Deutscher Bundestag **Drucksache 15/888**

15. Wahlperiode 07. 05. 2003

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz

Tätigkeitsbericht 2001 und 2002 des Bundesbeauftragten für den Datenschutz – 19. Tätigkeitsbericht –

Inhaltsverzeichnis

Zugeleitet mit Schreiben des Bundesbeauftragten für de n Datenschutz vom 7. Mai 2003 gemäß § 26 Abs. 1 des Bundesdatenschutzgesetzes i. d. F. der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66).

Abbildungsverzeichnis

1 Einführung – Überblick und Ausblick –

1.1 Eine zwiespältige Bilanz

Dieser 19. Tätigkeitsbericht (T B), den ich dem Deutschen Bundestag vorlege, ist der fünfte und letzte in meiner Amtszeit als Bundesbeauftragter für den Datenschutz. Er gibt einen Überblick über meine Tätigkeit in den Jahren 2001 und 2002, die wiederum neben der datenschutzrechtlichen Kontrolle stark von der Beratung des Deutschen Bundestages, der Bundesregierung und der öf fentlichen Stellen des Bundes in Fragen des Datenschutzes geprägt war. Vieles konnte zur Stärkung des Grundrechts au f informationelle Selbstbestimmung erreicht werden, in anderen Bereichen besteht weiterer Handlungsbedarf, und es gibt immer wieder neue Fragestellungen und Problemfelder, die einer datenschutzgerechten Lösung zugeführt werden müssen. Ein Tätigkeitsbericht kann deswegen immer nur eine Momentaufnahme ohne abschließenden Charakter sein. Er gibt Rechenschaft über die geleistete Arbeit und soll zugleich aufzeigen, wo aus Sicht des Datenschutzes weitere V erbesserungen erforderlich oder zumindest wünschenswert sind.

Bei meiner Arbeit in den letzten zwei Jahren habe ich – auch bei unterschiedlicher Position in der Sache – viel V erständnis und Unterstützung gefunden. Dafür danke ich den Mitgliedern des Deutschen Bundestages, aber auch den vielen Vertretern in Regierung und V erwaltung, die meinen Rat in Datenschutzfragen gesucht und angenommen und meine Tätigkeit insgesamt unterstützt haben. Mein Dank gilt aber auch den Mitarbeiterinnen und Mi tarbeitern meiner Dienststelle, die mich mit unvermin dert großem Engagement und hoher Leistungsbereitschaft bei der Erfüllung meiner gesetzlichen Aufgaben unterstützen.

Auch der jetzige Berichtszeitraum hat wieder gezeigt, dass das Gespür für die Belange des Datenschutzes in Politik und Verwaltung, aber auch allgemein in der Gesellschaft, in den Kreisen der privaten W irtschaft und nicht zuletzt bei den Bürgern, um deren Grundrechtsschutz es schließlich geht, zwar weiter gewachsen ist, dem Datenschutz aber noch lange nicht von allen der Stellenwert eingeräumt wird, der ihm als Garant von Bür gerrechten in einem freiheitlichen Rechtsstaat zukommen sollte. Ursache dafür sind auch of fenbar sich wiederholende Vorurteile und Missverständnisse. W eder sind innere Sicherheit und Datenschutz zwangsläufig Gegensätze, noch behindert Datenschutz effizientes Verwaltungshandeln oder stört die freie Entfaltung der wirtschaftlichen Kräfte und Möglichkeiten. Und auch die leider immer noch vertretene Meinung, wer nichts zu verber gen habe, brauche keinen Datenschutz, geht an der Sache völlig vorbei.

Eine Reihe von Punkten, die ich in meinem letzten Tätigkeitsbericht angesprochen habe, konnten im Berichtszeitraum gelöst oder zumindest einer Lösung näher gebracht werden. Dies gilt aber leider nicht für alle Problemfelder , die ich dort – zum T eil nicht zum ersten Mal – thematisiert habe. So hat die Bundesregie rung noch immer keinen Entwurf eines Arbeitnehmerdatenschutzgesetzes vorgelegt, obwohl sie hierzu vom Deutschen Bundestag mehrfach aufgefordert worden ist (vgl. Nr . 21.1). Auch zum unbefugten Aufnehmen und Verbreiten von personenbezogenen Bilddaten steht eine gesetzliche Regelung weiterhin aus, obwohl die Regelungsbedürftigkeit allg emein anerkannt wird (vgl. Nr. 8.1). Die Zahl der T elefonüberwachungen ist im Berichtszeitraum in Deutschland weiter deutlich angestiegen (vgl. Nr. 8.2.5), ohne dass es hierfür eine für mich nachvollziehbare, befriedigende Erklärung gibt. Auch das hierzu in Auftrag gegebene Forschungsvorhaben (vgl. Nr . 8.3) liegt noch nicht vor. Diese Entwicklung erfüllt mich unverändert mit großer Sorge. Wir dürfen nicht zulassen, dass sich in unserem Land schleichend und fa st unbemerkt eine Überwachungskultur entwickelt, deren tatsächliche Notwendigkeit nicht nachgewiesen ist.

1.2 Das neue BDSG – nur eine Etappe auf dem Weg zur umfassenden Reform des Datenschutzrechts

Im Juni 2002 konnte das 25-jährige Bestehen des Bundesdatenschutzgesetzes mit einem Festakt in Berlin gefeiert werden (vgl. Nr. 33.1). Ein Jahr davor ist endlich nach langem Ringen das Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze in Kraft getreten (vgl. Nr. 3.2), das nicht nur die europäische Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 in nationales Recht umgesetzt, sondern darüber hinaus bedeutsame Neuerungen gebracht hat. Wichtige Weichenstellungen für die Zukunft bedeuten nach meiner Einschätzung die Verankerung des Grundsatzes von Datenvermeidung und Datensparsamkeit im Gesetz, die Einführung der Vorabkontrolle, das Verbot der automatisierten Einzelentscheidung, die Regelung zur V ideoüberwachung und zum Einsatz von Ch ipkarten und die Einführung des Datenschutzaudits.

Aber gerade dieser letzte Punkt zeigt den großen Unterschied, der zwischen der gesetzlichen Theorie und der praktischen Umsetzung bestehen kann. Denn die ins BDSG eingefügte Regelung zum Datenschutzaudit läuft so lange leer , wie das erforderliche Ausführungsgesetz, das die Einzelheiten regeln soll, nicht in Kraft getreten ist. Bislang besteht hierfür noch nicht einmal ein Entwurf (vgl. Nr . 3.2.1). Damit können sich aber auch die positiven Wirkungen, die den Datenschutz zum Wettbewerbsvorteil machen und dadurch in die technische und wirtsc haftliche Entwicklung integrieren sollen, noch nicht entfalten. Im Gegenteil besteht die Gefahr, dass auf dem Markt Auditierungsverfahren angeboten und eingesetzt werden, die dann später den gesetzlichen Anforderungen nicht entsprechen, was zu V erwirrung und Verärgerung bei Unternehmen und Verbrauchern führen und letztlich der Akzeptanz des Datenschutzaudits schaden kann.

