schließen lassen (z. B. beim Öffnen empfangener Dokumente). In diesen Fällen ist die Eingangsmaske auszudrucken und die Absenderangaben sind zu dokumentieren.

Anlage 29 (zu Nr. 10.11.1)

SCHUFA-Klausel zu Telekommunikationsanträgen

Ich willige ein, dass die Firma*) der SCHUFA GmbH Daten über die Beantragung, Aufnahme und Beendigung dieses Telekommunikationsvertrages übermittelt und Auskünfte über mich von der SCHUFA erhält.

Unabhängig davon wird die Firma*) der SCHUFA auch Daten aufgrund nichtvertragsgemäßen Verhaltens (z. B. Forderungsbetrag nach Kündigung, Kartenmissbrauch) übermitteln. Diese Meldungen dürfen nach dem Bundesdatenschutzgesetz nur erfolgen, soweit dies nach Abwägung aller betroffenen Interessen zulässig ist.

Die SCHUFA speichert und übermittelt die Daten an ihre Vertragspartner im europäischen Binnenmarkt, um diesen Informationen zur Beurteilung der Kreditwürdigkeit von natürlichen Personen zu geben. Vertragspartner der SCHUFA sind vor allem Kreditinstitute, Kreditkarten- und Leasinggesellschaften. Daneben erteilt die SCHUFA Auskünfte an Handels-, Telekommunikations- und sonstige Unternehmen, die Leistungen und Lieferungen gegen Kredit gewähren. Die SCHUFA stellt personenbezogene Daten nur zur Verfügung, wenn ein berechtigtes Interesse hieran im Einzelfall glaubhaft dargelegt wurde. Zur Schuldnerermittlung gibt die SCHUFA Adressdaten bekannt. Bei der Erteilung von Auskünften kann die SCHUFA ihren Vertragspartnern ergänzend einen aus ihrem Datenbestand errechneten Wahrscheinlichkeitswert zur Beurteilung des Kreditrisikos mitteilen (Score-Verfahren).

Ich willige ein, dass im Falle eines Wohnsitzwechsels die Daten an die dann zuständige SCHUFA übermittelt werden.

Ich kann Auskunft bei der SCHUFA über die mich betreffenden gespeicherten Daten erhalten. Weitere Informationen über das SCHUFA-Auskunfts- und Score-Verfahren enthält eine Broschüre, die auf Wunsch zur Verfügung gestellt wird.

Die Adresse der SCHUFA lautet:.....

_____

Unterschrift

*) zu personalisieren

Anlage 30 (zu Nrn. 10.11.1, 31.1.1)

SCHUFA-Klausel

Ich willige ein, dass die Bank der SCHUFA GmbH Daten über die Beantragung, die Aufnahme und Beendigung dieser Kontoverbindung übermittelt.

Unabhängig davon wird die Bank der SCHUFA auch Daten aufgrund nicht vertragsgemäßen Verhaltens (z. B. Forderungsbetrag nach Kündigung, Scheck- und Kreditkartenmissbrauch) übermitteln. Diese Meldungen dürfen nach dem Bundesdatenschutzgesetz nur erfolgen, soweit dies nach der Abwägung aller betroffenen Interessen zulässig ist.

Insoweit befreie ich die Bank zugleich vom Bankgeheimnis.

Die SCHUFA speichert und übermittelt die Daten an ihre Vertragspartner im europäischen Binnenmarkt, um diesen Informationen zur Beurteilung der Kreditwürdigkeit von natürlichen Personen zu geben. Vertragspartner der SCHUFA sind vor allem Kreditinstitute sowie Kreditkarten- und Leasinggesellschaften. Daneben erteilt die SCHUFA auch Auskünfte an Handels-, Telekommunikations- und sonstige Unternehmen, die Leistungen und Lieferungen gegen Kredit gewähren. Die SCHUFA stellt personenbezogene Daten nur zur Verfügung, wenn ein berechtigtes Interesse hieran im Einzelfall glaubhaft dargelegt wurde. Zur Schuldnerermittlung gibt die SCHUFA Adressdaten bekannt. Bei der Erteilung von Auskünften kann die SCHUFA ihren Vertragspartnern ergänzend einen aus ihrem Datenbestand errechneten Wahrscheinlichkeitswert zur Beurteilung des Kreditrisikos mitteilen (Score-Verfahren).