Auch sonst ist die Umsetzung des neuen BDSG in der Praxis noch lange nicht vollzogen. So hat eine Umfrage bei den obersten Bundesbehörden zur Position des behördlichen Datenschutzbeauftragten bei ihnen selbst und in ihrem jeweiligen Geschäftsbereich (vgl. Nr. 3.2.5) teilweise noch deutliche Defizite ergeben, obwohl der interne Datenschutzbeauftragte auch für den öf fentlichen Bereich zum Zeitpunkt der Erhebung seit über einem Jahr gesetzlich vor geschrieben war. Auch bei der Videoüberwachung zeigen sich Unsicherheiten (vgl. Nrn. 3.2.2, 4.1), und noch lange hat nicht jede öf fentliche Stelle V ideokameras, die den öf fentlich zugänglichen Raum überwachen, entsprechend der gesetzlichen Vorschrift kenntlich gemacht. V ergleichbare Vollzugsdefizite zeigen sich auch bei nicht öffentlichen Stellen, und dies nicht nur bei der Videoüberwachung. Von den Postdienst- und T elekommunikationsunternehmen abgesehen, gehören datenschutzrechtliche Kontrolle und Beratu ng nicht öffentlicher Stellen

zwar nicht zu meinen Aufgaben. Ich kann aber dennoch feststellen, dass hier offensichtlich nicht überall die Vorschriften des BDSG bekannt sind und beachtet werden. Dies sollte auch bei der notwendigen Weiterentwicklung des Datenschutzrechts berücksichtigt werden. Es macht in meinen Augen wenig Sinn, wenn erweiterten und verbesserten gesetzlichen Datenschutzbestimmungen in der Praxis kein Vollzug folgt und dies nicht sanktioniert oder im schlimmsten Fall dieses Defizit noch nicht einmal festgestellt wird. Im Zuge der von der Bundesregierung angekündigten zweiten Stufe der BDSG-Novellierung sollte deswegen verstärkt darauf geachtet werden, das Gesetz überschaubar und praktikabel zu gestalten und seinen Vollzug zu verbessern.

Die Vorbereitungen zu dieser beabsichtigten Reform des Datenschutzrechts sind im Berichtszeitraum weiter vorangeschritten (vgl. Nr. 3.3). So liegt ein vom Bundesministerium des Innern in Auftrag gegebenes umfangreiches Gutachten vor, das eine umfassende und tiefgreifende Analyse des Modernisierungsbedarfs im Datenschutzrecht enthält und die Richtung für eine weit reichende Reform des Datenschutzes weist. Die Vorschläge der Gutachter, das Datenschutzrecht zu vereinfachen und möglichst viele Spezialvorschriften im BDSG zu integrieren, die Selbstbestimmung des Einzelnen zu stärken und gesellschaftliche Selbstregulierung sowie technischen Datenschutz verstärkt zu fördern, halte ich für sinnvoll und gut. Angesichts der in der Bundesrepublik Deutschland bereits sehr ausdifferenzierten Datenschutzregelungen wird es aber nicht einfach sein, diese Überlegungen zeitnah umzusetzen, zumal es sich hierbei um grundlegende Weichenstellungen und noch nicht um konkrete, ausformulierte Regelungsvorschläge handelt. Das Ziel, das informationelle Selbstbestimmungsrecht des Bürgers zu einem selbstverständlichen, integrierten Teil der technischen, gesellschaftlichen, wirtschaftlichen und rechtlichen Entwicklung zu machen und nicht mehr als einen Eingriff von außen in diese Entwicklung zu begreifen, sollte aber in jedem Falle mit Nachdruck weiterverfolgt werden.

1.3 Terrorismusbekämpfung und Innere Sicherheit – auch der Datenschutz ist gefordert

Der furchtbare Terroranschlag vom 11. September 2001 und die fortbestehende weltweite Bedrohung durch den internationalen Terrorismus, aber auch der Kampf gegen das organisierte Verbrechen und das stete Bemühen um eine verbesserte innere Sicherheit haben im Berichtszeitraum Recht und Praxis des Datenschutzes nachhaltig beeinflusst. Aufgrund der tief gehenden Bedeutung der gesetzlichen Maßnahmen zur Terrorismusbekämpfung auch für den Datenschutz habe ich diesem Thema ein eigenes Kapitel gewidmet (vgl. Nr. 2). Auch wenn erste politische Äußerungen und erste Gesetzentwürfe zum Teil einen anderen Tenor hatten, hat sich im Ergebnis wieder gezeigt, dass wirksame Bekämpfung von Terror und Kriminalität und Datenschutz als Ausdruck des Grundrechts auf freie Entfaltung der Persönlichkeit und informationelle Selbstbestimmung keine unüberbrückbaren Gegensätze sein müssen, sondern sich sehr wohl in einem ausgewogenen Interessenausgleich untereinander verbinden lassen. Obwohl ich mit meinen Bedenken nicht immer durchdringen konnte, bewerte ich es als besonders positiv, dass es erstmals gelungen ist, neue Eingriffsbefugnisse für die Sicherheitsbehörden zu befristen und einer Erfolgskontrolle zu unterwerfen. Nur so kann auf Dauer festgestellt werden, welche Eingriffe und Beschränkungen beim Datenschutz wirklich zur Verbesserung der Gefahrenabwehr und inneren Sicherheit erforderlich sind und wo sich die Erwartungen der Sicherheitsbehörden und des Gesetzgebers nicht erfüllt haben, sodass ein Fortbestand der entsprechenden Befugnisse nicht gerechtfertigt ist. Damit ist der Weg frei, Einschränkungen des Datenschutzes auch wieder abzubauen, wenn sie sich im Nachhinein als nicht wirksam und damit als nicht notwendig herausgestellt haben. Voraussetzung dafür ist, dass die Evaluierung ehrlich und nachvollziehbar vorgenommen wird und die Bereitschaft fortbesteht, daraus dann zu gegebener Zeit auch die Konsequenzen zu ziehen.

Die Folgen des Terrors wirken sich aber nicht nur auf die nationale Gesetzgebung aus, sie sind international, wie der Terror selbst (vgl. Nr. 32.1). Die Strategien zur Vermeidung weiterer Anschläge und zur Bekämpfung der Täter zielen weltweit auf verbesserte Überwachung, grenzüberschreitenden Zugriff von Sicherheitsbehörden auf möglichst umfassende Datenbestände und einen ungehinderten Datenaustausch ab. Auch hier wird es gelten, die datenschutzrechtlichen Grundsätze von Erforderlichkeit und Verhältnismäßigkeit strikt zu beachten und insbesondere Missbrauchsmöglichkeiten von vornherein zu unterbinden. Ohne einen verstärkten internationalen Datenschutz kann dies kaum gelingen.

Neben neuen Gesetzesinitiativen sind im Zuge der Terrorbekämpfung aber auch alte Instrumente wieder aktuell geworden. Dies gilt insbesondere für die Rasterfahndung (vgl. Nr. 13.1). Auf Landesebene hat sie zu einer Reihe von Prozessen und unterschiedlich lautenden Gerichtsurteilen geführt. Soweit das BKA aufgrund eines Beschlusses der Gremien der Ständigen Konferenz der Innenminister und -senatoren der Länder in seiner Funktion als Zentralstelle der Polizeien des Bundes und der Länder beauftragt worden ist, unterstützend tätig zu werden, hat meine Prüfung ergeben, dass sich dieses dabei im Rahmen der ihm durch das BKA-Gesetz eingeräumten Befugnisse zur Erfüllung seiner Zentralstellenaufgabe gemäß § 2 i. V. m. § 7 BKA-Gesetz gehalten hat, auch soweit es selbst bei diversen nicht öffentlichen Stellen um Übermittlung von Personaldaten ersucht hat. Ob der Gesetzgeber aber wirklich dem BKA mit § 7 Abs. 2 Satz 2 BKA-Gesetz eine Befugnis zur massenhaften Erhebung personenbezogener Daten von Unverdächtigen einräumen wollte, ist gleichwohl fraglich. Da derartige Maßnahmen auf der rechtsstaatlich solideren Grundlage der hierfür jeweils geschaffenen landesgesetzlichen Regelungen zur Rasterfahndung durchgeführt werden können, sollte künftig bei Fortbestehen der jetzigen Gesetzeslage auf eine massenhafte Erhebung personenbezogener Daten durch das BKA verzichtet werden. Anderenfalls sollte der Bundesgesetzgeber zumindest eine eigenständige Gesetzesgrundlage für das BKA schaffen. In jedem Falle halte ich es für außerordentlich bedenklich, dass sich das Verfahren so lange hingezogen hat und erste Datenlöschungen erst jetzt im Frühjahr 2003 vorgenommen werden sollen. Insgesamt haben die Rasterfahndungen immer noch zu keinem abschließenden Ergebnis geführt, was die Frage herausfordert, wie effizient dieses Instrument tatsächlich für die Bekämpfung des Terrors genutzt werden kann.

1.4 Kommt der gläserne Finanzmarkt?

Beim Kampf gegen Terrorismus und organisierte Kriminalität richtet sich der Blick auch immer wieder auf die Geldströme,

die solche Taten erst ermöglichen oder daraus resultieren. So hat es im Berichtszeitraum eine Reihe von Initiativen und Maßnahmen gegeben, die hier ansetzen. Hierzu zählen das Geldwäschebekämpfungsgesetz vom 18. August 2002, das u. a. beim Bundeskriminalamt eine „Zentralstelle für Verdachtanzeigen“ geschaffen hat (vgl. Nr. 13.7), das Vierte Finanzmarktförderungsgesetz vom 21. Juni 2002, das in § 24c des Gesetzes über das Kreditwesen eine Rechtsgrundlage für einen automatisierten Abruf von Kontoinformationen durch die Bundesanstalt für Finanzdienstleistungsaufsicht eingeführt hat und in § 25a Abs. 1 Nr. 4 des Gesetzes über das Kreditwesen eine Regelung zum so genannten Konto-Screening enthält (vgl. Nr. 10.2), und die Errichtung der Datenbank „ZAUBER“ beim Bundesamt für Finanzen zur Auswertung von Umsatzsteuer-Betrugsfällen und zur Entwicklung von Risikoprofilen (vgl. Nr. 15.3). Das Aufdecken illegaler Finanzströme, die Bekämpfung von Geldwäsche und Kriminalität sind unbestreitbar von herausragender Bedeutung und erfordern angemessene gesetzliche Maßnahmen. Die einzelnen Regelungen mögen für sich genommen trotz mancher datenschutzrechtlicher Bedenken auch nötig oder zumindest sinnvoll sein. Die Summe der neuen Eingriffsmöglichkeiten und neu angelegten Dateien, verbunden mit noch weiter reichenden Überlegungen für die Zukunft können aber zu einer weit gehenden Transparenz des Finanzmarktes und des Anlageverhaltens jedes Bürgers führen und zu einer Bedrohung für sein Grundrecht auf informationelle Selbstbestimmung werden. Dies gilt umso mehr, wenn im Zuge der Kriminalitätsbekämpfung auch unbescholtene Bürger grundlos in Verdacht geraten, den sie mangels Kenntnis hiervon auch nicht ausräumen können oder sich für rechtmäßiges Verhalten plötzlich rechtfertigen müssen. Auch die Gefahr, dass einmal für ganz bestimmte Zwecke angelegte Datenbestände später noch für ganz andere Zwecke herangezogen werden, erscheint durchaus real. Deswegen sind die Grundsätze von Erforderlichkeit und Verhältnismäßigkeit strikt zu beachten.

1.5 Online auf dem Vormarsch

Ständig verbesserte Möglichkeiten der elektronischen Kommunikation, aber auch der Zugang immer breiterer Bevölkerungskreise zum Internet haben im Berichtszeitraum zu einer Reihe von Maßnahmen geführt, die auch die „amtliche Kommunikation“ in diese Entwicklung einbinden sollen. Mit dem Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 13. Juli 2001 wurde grundsätzlich die Möglichkeit eröffnet, elektronische Dokumente bei Gerichten einzureichen (vgl. Nr. 8.10.1). Dabei ist ein wesentlicher Aspekt des Elektronischen Rechtsverkehrs, auch auf diesem Wege auf die Datenbanken der Register gerichte zugreifen zu können. Hier gibt es bereits gesetzliche Regelungen für automatisierte Abrufe aus dem Handelsregister, dem Vereinsregister und dem Schuldnerverzeichnis.

Das Dritte Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften vom 21. August 2002 hat parallel dazu die elektronische Kommunikation zwischen Bürger und Verwaltung ermöglicht (vgl. Nr. 8.10.2). Dies wiederum ist Voraussetzung für eGovernmentprojekte (vgl. hierzu Nr. 4.7), die auf allen Ebenen zunehmend vorangetrieben werden. Die Bundesregierung plant im Rahmen ihrer Initiative BundOnline 2005 bis zum Jahre 2005 alle internetfähigen Dienstleistungen der Bundesverwaltung auch über das Internet online bereitzustellen. Durch das Programm VISA 2000 des Auswärtigen Amtes (vgl. Nr. 6.1) soll nicht nur der Verkehr zwischen den beteiligten Dienststellen online abgewickelt, sondern in Zukunft auch eine elektronische Antragstellung ermöglicht werden. Auch im Bereich der politischen Wahlen wird geprüft, inwieweit diese elektronisch unterstützt werden können (vgl. Nr. 7.8.2).

All diese Überlegungen und neuen technischen Möglichkeiten tragen nicht nur zu einem bequemen, schnellen und effizienten Geschäfts- bzw. Verwaltungsablauf bei, sie werfen auch vielfältige datenschutzrechtliche Probleme auf, und das nicht nur in technischer Hinsicht. Welche Konsequenzen sich für den Datenschutz ergeben können, zeigt beispielhaft die durch Ergänzung des § 9 der Insolvenzordnung geschaffene Möglichkeit, öffentliche Bekanntmachungen in Insolvenzverfahren auch im Internet vorzunehmen (vgl. Nr. 10.7). Ohne besondere Vorkehrungen könnte durch diese neue Form der Veröffentlichung der gebotene Schutz der betroffenen Schuldner leicht unterlaufen werden. Denn was einmal im Internet veröffentlicht war, bleibt zeitlich und örtlich unbegrenzt verfügbar, unabhängig von gesetzlichen Löschungsvorschriften, und kann den Betroffenen u. U. noch nach Jahrzehnten vorgehalten werden. Im konkreten Fall ist es zu einer Lösung gekommen, die allerdings nicht vollständig befriedigt. Generell zeigt dieses Beispiel aber, dass Internet und Online-Kommunikation mehr sind als nur eine neue Form, Nachrichten zu verbreiten. Damit verbunden ist die Möglichkeit, einmal dort veröffentlichte Informationen ohne besonderen Zeitaufwand und ohne besondere finanzielle oder personelle Ressourcen weltweit zusammenführen, auswerten, speichern und weitergeben zu können, ohne dass dies noch in irgendeiner Form kontrollierbar oder reglementierbar wäre. Ich halte deswegen das vielfach zu hörende Argument, bestimmte Informationen seien auch bisher schon veröffentlicht worden und das Internet stelle nur eine zeitgemäße Form der Bekanntmachung dar, für falsch.

Auch die zunehmende Vernetzung der Verwaltungen untereinander und mit dem Bürger, die Online-Abwicklung von Verwaltungsverfahren machen die Verwaltung nicht nur moderner und effizienter. Vielfach wird übersehen, dass unter dem Zeichen von Modernität und Effizienz Datenverbünde und Informationsflüsse entstehen könnten, deren Verhinderung ursprüngliches Anliegen des Datenschutzes und Gegenstand des Volkzählungsurteils war. Natürlich steigert es die Effizienz und spart Kosten, wenn nicht jede Behörde ihre eigenen Datenbestände anlegen und verwalten muss, sondern unproblematisch auf elektronischem Wege anderswo die Informationen abfragen kann, die sie zu benötigen meint. Aber genau diese Möglichkeiten hat das Bundesverfassungsgericht bereits in seinem Grundsatzurteil vom 15. Dezember 1983 – also vor bald 20 Jahren – sehr anschaulich beschrieben und sie haben es dazu bewogen, dem das Grundrecht auf informationelle Selbstbestimmung entgegenzusetzen. Dies gilt auch heute noch, wo die gleichen Fragen unter völlig neuen Vorzeichen diskutiert werden. Das heißt natürlich nicht, dass eGovernment und Verwaltungsmodernisierung nicht stattfinden dürfen – im Gegenteil, es führt kein Weg daran vorbei –, aber der Datenschutz wird hier künftig über die rein technischen Fragen hinaus ganz besonders gefordert sein. Und der Bürger wird sich fragen müssen, wie gläsern er um seiner Bequemlichkeit willen werden will.