Ich willige ein, dass im Falle eines Wohnsitzwechsels die Daten an die zuständige SCHUFA übermittelt werden.

Ich kann Auskunft bei der SCHUFA über die mich betreffenden gespeicherten Daten erhalten. Weitere Informationen über das SCHUFA-Auskunfts- und Score-Verfahren enthält eine Broschüre, die auf Wunsch zur Verfügung gestellt wird.

Die Adresse der SCHUFA lautet: .....

_____

Unterschrift

Anlage 31 (zu Nr. 29.2)

Merkblatt „Postgeheimnis und Datenschutz“

Unternehmen, die Postdienstleistungen für die Öffentlichkeit erbringen oder an der Erbringung solcher Dienstleistungen mitwirken, sind hinsichtlich ihrer Postdienstleistungen zur Wahrung des Postgeheimnisses verpflichtet. Außerdem unterliegen sie den besonderen datenschutzrechtlichen Regelungen des Postgesetzes (PostG), der Postdienstunternehmen-Datenschutzverordnung (PDSV) und des Bundesdatenschutzgesetzes (BDSG).

Postgeheimnis

Das Postgeheimnis ist in **§ 39 PostG** näher geregelt. Nach dieser Vorschrift unterliegen dem Postgeheimnis die näheren Umstände des Postverkehrs bestimmter natürlicher oder juristischer Personen sowie der Inhalt von Postsendungen. Zu den näheren Umständen des Postverkehrs gehören alle Verbindungsdaten, die nicht den Inhalt einer konkreten Postsendung selbst betreffen, wie z. B. Name und Anschrift des Absenders und Empfängers, Ort und Zeit der Aufgabe der Postsendung, Art und Weise der Inanspruchnahme der Dienstleistung. Es muss sich um Umstände handeln, die in einem unmittelbaren Zusammenhang mit dem Postverkehr stehen. Der Schutz des Postgeheimnisses bezieht sich auf alle Postdienstleistungen im Sinne des § 4 Nr. 1 PostG. Dies sind die Beförderung von

- Briefsendungen,
- adressierten Paketen, deren Einzelgewicht 20 Kilogramm nicht übersteigt,
- Büchern, Katalogen, Zeitungen oder Zeitschriften,

unabhängig davon, ob es sich um offene oder verschlossene Sendungen handelt.

Dementsprechend ist es den Unternehmen und deren Mitarbeitern untersagt, sich oder anderen über das für die Erbringung der Postdienste erforderliche Maß hinaus Kenntnis vom Inhalt von Postsendungen oder den näheren Umständen des Postverkehrs zu verschaffen. Eine Ausnahme von diesem Verbot ist nur in den Fällen des § 39 Abs. 4 Nr. 1–4 PostG möglich. Allerdings sind die Ausnahmetatbestände sehr eng auszulegen und stehen generell unter der Voraussetzung der Erforderlichkeit. Dies bedeutet, dass die genannten Maßnahmen nur in Betracht kommen, wenn und soweit keine andere Möglichkeit besteht, die erstrebten Informationen bzw. Ziele zu erreichen.

Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort. Verstöße gegen das Postgeheimnis können gemäß § 206 StGB mit einer Geld- oder Freiheitsstrafe geahndet werden. Das Postgeheimnis gilt auch innerhalb des Unternehmens.

Datenschutz

Für die Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung bei Postdienstunternehmen finden zunächst die bereichsspezifischen Datenschutzbestimmungen des PostG und der PDSV Anwendung. Soweit die PDSV keine anderen Regelungen enthält, gelten die in § 1 Abs. 4 PDSV aufgezählten Bestimmungen des BDSG.