1.6 Reform der Arbeitsverwaltung – Arbeit für den Datenschutz

Die Reform der Arbeitsverwaltung und die Verbesserung der Vermittlung von Arbeitslosen sind Ziele, die uneingeschränkte Unterstützung verdienen. Bei den neuen W egen, die hierzu im Berichtszeitraum beschritten worden sind, bleiben Fragen des Datenschutzes ab er vielfach offen. So sieht das Gesetz zur Verbesserung der Zusammenarbeit zwischen Arbeitsämtern und Trägern der Sozialhilfe vom 20. November 2000 eine Förderung von Modellprojekten zur Verbesserung der Zusammenarbeit von Arbeits- und Sozialämtern vor, mit denen die Vermittlung arbeitsloser Sozialhilfeempfänger verbessert werden soll (vgl. Nr. 23.2.1). Der hierfür erforderliche Datenaustausch zwischen den Ämtern, die zu unterschiedlichen Gebietskörperschaften gehören, mit privaten Stellen und in die vorgesehene Evaluierung eingebundenen Forschungsinstituten ist aber nicht hinreichend geregelt worden, sodass in der Praxis jetzt viele datenschutzrechtliche Fragen noch ungeklärt sind.

Auch die Umsetzung der Vorschläge der so genannten Hartz-Kommission hat zum Teil erhebliche Auswirkungen auf rechtliche Regelungen zum Sozialda tenschutz (vgl. Nr. 23.2.2). Auch hier geht es u. a. um Datenflüsse zwischen der Arbeitsverwaltung und zum Teil privat organisierten Personal-Service-Agenturen, um den Zugang privater Vermittler zu den Computersystemen der Arbeitsämter sowie um die Entwicklung einer digitalen Signaturkarte für den Abruf von V erdienst- und Arbeitsbescheinigungen.

An diesem Beispiel zeigt sich deutlich, wie wichtig es ist, datenschutzrechtliche Aspekte von vornherein in alle Überlegungen der V erwaltungsmodernisierung, der Privatisierung bislang staatlicher Aufg abenerfüllung und der Ef fizienzsteigerung beim Verwaltungshandeln mit einzubeziehen. Das Datenschutzrecht bietet genügend Möglichkeiten, um zu sinnvollen, datenschutzkonformen Lösungen zu kommen. Probleme entstehen nicht dadurch, dass der Datenschutz Reform- und Modernisierungsprojekte an sich behindern oder gar vereiteln würde, sondern dadurch, dass vielfach geplant und entschieden wird, ohne an Datenschutz überhaupt zu denken, und dies, obwohl es um Grundrechtsschutz der Bürger geht.

1.7 Wie elektronisch wird das Gesundheitswesen?

Grundlegende Reformen stehen auch im Gesundheitswesen an. Um den vielfältigen Problemen und den ständig steigenden Kosten zu begegnen, wird auch immer wieder der Einsatz elektronischer Mittel propagiert, und dies auf unterschiedlichen Ebenen und zu verschiedenen Zwecken. So wurde und wird im Rahmen der Gesundheitsreform überlegt, einen Datenpool aller Leistungserbringer für Steuerungsaufgaben der gesetzlichen Krankenversicherung und für gesundheitspolitische Auswertungen zu schaf fen (vgl. Nr. 24.1.1). Unter dem Oberbegrif f Telematik im Gesundheitswesen (vgl. Nr. 28.1) wird die Anwendung von Telekommunikation und Informatik verstanden, um die medizinische Versorgung zu optimieren, patientenorientierte Angebote zu verbessern, Wirtschaftspotenziale zu erschließen bzw. Kosten zu senken. Hierunter fallen das elektronische Rezept (vgl. Nr. 28.2), die elektronische Gesundheitskarte (vgl. Nr. 28.3) oder auch die elektronische Patientenakte (vgl. Nr. 28.4).

Die Vielfalt der auch in der Öffentlichkeit diskutierten elektronischen Möglichkeiten und Anwendungen ist verwirrend und der betroffene Bürger verliert den Überblick, was wo für wen über seine Gesundheit gespeichert werden soll, wer Zugriff auf diese Daten hat, zwischen welchen Stellen welcher Datenaustausch stattfinden soll, wer was in welcher Form auswerten darf und was bei dem allen aus seinem Grundrecht auf informationelle Selbstbestimmung und dem Schutz hoch sensibler Gesundheitsdaten wird.

Ich halte es deswegen für entscheidend, dass am Ende der Diskussion Lösungen gefunden werden, die für den Patienten absolut transparent sind und bei denen er Herr seiner Daten bleibt. Akzeptanz wird der Einsatz neuer T echniken in diesem Bereich nur finden können, wenn der Bür ger sein Misstrauen verliert und dies nicht als V ersuch begreift, ihn zu kontrollieren, sein V erhalten auszuspionieren oder Aufschluss über seinen tatsächlichen Gesundheitszustand zu erlangen. Auch hier sind deswegen datenschutzrechtliche Überlegungen von vornherein in die Reformvorhaben als integraler Bestandteil mit einzubeziehen.

1.8 Reformüberlegungen auch bei elektronischen Medien

Während es im Datenschutz bei Telediensten vornehmlich darum geht, die Anwendung des T eledienstedatenschutzgesetzes voranzubringen und diesem Gesetz flächendeckend Respekt und Beachtung zu verschaf fen (vgl. Nr. 11.2.2), bahnt sich für die elektronischen Medien die nächste Gesetzesänderung an. Nach den Reformüberlegungen des zuständigen Ministeriums für W irtschaft und Arbeit, die auf eine Entschließung des Deutschen Bundestages zurückgehen, sollen zum einen die Bereiche T eledienste, Mediendienste und Rundfunk in einem Gesetz zusammengeführt und so auch das entsprechende Datenschutzrecht vereinfacht werden, zum anderen soll die bestehende Datenschutzaufsicht in diesem Bereich durch fr eiwillige und eigenverantwortliche Selbstregulierung der Me dienwirtschaft ergänzt und entlastet werden (vgl. Nr. 11.2.1). Dieses Vorhaben, dessen nähere Ausgestaltung noch offen ist, passt sich gut in die generellen Überlegungen zur Reform des Datenschutzrechts an, bei denen es auch um V ereinfachung des Regelungsdickichts, Reduktion der spez ialgesetzlichen Vorschriften und um Ausbau von Selbstregulierung und Selbstkontrolle geht. Wenn auf diesem W eg das Datenschutzrecht überschaubarer, praktikabler wird und seine Einhaltung besser kontrolliert werden kann, verdienen entsprechende Reformbemühungen Unterstützung.

1.9 Genomanalyse – was ist zulässig?

Es gibt wohl keine personenbezogeneren Daten als das menschliche Genom. Durch de n technisch/medizinischen Fortschritt in der molekular genetischen Forschung und die daraus sich ergebende Möglichkeit von DNA-Analysen eröffnen sich ungeahnte Möglichkeiten, im Guten wie im Schlechten.

Im Bereich des Strafverfahrens gibt es zur Nutzung der DNA-Analyse bereits einschlägige Normen, die die Feststellung, Speicherung und V erwendung von DNA-Identifikationsmustern regeln (vgl. Nr. 8.2.3), aber noch immer sind

hierzu nicht alle Fragen geklärt. Zwar ist durch das Gesetz zur Änderung der Strafprozessordnung vom 6. August 2002 in § 81e StPO jetzt klargestellt worden, dass auch die Untersuchung von Spurenmaterial einer unbekannten Person nur durch den Richter angeordnet werden darf (vgl. Nr. 8.2.3.1). Eine entsprechende Klarstellung, dass auch DNA-Analysen für Zwecke künftiger Strafverfahren nach § 81g StPO und § 2 DNA-Identitätsfeststellungsgesetz ausschließlich aufgrund richterlicher Anordnung durchgeführt werden dürfen, fehlt aber nach wie vor (vgl. Nr. 8.2.3.3). Auch eine gesetzliche Regelung für die Durchführung von DNA-Massentests halte ich für erforderlich (vgl. Nr. 8.2.3.2). Skeptisch beurteile ich hingegen Überlegungen, den Straftatenkatalog des § 81g Abs. 1 StPO auszuweiten (vgl. 8.2.3.4) oder sogar vorsorglich von allen Bürgern oder allen Männern DNA-Identifizierungsmuster zu erheben und in eine DNA-Analyse-Datei einzustellen, was meines Erachtens eindeutig gegen das Grundgesetz verstieße (vgl. Nr. 13.3).

Ich sehe die Gefahr, dass der scheinbar objektive und unanfechtbare Beweiswert von Genanalysen neue Missbrauchsmöglichkeiten schaffen kann; das reicht vom Austausch oder der Manipulation von Genproben bis hin zum Legen falscher genetischer Spuren.

Aber der Einsatz von Genomanalysen beschränkt sich schon lange nicht mehr auf die Verbrechensbekämpfung und die Überführung von Straftätern. Ob es um die Feststellung von Kindschaftsverhältnissen geht, um den Abschluss von Lebens- oder Krankenversicherungsverträgen, um Einstellungen oder Kündigungen im Arbeitsleben, überall ist die Nutzung von Gentests denkbar oder wird sogar bereits praktiziert. Anders als im Strafverfahren fehlen hier aber spezielle rechtliche Regelungen und das allgemeine Datenschutzrecht reicht vielfach nicht aus, um Missbrauch entgegenzutreten, fairen Interessenausgleich zu gewährleisten und diesen Kernbereich der Persönlichkeit eines jeden Menschen wirkungsvoll zu schützen (vgl. Nr. 28.5).

Dies kann zu fatalen Konsequenzen führen, wenn nicht bald Rechtssicherheit geschaffen wird, was zulässig ist und was nicht. Zentrales Anliegen dabei ist, ein gegen jedermann gerichtetes, ausdrückliches und strafbewehrtes Verbot zu schaffen, ohne besondere Befugnis die Analyse des Genoms eines anderen durchzuführen oder durchführen zu lassen oder Ergebnisse einer entsprechenden Analyse zu verarbeiten oder zu nutzen.

Meiner Forderung nach einer entsprechenden umfassenden gesetzlichen Regelung wurde bislang nicht entsprochen, wenn ihre Berechtigung auch – soweit ersichtlich – allgemein anerkannt wird. Es ist sicher wichtig und richtig, ein solches Vorhaben gründlich vorzubereiten, zu diskutieren und wegen der länderübergreifenden Auswirkungen auch in den europäischen Kontext einzustellen. Dies darf aber nicht dazu führen, dass eine Regelung unvertretbar lange auf sich warten lässt und in der Zwischenzeit gesellschaftspolitische Fakten geschaffen werden, wie sich dies bei der heimlichen Überprüfung von Vaterschaften schon anbahnt.

1.10 Der Bürger wird geortet

Der technologische Fortschritt eröffnet immer neue Möglichkeiten, an die früher nicht zu denken war. Meist werden die Vorteile herausgestellt, die für den Einzelnen damit verbunden sind, die oft negative Kehrseite wird vielfach verschwiegen oder zumindest herunter gespielt. So werden zunehmend Systeme entwickelt, die es in technisch unterschiedlicher Weise und zu unterschiedlichen Zwecken erlauben, den genauen Aufenthalt eines Menschen festzustellen. Vielfach geschieht dies über das Handy, das heute weit verbreitet ist. So wurden im Berichtszeitraum in § 9 Abs. 4 Bundesverfassungsschutzgesetz und § 100i Strafprozessordnung die rechtlichen Grundlagen für den Einsatz des so genannten IMSI-Catchers geschaffen (vgl. Nr. 8.2.4), mit dessen Hilfe eine bestimmte Person über ihr Mobiltelefon geortet werden kann, aber auch eine Vielzahl weiterer Bürger, die sich zufällig in der Nähe aufhalten. Ortungsmöglichkeiten bieten inzwischen auch zusätzliche Funktionen im Handy und bestimmte Dienste in den Mobilfunknetzen (vgl. Nr. 11.10.4), die es erlauben, den genauen Standort des Handys und damit auch seines Inhabers zu bestimmen. Mit anderer Technik und zu anderen Zwecken erfolgt eine Ortung künftig auch im Zusammenhang mit der Mauterhebung für LKW auf deutschen Autobahnen (vgl. Nr. 29.1), die natürlich nicht nur Standort und Fahrtroute der LKW erfasst, sondern auch von deren Fahrern. Weitere Ortungsmöglichkeiten von Personen sind in der Entwicklung oder kommen sogar schon zum Einsatz.

All diesen Möglichkeiten und Systemen ist gemeinsam, dass sich gegen ihren Einsatz im Einzelfall, soweit er auf gesetzlicher Grundlage und unter Beachtung der datenschutzrechtlichen Bestimmungen erfolgt, grundsätzlich nichts sagen lässt: Es ist legitim, die neuen technischen Entwicklungen zu nutzen, um Terroristen zu bekämpfen oder Straftäter zu verfolgen, um Gefahren von Kindern abzuwehren, Menschen in Not aufzuspüren oder auch nur die Arbeit von Außendienstmitarbeitern zu optimieren oder verlorene Handys wiederzufinden. Zugleich werden aber technische Kontrollsysteme und eine Überwachungsstruktur aufgebaut, die, einmal vorhanden, auch noch zu ganz anderen Zwecken genutzt werden könnten und deren gesetzes- und datenschutzkonforme Anwendung letztlich nicht mehr kontrollierbar ist. Soft- und Hardware, die das Aufspüren von Menschen mit deren Einverständnis und zu ihrem Schutz erlauben, lassen sich technisch in gleicher Weise auch ohne das Einverständnis und zum Nachteil des Betroffenen einsetzen, und zwar auch dann, wenn dieser sich nichts hat zu schulden kommen lassen. Häufige Ortungen der gleichen Person erlauben darüber hinaus auch die Erstellung von Bewegungsprofilen. Auch hier zeigt sich wieder, dass die Summe von nützlichen und für sich gesehen datenschutzkonformen Anwendungen insgesamt ein Bedrohungspotenzial für das Grundrecht auf informationelle Selbstbestimmung darstellt, das von den Betroffenen und auch in der gesellschaftspolitischen Diskussion so zunächst nicht wahrgenommen wird. Umso wichtiger ist es, sich rechtzeitig Gedanken darüber zu machen, welche technischen und rechtlichen Voraussetzungen geschaffen werden müssen, um den Nutzen der neuen technologischen Möglichkeiten zu bewahren und die Bedrohung für das Persönlichkeitsrecht des Bürgers so gering wie möglich zu halten.

1.11 Biometrie – der Bürger wird vermessen

Nicht zuletzt aufgrund gestiegener Sicherheitsanforderungen und des Wunsches nach absolut täuschungs- oder fälschungssicherer Identifikation bzw. Verifikation von Personen rücken biometrische Verfahren immer mehr in den Blickpunkt

(vgl. Nr. 4.2). Nachdem es bislang wegen mangelnder technischer Einsatzreife entsprechender Verfahren mehr um theoretische Überlegungen ging, ist die Technik nun weiter ausgereift und es kommt zu ersten Modellversuchen und gesetzgeberischen Initiativen wie in § 4 Abs. 3 und 4 des Passgesetzes und in § 1 Abs. 4 und 5 des Gesetzes über Personalausweise. Weitere Einsatzmöglichkeiten in fast allen Lebensbereichen werden mehr oder weniger konkret diskutiert und es entsteht mitunter der Eindruck, biometrische Verfahren seien die sicherheitstechnische Lösung der Zukunft überall dort, wo die Identität einer Person zweifelsfrei festgestellt oder eine Person verifiziert werden soll. Es ist nicht meine Aufgabe zu beurteilen, ob die Biometrie das halten kann, was sich manch einer von ihr verspricht. Datenschutzrechtlich ist gegen den Einsatz entsprechender Verfahren grundsätzlich auch nichts einzuwenden, solange die Grundprinzipien des Datenschutzes wie Datensparsamkeit, Datensicherheit, Transparenz, strikte Zweckbindung, Erforderlichkeit und Verhältnismäßigkeit, um nur die wichtigsten zu nennen, beachtet werden. Auch darf es zu keinen zentralen Referenzdateien kommen, mit denen an verschiedenen Stellen und zu verschiedenen Zwecken erhobene biometrische Daten abgeglichen werden. Eine solche Entwicklung würde den Weg frei machen zu umfassender Profilbildung und Überwachung jeden einzelnen Bürgers und eine Vielzahl von Missbrauchsmöglichkeiten eröffnen. Um den fortschreitenden Einsatz biometrischer Verfahren in geregelte und grundrechtskonforme Bahnen zu lenken, wird zu prüfen sein, ob es hierfür spezieller datenschutzrechtlicher Normen bedarf.