Grundsätzlich erlaubt ist gemäß § 41 Abs. 2 PostG,

- Bestandsdaten (Daten natürlicher oder juristischer Personen, die für das Begründen, inhaltliche Ausgestalten und Ändern eines Vertragsverhältnisses erforderlich sind, insbesondere Name, Anschrift des Kunden [Absenders] und Art der in Anspruch genommenen Postdienstleistungen)
- Verkehrsdaten (Daten von Postkunden, die für den Zweck des Vertragsverhältnisses erforderlich sind, insbesondere Häufigkeit und Umfang der in Anspruch genommenen Postdienstleistungen)
- Auslieferungsdaten (Daten, die zum Nachweis einer ordnungsgemäßen Behandlung, Zustellung oder Rückführung der Sendung erforderlich sind)
- Entgeltdaten (Daten, die für das ordnungsgemäße Ermitteln, Abrechnen und Auswerten sowie zum Nachweis der Richtigkeit von Leistungsentgelten erforderlich sind)

für den jeweiligen Zweck zu erheben, zu verarbeiten und zu nutzen.

Daten, die sich auf die Inhalte von Postsendungen beziehen, unterliegen dagegen dem Verarbeitungsverbot.

Das unbefugte Speichern, Verändern oder Übermitteln von personenbezogenen Daten, die in den Schutzbereich des PostG, der PDSV oder des BDSG fallen, sind unzulässig und gemäß § 43 BDSG strafbewehrt.

Zudem gibt es zahlreiche spezielle EDV-bezogene Straf- und Ordnungswidrigkeitenvorschriften, wonach die unbefugte Einsichtnahme, Speicherung, Veränderung, Übermittlung, Nutzung oder anderweitige Beschaffung, Löschung oder Unbrauchbarmachung solcher Daten verboten ist und mit Strafen bzw. Geldbußen geahndet wird (z. B. §§ 202a, 303a StGB, § 44 BDSG).

Diesem Merkblatt ist eine Zusammenstellung der wichtigsten Regelungen des Postgesetzes, der PDSV und des BDSG beigefügt. Die vollständigen Gesetzes- und Verordnungstexte sind auf der Homepage der Regulierungsbehörde (www.regtp.de) einzusehen und stehen als download zur Verfügung. Darüber hinaus können Sie weitere Informationen zum Thema Datenschutz auf der Website des Bundesbeauftragten für den Datenschutz unter http://www.datenschutz.bund.de abrufen.

Anlage 32 (zu Nr. 29.2)

Verpflichtungserklärung zur Wahrung des Postgeheimnisses und des Datengeheimnisses gemäß § 5 Bundesdatenschutzgesetz (BDSG)

Herr/Frau

. . . . . .

beschäftigt bei

. . . . . .

wird hiermit auf die Wahrung des Postgeheimnisses und des Datengeheimnisses nach § 5 BDSG verpflichtet.

Mir ist bekannt, dass ich bei der Erbringung der Postdienstleistungen zur Wahrung des Postgeheimnisses verpflichtet bin und den datenschutzrechtlichen Regelungen des Postgesetzes (PostG), der Postdienstunternehmen-Datenschutzverordnung (PDSV) und des Bundesdatenschutzgesetzes (BDSG) unterliege. Das Postgeheimnis gilt auch innerhalb des Unternehmens.

Mir ist das Merkblatt „Postgeheimnis und Datenschutz“ ausgehändigt worden. Außerdem ist mir der wesentliche Inhalt der Vorschriften des BDSG, des Postgesetzes und der PDSV erläutert und eine Zusammenfassung der wichtigsten Regelungen übergeben worden.

Ich bin darauf hingewiesen worden, dass es untersagt ist, geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekannt zu geben, zugänglich zu machen oder zu nutzen.

Diese Verpflichtungen bestehen auch nach Beendigung meiner Tätigkeit fort.

Die Verpflichtung zur Wahrung des Datengeheimnisses umfasst insbesondere folgende Punkte:

- Daten und andere Informationen dürfen nicht zu einem anderen als dem geschäftlichen Zweck vervielfältigt werden; insbesondere ist es untersagt, das Datenmaterial für private Zwecke zu kopieren und/oder an Dritte – auch innerhalb des eigenen Unternehmens – weiter zu geben.
- Es dürfen nur die für die konkrete Aufgabenerfüllung notwendigen Daten abgerufen werden.
- Es ist untersagt, Daten zu verfälschen, unechte Daten herzustellen sowie vorsätzlich unechte oder verfälschte Daten zu gebrauchen.
- Unterlagen mit personenbezogenen Daten sind sicher vor dem Zugriff Dritter aufzubewahren.

Die aufgezählten Punkte sind sinngemäß auch beim Umgang mit Programmen zu beachten.

Ich bin darüber belehrt worden, dass Verstöße gegen das Postgeheimnis oder das Datengeheimnis nach § 206 des Strafgesetzbuches (StGB), § 43 BDSG und anderen einschlägigen Rechtsvorschriften (z. B. §§ 202a, 303a StGB) mit einer Freiheits- oder Geldstrafe geahndet werden können.

Der Empfang und die Kenntnisnahme dieser Verpflichtungserklärung sowie des Merkblattes „Postgeheimnis und Datenschutz“ wird durch meine Unterschrift bestätigt.

Die oben genannten Verpflichtungen werde ich einhalten.

. . . .

(Ort, Datum) (Unterschrift des/der Verpflichteten)

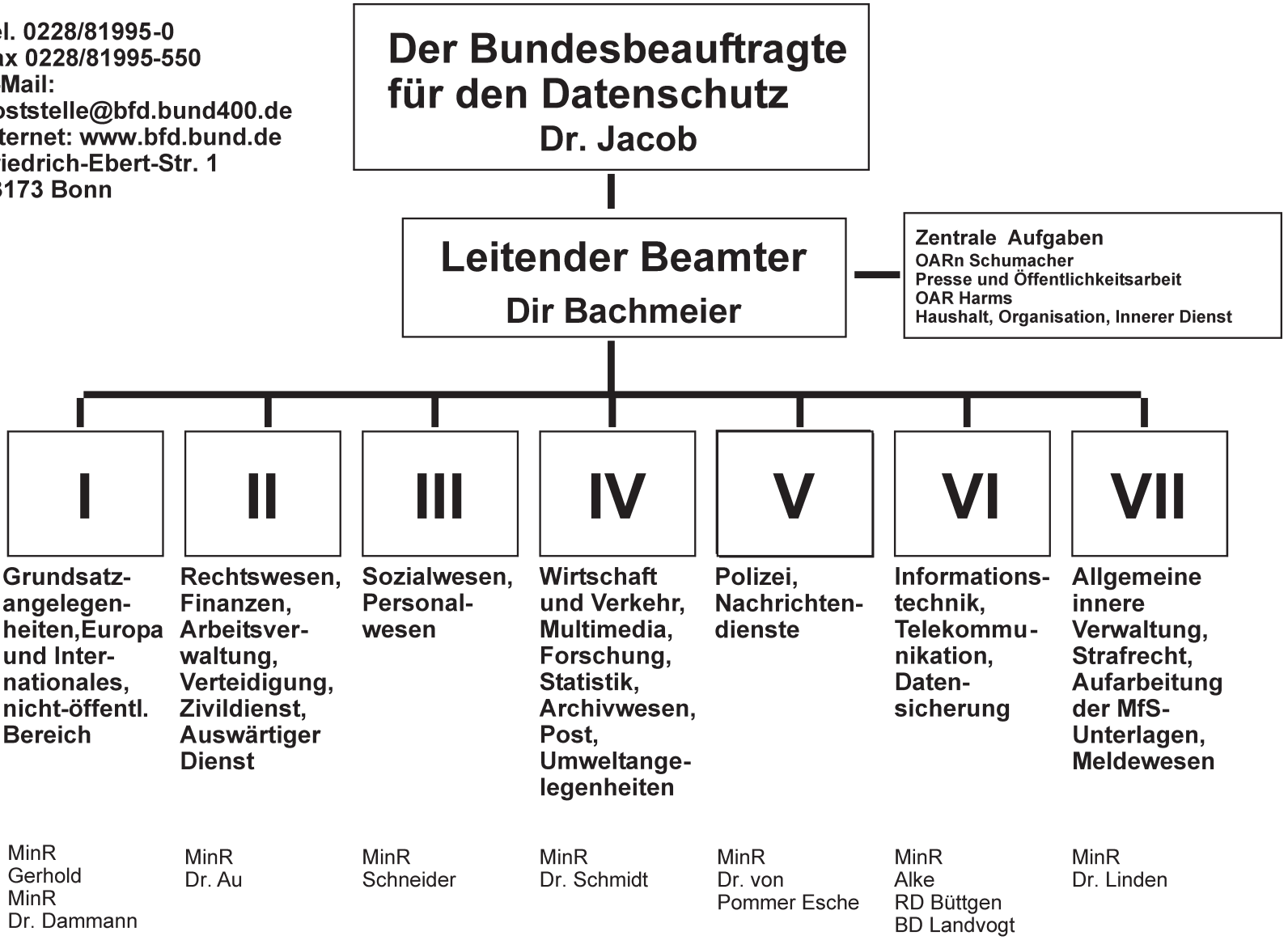
Ich habe die Verpflichtung durchgeführt. . . . . .