1.12 Streit um Stasi-Unterlagen vorerst beendet

Der rechtspolitische Streit um die Herausgabe von Stasi-Abhörprotokollen prominenter Zeitgenossen hat sowohl die Öffentlichkeit als auch die Justiz über Jahre beschäftigt (vgl. Nr. 7.6.1), wobei zum Teil aus dem Blick geriet, worum es jenseits des konkreten Einzelfalls geht, nämlich um einen wirksamen Opferschutz und die Frage, ob rechtswidrig unter Verletzung elementarer Grundrechte erlangte Informationen über Personen gegen deren Willen weitergegeben und veröffentlicht werden dürfen, wenn es sich hierbei um Personen der Zeitgeschichte handelt. Meine in dieser Auseinandersetzung von Anfang an vertretene Rechtsauffassung ist im März 2002 vom Bundesverwaltungsgericht in letzter Instanz in vollem Umfang bestätigt worden.

Damit war die Angelegenheit aber noch nicht beendet. Da sich die Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR durch das Urteil gehindert sah, ihren Aufgaben hinsichtlich der historischen, politischen und juristischen Aufarbeitung der Tätigkeit des Staatssicherheitsdienstes bezogen auf Personen der Zeitgeschichte, Inhaber politischer Funktionen und Amtsträger im bisherigen Umfang nachzukommen, wurde eine Änderung des Stasi-Unterlagen-Gesetzes eingeleitet. Nach der ursprünglichen Fassung des entsprechenden Gesetzentwurfs wären die Wirkungen des Urteils des Bundesverwaltungsgerichts weitgehend aufgehoben und der Schutz prominenter Opfer des Staatssicherheitsdienstes der ehemaligen DDR erheblich eingeschränkt worden. Auch Informationen, die unter Verletzung des Brief-, Post- und Fernmeldegeheimnisses oder unter Verstoß gegen die Unverletzlichkeit der Wohnung gewonnen worden waren, hätten nach entsprechender Interessenabwägung durch die Bundesbeauftragte gegen den Willen der Betroffenen veröffentlicht werden können.

Im Laufe des Gesetzgebungsverfahrens ist es gelungen, einen verbesserten Opferschutz zu erreichen, auch wenn die Abwägungsklausel letztlich geblieben ist. Ich halte deswegen das Fünfte Gesetz zur Änderung des Stasi-Unterlagen-Gesetzes in der vom Deutschen Bundestag beschlossenen Fassung für vertretbar, wenn es verantwortungsbewusst im Interesse der Opfer angewandt wird, woran zu zweifeln ich keinen Anlass habe.

Wenn auch die Auseinandersetzung um die Herausgabe von Stasi-Unterlagen Prominenter mit der Entscheidung des Bundesverwaltungsgerichts und der Änderung des Stasi-Unterlagen-Gesetzes zunächst beendet ist, so ist die dahinter stehende Grundsatzproblematik, welche Beeinträchtigung ihrer Grundrechte im öffentlichen Leben stehende Persönlichkeiten hinnehmen müssen und wie weit insbesondere ihr allgemeines Persönlichkeitsrecht und ihr Recht auf informationelle Selbstbestimmung eingeschränkt ist, trotz einer Vielzahl von Urteilen zu Einzelfällen noch nicht abschließend geklärt.

1.13 Müssen Krankenkassen alles sehen?

Im Berichtszeitraum ist meine Rechtsauffassung auch noch in einem anderen Fall durch höchstrichterliche Entscheidung bestätigt worden: Das Bundessozialgericht hat im Juli 2002 festgestellt, dass die Krankenkassen nicht aus eigenem Recht Einsicht in Behandlungsunterlagen ihrer Versicherten verlangen können, sondern insoweit auf ein Tätigwerden des Medizinischen Dienstes der Krankenkassen angewiesen sind (vgl. Nr. 24.1.4). Dies kann auch nicht durch das Einholen entsprechender Einwilligungserklärungen der Versicherten zur Übermittlung von Behandlungsunterlagen umgangen werden. Diesem Urteil messe ich große Bedeutung bei, die über den entschiedenen Fall hinausreicht. Es stellt sich die gleiche Problematik bei der Frage, ob die Pflegekassen Einsicht in die Pflegedokumentation Pflegebedürftiger nehmen dürfen (vgl. Nr. 24.2.2). Auch hier vertrete ich die Auffassung, dass zwischen Abrechnungsunterlagen und der Pflegedokumentation, die unter anderem hochsensible Anamnese- und Diagnosedaten enthält, unterschieden werden muss und dass letztere nur an den Medizinischen Dienst der Krankenkassen übermittelt werden darf.

Bei den privaten Krankenversicherern ist die Situation nicht die gleiche, aber auch hier besteht Einigkeit, dass sensible Unterlagen wie etwa OP-Protokolle bei den Krankenhäusern nicht pauschal unter Hinweis auf eine generelle Einwilligung und Schweigepflichtentbindung des Versicherten angefordert werden dürfen, sondern nur, wenn dies im Einzelfall zur Feststellung der Leistungspflicht erforderlich ist (vgl. Nr. 28.7.2).

Zur Beurteilung der Leistungspflicht im Einzelfall erheben die privaten Krankenversicherungen der ärztlichen Schweigepflicht unterliegende Gesundheitsdaten bei Ärzten, Krankenhäusern sowie auch bei Rentenversicherungsträgern, soweit es beispielsweise um die Feststellung der Voraussetzungen für die Zahlung einer Berufsunfähigkeitsrente geht. Dabei wird auf eine allgemein gehaltene, in pauschaler Form abgegebene Schweigepflichtentbindungserklärung zurückgegriffen, die die Versicherten bei dem oftmals Jahre zurückliegenden Vertragsabschluss abgegeben haben. Meiner

Auffassung nach sind solche pauschalen und lange zurückliegenden Erklärungen keine hinreichende Grundlage für die Übermittlung von Gesundheitsdaten durch die meiner Aufsicht unterstehenden Rentenversicherungsträger. Auch Eingaben aus dem Bereich der privaten Krankenversicherung belegen, dass Versicherte sich zum Teil an die lange zurückliegenden Erklärungen zur Schweigepflichtentbindung gar nicht mehr erinnern. In einer gemeinsamen Arbeitsgruppe von Vertretern der Datenschutzaufsichtsbehörden und der Versicherungswirtschaft, an der auch ich mich beteilige, soll daher eine Überarbeitung des bisherigen Verfahrens angestrebt werden. Ziel ist, hier zu mehr Transparenz und einer Stärkung der Patientenrechte zu kommen.