(Unterschrift des Verpflichtenden)

Original: für die Personalakte

Kopie: für den Beschäftigten, für den betrieblichen Datenschutzbeauftragten

Tel. 0228/81995-0
Fax 0228/81995-550
E-Mail:
poststelle@bfd.bund400.de
Internet: www.bfd.bund.de
Friedrich-Ebert-Str. 1
53173 Bonn



Sachregister

Als Fundstelle ist die Nummer des Kapitels oder des Abschnittes angegeben, in dem der Begriff verwendet wird.

Abkürzungsverzeichnis

AA	Auswärtiges Amt
Abb.	Abbildung
ABl.EG	Amtsblatt der Europäischen Gemeinschaften
Abs.	Absatz
AFIS	Automatisiertes Fingerabdruck-Identifizierungssystem
AG	Aktiengesellschaft; aber auch: Arbeitsgruppe
AGB	Allgemeine Geschäftsbedingungen
AIS	Arbeitgeber-Informations-Service
AjES-Verfahren	Verfahren zur Aufnahme jüdischer Emigranten aus der (früheren) Sowjetunion
AK II	Arbeitskreis II „Innere Sicherheit“ der IMK
AO	Abgabenordnung
APC	Arbeitsplatzcomputer
Art.	Artikel
ASIS	Ausbildungs-Stellen-Informations-Service
ASYLON	Asyl-online
AsylVfG	Asylverfahrensgesetz
ATG	Aktionsforum Telematik im Gesundheitswesen
ATM	Asynchronous Transfer Mode
AuslG	Ausländergesetz
AuslG-VV	Allgemeine Verwaltungsvorschriften zum Ausländergesetz
AVS	Automatisiertes Vollstreckungssystem
AWG	Außenwirtschaftsgesetz
AZR	Ausländerzentralregister
AZR-Gesetz	Ausländerzentralregister-Gesetz
BA	Bundesanstalt für Arbeit
BAFl	Bundesamt für die Anerkennung ausländischer Flüchtlinge
BAG	Bundesamt für Güterverkehr
BAN	Aktennachweis des Bundesgrenzschutzes
BargeldVV	Verwaltungsvorschrift zur Überwachung des grenzüberschreitenden Bargeldverkehrs
BAZ	Bundesamt für den Zivildienst
BBG	Bundesbeamtengesetz
BDO	Bundesdisziplinarordnung
BDSG	Bundesdatenschutzgesetz
BDSG-E	Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze
BEK	Barmer Ersatzkasse
BfA	Bundesversicherungsanstalt für Angestellte
BfD	Bundesbeauftragter für den Datenschutz
BfF	Bundesamt für Finanzen
BfV	Bundesamt für Verfassungsschutz
BG	Berufsgenossenschaft
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofes in Strafsachen
BGHZ	Entscheidungen des Bundesgerichtshofes in Zivilsachen
BGS	Bundesgrenzschutz
BGSG	Bundesgrenzschutzgesetz
BISS	BMI-Informationssystem
BK	Bundeskanzleramt
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
BMF	Bundesministerium der Finanzen
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BMVBW	Bundesministerium für Verkehr, Bau- und Wohnungswesen
BMVg	Bundesministerium der Verteidigung
BMWi	Bundesministerium für Wirtschaft und Technologie
BND	Bundesnachrichtendienst
BNDG	Gesetz über den Bundesnachrichtendienst
BPA	Bundespresseamt
BR-Drs.	Bundesratsdrucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStBl	Bundessteuerblatt
BStU	Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BT-Drs.	Bundestagsdrucksache
BVA	Bundesverwaltungsamt
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfSchG	Bundesverfassungsschutzgesetz