1.14 Ausblick

Das Datenschutzrecht ist nicht statisch, sondern ständig im Fluss. Durch den technologischen Fortschritt sowie politische, wirtschaftliche und gesellschaftliche Veränderungen ergeben sich ständig neue Themen und Problemfelder, für die es eine adäquate datenschutzrechtliche Antwort zu finden gilt. Dabei geht es im Kern immer darum, das vom Grundgesetz geschützte Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung jeden Bürgers in immer wieder verändertem Umfeld und gegen ständig neue Herausforderungen zu verteidigen und zu sichern. In meinem kurzen Überblick habe ich versucht, einige der Themen zu skizzieren, die im Berichtszeitraum die datenschutzrechtliche Diskussion bestimmt haben. Einige der Probleme sind mehr oder weniger zufriedenstellend gelöst, bei anderen befindet sich die Lösung zumindest in Arbeit, als Teil der ständigen Fortschreibung des Datenschutzrechts in Deutschland. Der rein nationale Rahmen ist aber vielfach schon zu eng. Fortschreitende Globalisierung und im wahrsten Sinne des Wortes grenzenloser Datenfluss machen eine Einbindung dieses Rechts in einen gesamteuropäischen Rahmen oder darüber hinaus sogar internationale Vereinbarungen immer wichtiger. Das beste Datenschutzrecht bleibt wirkungslos, wenn es vom Ausland aus problemlos umgangen werden kann und selbst schwere Verstöße gegen datenschutzrechtliche Bestimmungen sanktionslos bleiben, weil die verantwortliche Stelle unerreichbar im ferneren Ausland ihren Sitz hat.

An dieser Stelle möchte ich den Blick aber auch auf einige Themen lenken, die zurzeit noch nicht im Zentrum der aktuellen Datenschutzdiskussion stehen, aber in Zukunft durchaus Brisanz entfalten könnten:

Weiter oben (Nr. 1.2) habe ich bereits darauf hingewiesen, dass die korrekte Umsetzung und Beachtung datenschutzrechtlicher Bestimmungen noch lange nicht überall gewährleistet ist. Die Datenschutzaufsichtsbehörden können in der Regel nur Eingaben und Beschwerden nachgehen oder allenfalls stichprobenartig anlassunabhängige Kontrollen durchführen. Das Risiko bei der Missachtung geltenden Datenschutzrechts ist deswegen insbesondere im nicht öffentlichen Bereich immer noch relativ gering und der Bürger reagiert mit Unverständnis und Hilflosigkeit, wenn er den Eindruck gewinnen muss, der Schutz seines Grundrechts auf informationelle Selbstbestimmung bestehe häufig nur auf dem Papier. Ich halte deswegen Überlegungen, wie der Gesetzesvollzug weiter verbessert werden kann, für erforderlich. Auch die Struktur der Datenschutzaufsicht in Deutschland ist für Außenstehende schwer durchschaubar, wie ich anhand vieler fehlgeleiteter schriftlicher oder mündlicher Anfragen und Beschwerden immer wieder feststellen muss. Lässt sich die unterschiedliche Kontrollzuständigkeit für Bundes- und Landes- bzw. Kommunalbehörden schon allein aufgrund der unterschiedlichen Rechtsgrundlagen noch gut vermitteln, so erschließt sich die Zuständigkeit der verschiedenen Aufsichtsbehörden der Länder für Beratung und Kontrolle des nicht öffentlichen Bereichs trotz einheitlicher Rechtsgrundlage im Bundesdatenschutzgesetz vielen Bürgern nicht. In Kreisen der Wirtschaft werden mitunter die schwierigen und vor allem zeitaufwendigen Abstimmungsverfahren beklagt, wenn es um datenschutzrechtliche Fragen und Gesetzesauslegungen geht, die bundeseinheitlich geklärt sein müssen oder sogar international Auswirkungen haben. Es wäre im Zuge der Neuordnung des Datenschutzrechts zu erwägen, für international oder bundesweit operierende Großunternehmen und Verbände eine zentrale Aufsichtsstelle zu schaffen, mit der Datenschutzfragen verbindlich und schnell geklärt werden können. Dies würde nach meiner Überzeugung die Belange des Datenschutzes im nicht öffentlichen Bereich fördern.

Anlass zu Sorge geben auch die ständig anwachsenden Datenbestände und ihre vielfältigen Verknüpfungsmöglichkeiten, und zwar sowohl im öffentlichen wie auch im nicht öffentlichen Bereich. Es scheint mir deswegen angebracht zu sein, noch einmal die Worte des Bundesverfassungsgerichts in Erinnerung zu rufen, mit denen es das Grundrecht auf informationelle Selbstbestimmung begründet hat. Dort heißt es zur Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden:

„Diese Befugnis bedarf unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes. Sie ist vor allem deshalb gefährdet, weil bei Entscheidungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muss, vielmehr heute mit Hilfe der automatischen Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (personenbezogene Daten [vgl. § 2 Abs. 1 BDSG]) technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind. Sie können darüber hinaus – vor allem beim Aufbau integrierter Informationssysteme – mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekannten Weise die Möglichkeiten einer Einsichts- und Einflußnahme erweitert, welche auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen. Individuelle Selbstbestimmung setzt aber – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten“ (BVerfG, Urteil vom 15. Dezember 1983 – 1BvR 209/83 u. a.).

Genau diese Entwicklung tritt heute aber ein, wenn hierfür vielfach auch Gesichtspunkte der Kostensenkung, der Modernität und Effizienz ins Feld geführt werden. Dadurch

können erhebliche Datenmissbrauchspotenziale entstehen, deren Kontrolle aufgrund fehlender T ransparenz immer schwieriger wird.

Dabei geht gerade auch in der Privatwirtschaft der Trend zu immer umfangreicheren Datensammlungen und Datenverbänden. So wird das Netz von allen möglichen Warndateien immer dichter. Neben zahlreichen Kreditauskunftssystemen entwickelt jetzt die W ohnungswirtschaft eigene W arndateien (vgl. Nr. 10.8), so auch eine bei der SCHUFA (vgl. Nr. 10.5.1), und auch die V ersicherungswirtschaft verfügt über ein zentrales Hinweissystem. Dabei besteht ein legitimes Interesse der Wirtschaft, sich vor Betrügern, schwarzen Schafen und zahlungsunfähigen oder -unwilligen Kunden zu schützen und die einzelne Datei oder das einzelne Auskunftssystem ist im Regelfall datenschutzrechtlich nicht zu beanstanden. Gefahren sehe ich dort, wo die einzelnen Systeme zusammengeschaltet werden können oder einzelne Institutionen aus allen Systemen Informationen abrufen und so den einzelnen Kunden für sich gläsern machen können. Es darf nicht dazu kommen, dass z. B. ein junger Mensch, der mit zwanzig seine Handyrechnung nicht bezahlen konnte, anschließend kein Konto mehr eröffnen kann, keine Wohnung findet, keine Versicherung abschließen kann und sozusagen auf Dauer zur elektronischen Unperson wird. So weit sind wir zum Glück noch nicht, aber die sich abzeichnende Entwicklung könnte eine solche Richtung nehmen, wobei alle möglichen privat or ganisierten „schwarzen Listen“ im Internet noch ein zusätzliches Problem darstellen. Noch viel schlimmer sind solche Entwicklungen, wenn der einzelne Bürger auch noch ohne eigenes Fehlverhalten in das elektronische Warnsystem gerät, sei es aufgrund einer Verwechselung oder durch nachlässiges oder nicht vertragskonformes Meldeverhalten der einzelnen Teilnehmer solcher Systeme. Hierfür gibt es leider immer wieder Beispiele, die bis an den Rand der Existenzvernichtung gehen können. Hier sind Regelungen, die es in einer solchen Situation nicht allein dem einzelnen Betrof fenen überlassen, den Kampf mit der Hydra der elektronischen W arnsysteme aufzunehmen, dringend geboten, etwa in Form eines „Folgenbeseitigungsanspruchs“, der bei W eitergabe unrichtiger Informationen oder bei rechtswidrigen Übermittlungen der verantwortlichen Stelle aufgibt, daraus resultierende Folgen für den Betroffenen selbst zu beseitigen, und zwar nicht nur im eigenen System, sondern auch überall dort, wo sich durch Fortpflanzung des Fehlers für den Betrof fenen nachteilige Auswirkungen ergeben. Zahlreiche Eingaben bei mir belegen, dass dies kein nur th eoretisches Problem ist, das nicht juristisch geschulte Bürger vielfach überfordert.