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
bzw.	beziehungsweise
C.SIS	technische Unterstützungseinheit des Schengener Informationssystems
CCIVBB	Competence Center Informationsverbund Berlin-Bonn
CD-ROM	Compact Disc – Read Only Memory
CERT	Computer Emergency Response Team
CIS	Zollinformationssystem (Customs Information System)
CJ-PD	Projektgruppe Datenschutz des Europarates
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
coArb	Computerunterstützte Arbeitsvermittlung
COMPAS	Computerunterstütztes Ausbildungsvermittlungssystem
d. h.	das heißt
DAK	Deutsche Angestellten-Krankenkasse
DAV	Dienstanschlussvorschriften
DDR	Deutsche Demokratische Republik
DEA	US-amerikanische Drogenbekämpfungsbehörde
DFS	Deutsche Flugsicherung GmbH
DHCP	Dynamic Host Configuration Protocol
DIHT	Deutscher Industrie- und Handelstag
DM	Deutsche Mark
DNA	Desoxyribonuclein acid (acid=Säure)
DNS	Domain Name Service
DRK	Deutsches Rotes Kreuz
DTAG	Deutsche Telekom AG
DV/dv	Datenverarbeitung
ECHELON	Abhörsystem der NSA
E-Commerce	Electronic Commerce/Elektronischer Handel
EDS	Europäische Drogenstelle
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft(en)

EG-ZIS	Europäisches Zollinformationssystem
E-Mail	Electronic Mail
EMRK	Europäische Menschenrechtskonvention
EP	Europäisches Parlament
EStG	Einkommensteuergesetz
EU	Europäische Union
EURODAC	Europäisches daktyloskopisches Fingerabdrucksystem zur Identifizierung von Asylbewerbern
EUROPOL	Europäisches Polizeiamt
EVN	Einzelverbindungsnachweis
EWG	Europäische Wirtschaftsgemeinschaft
EWR	Europäischer Wirtschaftsraum
f.	folgend
FAG	Fernmeldeanlagengesetz
FAQ	Frequently Asked Questions/Häufig gestellte Fragen
FCL	Flight Crew License
FEDMA	Federation of European Direct Marketing Associations
FeV	Fahrerlaubnis-Verordnung
ff.	folgende
FGO	Finanzgerichtsordnung
FGO-ÄndG	Gesetz zur Änderung der Finanzgerichtsordnung und anderer Gesetze
FRV	Fahrzeugregisterverordnung
FÜV	Fernmelde-Überwachungs-Verordnung
FVG	Finanzverwaltungsgesetz
G10	Gesetz zu Artikel 10 GG
GBA	Generalbundesanwalt beim Bundesgerichtshof
GBG	Geschlossene Benutzergruppe
GG	Grundgesetz
ggf.	gegebenenfalls
GGO	Gemeinsame Geschäftsordung der Bundesministerien
GmbH	Gesellschaft mit beschränkter Haftung
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GüKG	Güterkraftverkehrsgesetz
GwG	Geldwäschegesetz
HPC	Health Professional Card
HVBG	Hauptverband der gewerblichen Berufsgenossenschaften
i. S.	im Sinne
i. S. d.	im Sinne des (der)
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ICD-10	International Classification of Diseases – 10th Revision
IDS	Intrusion Detection System
IHK	Industrie- und Handelskammer
IM	Inoffizieller Mitarbeiter
IMEI	International Mobile Equipment Identity
IMK	Innenministerkonferenz
IMSI	International Mobile Subscriber Identity
INPOL	Informationssystem der Polizei
INZOLL	Informationssystem für den Zollfahndungsdienst

IP	Internet Protocol
IP-LAN	Internet Protocal – Local Area Network
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Informationstechnik
IuK	Informations- und Kommunikationstechnologie
IuKDG	Informations- und Kommunikationsdienstegesetz
IVBB	Informationsverbund Berlin-Bonn
JAA	Joint Aviation Authorities
JAR	Joint Aviation Requirement
KAN	Kriminalaktennachweis
KBA	Kraftfahrt-Bundesamt
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung
KDVG	Kriegsdienstverweigerungsgesetz
KISLS	Kommunikations- und Informationssystem Luftsicherheit
KOM	(Europäische) Kommission
KVK	Krankenversicherungskarte
LAN	Local Area Network
LBA	Luftfahrt-Bundesamt
LfD	Landesbeauftragter für den Datenschutz
LG	Landgericht
LuftVG	Luftverkehrsgesetz
LuftVZO	Luftverkehrs-Zulassungs-Ordnung
m. E.	meines Erachtens
MAD	Militärischer Abschirmdienst
MADG	Gesetz über den MAD
MAdLAN	Multilinguales Adresssystem im Local Area Network
MAZ	Magnetische Bildaufzeichnung
MfS	Ministerium für Staatssicherheit/Amt für nationale Sicherheit (der ehemaligen DDR)
MiStra	Mitteilungen in Strafsachen
MiZi	Mitteilungen in Zivilsachen
MRRG	Melderechtsrahmengesetz
N.SIS	Nationaler Bestand des Schengener Informationssystems
NADIS	Nachrichtendienstliches Informationssystem
NaStrAG	Namensaktiengesetz
Nr.	Nummer
Nrn.	Nummern
NSA	National Security Agency
o. g.	oben genannt
OECD	Organization for Economic Co-operation and Development/Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OLAF	Europäisches Amt für Betrugsbekämpfung
OLG	Oberlandesgericht
OSS	Open Source Software
PC	Personalcomputer
PDSV	Postdienstunternehmen-Datenschutzverordnung
PERFIS	Personalführungs- und Informationssystem der Bundeswehr
PersVG	Personalvertretungsgesetz
PERSY	Personalbezogenes Dateiensystem des Auswärtigen Amtes
PIN	persönliche Identifikationsnummer

PK	Personenkennzeichen
PKGrG	Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes-Kontrollgremium
PostG	Postgesetz
PTB	Physikalisch-Technische-Bundesanstalt
PTRegG	Gesetz über die Regulierung der Telekommunikation und des Postwesens
PZD	Personenzentraldatei
RegTP	Regulierungsbehörde für Telekommunikation und Post
Reha	Rehabilitation
RKpS	Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen
s.	siehe
s. o.	siehe oben
s. u.	siehe unten
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
SDÜ	Schengener Durchführungsübereinkommen
SG	Soldatengesetz
SGB	Sozialgesetzbuch
SGB I	Sozialgesetzbuch Erstes Buch (Allgemeiner Teil)
SGB III	Sozialgesetzbuch Drittes Buch (Arbeitsförderung)
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 X	Sozialgesetzbuch Zehntes Buch (Verwaltungsverfahren)
SGB XI	Sozialgesetzbuch Elftes Buch (soziale Pflegeversicherung)
SigG	Signaturgesetz
SIM	Subscriber Identity Module
SIRENE	Supplementary Information Request at the National Entry (= Nationales Büro im Rahmen der Schengen-Kooperation)
SIS	Schengener Informationssystem
SIS	Stellen-Informations-Service
SMS	Short Message Service
sog.	so genannt
SPersAV	Verordnung über die Führung der Personalakten der Soldaten und der ehemaligen Soldaten – Personalaktenverordnung Soldaten –
SSL	Secure Socket Layer
S-T-A	Sprach- und Textanalysesystem
STADA	Staatsangehörigkeitsdatei
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StUG	Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz)
StVÄG	Strafverfahrensänderungsgesetz
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrs-Zulassungs-Ordnung
SÜG	Sicherheitsüberprüfungsgesetz
TB	Tätigkeitsbericht
TCP/IP	Transmission Control Protocol/Internet Protocol
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikationsdienstunternehmen-Datenschutzverordnung; ab Dezember 2000: Telekommunikations-Datenschutzverordnung
THW	Technisches Hilfswerk
TK	Telekommunikation

TK-Anlage	Telekommunikationsanlage
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung
TKV	Telekommunikations-Kundenschutzverordnung
T-PD	Beratender Ausschuss des Europaratsübereinkommens
Ü 1	einfache Sicherheitsüberprüfung
Ü 2	erweiterte Sicherheitsüberprüfung
Ü 3	erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen
u.a.	unter anderem
u.ä.	und ähnliches
UMTS	Universal Mobile Telecommunications System
UmwG	Umwandlungsgesetz
URL	Uniform Resource Locator
USEIT	Unix Security Enhancement and Information Tool (Administrationssoftware für Unix-Rechner)
usw.	und so weiter
VDR	Verband Deutscher Rentenversicherungsträger
vgl.	vergleiche
VICLAS	Violent Crime Linkage Analysis System
VISA	Computerprogramm zur Führung der Dateien nach §§ 7 und 8 Ausländerdateienverordnung
VMBl.	Ministerialblatt des Bundesministeriums der Verteidigung
VZR	Verkehrszentralregister
WAP	Wireless Application Protocol
WBV	Wehrbereichsverwaltung
WEWIS	Wehrersatzwesen-Informationssystem
WORM	Write once – Read Multiple (einmal beschreibbare CD-ROM)
WP	Working Party ((Dokument der) Artikel 29-Gruppe)
www	world wide web
z. B.	zum Beispiel
z. T.	zum Teil
ZAV	Zentralstelle für Arbeitsvermittlung
ZDG	Zivildienstgesetz
ZDPersAV	Verordnung über die Führung der Personalakten im Zivildienst – Zivildienst-Personalaktenverordnung –
ZEVIS	Zentrales Verkehrsinformationssystem
ZIS	Zollinformationssystem
ZKA	Zentraler Kreditausschuss
ZKA	Zollkriminalamt
ZOLLVG	Zollverwaltungsgesetz
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister

Tätigkeitsbericht	Berichtszeitraum	Bundestagsdrucksachennummer
1.	1978	8/2460
2.	1979	8/3570
3.	1980	9/93
4.	1981	9/1243
5.	1982	9/2386
6.	1983	10/877
7.	1984	10/2777
8.	1985	10/4690
9.	1986	10/6816
10.	1987	11/1693
11.	1988	11/3932
12.	1989	11/6458
13.	1990	12/553
14.	1991 – 1992	12/4805
15.	1993 – 1994	13/1150
16.	1995 – 1996	13/7500
17.	1997 – 1998	14/850

Druck: MuK. Medien- und Kommunikations GmbH, Berlin
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