Auch im Bereich von W erbung, Markt- und Meinungsforschung werden mit immer neuen Ideen immer mehr Kundendaten zusammengetragen und ausgewertet, um zu immer ausgefeilteren Kundenprofilen zu kommen. Dabei halte ich Profilbildungen hier wie auch in anderen Bereichen generell für fragwürdig. Das Zusammenstellen von personenbezogenen Daten eines bestimmten Menschen, das sein V erhalten ganz oder teilweise abbildet und ihn dadurch für Dritte berechen- und verfügbar macht, ist schon dann problematisch, wenn dies mit seinem W issen geschieht, weil er im Zweifelsfall die weit reichenden K onsequenzen nicht abschätzen kann. Erfolgt dies aber hinter seinem Rücken und noch dazu mittels heimlicher Datenerh ebungen oder -übermittlungen, liegt ein schwerer Verstoß gegen das informationelle Selbstbestimmungsrecht vor. Leider bieten die technologische Entwicklung und der rasant wachsende Bestand von personenbezogenen Daten auf alle n Gebieten immer bessere Möglichkeiten, zu ausgefeilt en Profilbildungen zu gelangen. Auch hier könnte in Zukunft der Gesetzgeber gefordert sein.

1.15 Hinweise für die Ausschüsse des Deutschen Bundestages, Beratungen und Kontrollen, Beanstandungen

Auch diesmal habe ich in der Anlage 1 zusammengefasst, welche Kapitel und Abschnitte dieses Berichts für welchen Ausschuss des Deutschen Bundestages von besonderem Interesse sein könnten.

Anlage 2 gibt einen Überblick über die von mir und meinen Mitarbeitern durchgeführten Kontrollen, Beratungen und Informationsbesuche. Diese Tätigkeit ist ein Kernbereich meiner Arbeit. Die Kenntnisse und Einblicke, die ich bei Prüfungen und Gesprächen vor Ort in den meiner Zuständigkeit unterfallenden öffentlichen Stellen des Bundes, T elekommunikations- und Postdi enstleistungsunternehmen und privaten Unternehmen, die unter das Sicherheitsüberprüfungsgesetz fallen, gewinne, sind wichtig und wertvoll für meine Beratung des Deutschen Bundestages und der Bundesregierung. Sie stellen eine V erbindung dar zu den Bedürfnissen und Problemen in der Praxis und helfen umgekehrt, die Intentionen der datenschutzrechtlichen V orschriften zu verdeutlichen und ihre volle Anwendung zu verbessern.

Allerdings muss ich dabei mitunter auch Verstöße gegen die Vorschriften des Bundesdatenschutzgesetzes oder andere datenschutzrechtliche Bestimmungen wie das T elekommunikationsgesetz oder Postgesetz feststellen oder sonstige Mängel bei der V erarbeitung oder Nutzung personenbezogener Daten, die ich nach § 25 BDSG förmlich zu beanstanden habe. Von einer Beanstandung kann ich absehen, wenn die Verstöße oder Mängel von geringer Bedeutung sind oder sofort beseitigt werden. Eine Übersicht über die ausgesprochenen Beanstandungen enthält Anlage 3. Dabei ist bemerkenswert, dass die Zahl der Beanstandungen im Berichtszeitraum im Vergleich zu mein em letzten Tätigkeitsbericht deutlich angestiegen ist.

2 Der 11. September 2001 und seine datenschutzrechtlichen Auswirkungen – Zäsur auch für den Datenschutz

2.1 Öffentliche Sicherheit und Datenschutz – gestörte Balance?

Der 11. September 2001 erschütterte das Sicherheitsempfinden vor allem der westlichen W elt nachhaltig. Die Anschläge auf Djerba und Bali im ver gangenen Jahr zeigten zudem deutlich, dass der internationale T errorismus seinen Feldzug fortsetzt.

Die sofort nach den beispiellosen T errorakten in New York und Washington einsetzende Diskussion um präventiv wirksame Antiterrormaßnahmen verdeutlichte klar das intensive Spannungsverhältnis zwischen den Sicherheitsinteressen des Staates und den durch staa tliche Eingriffsbefugnisse zwangsläufig betroffenen Freiheitsrechten der Bür gerinnen und Bürger. Staatliches Handeln als Antwort auf die – nach

wie vor – akute Bedrohungslage war unabweisbar; neue Befugnisse der Sicherheitsbehörden schienen zwingend geboten. Es stellte sich aber die Frage nach dem Verhältnis zum Grundrecht auf informationelle Selbstbestimmung mit der auch politisch gebotenen Prämisse, sich von Terroristen nicht den Abbau von Bürgerrechten aufzwingen zu lassen.

Bei der Fülle geplanter neuer Maßnahmen zur Terrorismusbekämpfung verbunden mit Befugnissen der Sicherheitsbehörden, die tiefe Eingriffe in das Persönlichkeitsrecht auch unbescholtener und unbeteiligter Bürger bedingen, ging es aus der Sicht des Datenschutzes vor allem darum, die Balance zwischen dem nachvollziehbaren Sicherheitsinteresse des Staates für seine Bürger und den schutzwürdigen Freiheitsrechten des Einzelnen zu halten, zumindest deren Kernbereich zu wahren.

In der politischen Diskussion unmittelbar nach den Anschlägen gab es deutliche Aussagen, den „Datenschutz tiefer zu hängen", verbunden mit der Aufforderung, angebliche Hürden des Datenschutzes in Richtung auf eine effiziente Antiterrorgesetzgebung nicht mehr oder nur noch beschränkt zu dulden. Dagegen wandten sich die Datenschutzbeauftragten des Bundes und der Länder bereits mit der Entschließung vom 1. Oktober 2001 (s. Anlage 17) und weiter mit der Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (s. Anlage 18). Hierin bekräftigen sie die Auffassung, dass bei der künftigen Gesetzgebung die grundlegenden Rechtsstaatsprinzipien, nämlich das Grundrecht der freien Entfaltung der Persönlichkeit, das Verhältnismäßigkeitsprinzip und der Erforderlichkeitsgrundsatz zu beachten sind („diese verfassungsrechtlichen Garantien prägen den Rechtsstaat, den wir gemeinsam zu verteidigen haben").

Die Datenschutzbeauftragten verdeutlichten gleichwohl, dass sie zu einem „offenen und konstruktiven Dialog über etwa notwendige Anpassungen an die neue Bedrohungslage bereit" seien.

Ich habe schon im Vorfeld des ersten Arbeitsentwurfs des BMI vom 12. Oktober 2001 (s. Nr. 2.2.2) deutlich gemacht, den Kampf des demokratischen Rechtsstaats gegen den Terrorismus mit Nachdruck zu unterstützen. Dabei war mir wichtig klarzustellen, dass einige Forderungen auch aus meiner Sicht eher vertreten werden könnten, wenn sie befristet und einer Erfolgskontrolle (Evaluierung) unterworfen würden (s. Nr. 2.3.1).

2.2 Gesetzgebungsverfahren zum Terrorismusbekämpfungsgesetz

Zentrales Anliegen der Bundesregierung war die Früherkennung terroristischer Planungen, d. h. die Ziel- und Zweckrichtung der geplanten Sicherheitsmaßnahmen sollten in erster Linie präventiv wirken. Vor allem daran musste sich auch aus datenschutzrechtlicher Sicht das umfangreiche Gesetzespaket, als Sicherheitspaket I und II bezeichnet, messen lassen.

2.2.1 Sicherheitspaket I

Das Sicherheitspaket I enthielt vor allem die Änderungen des Vereinsgesetzes (Aufhebung des so genannten Religionsprivilegs) und die Luftverkehrs-Zuverlässigkeitsüberprüfungsverordnung (s. Nr. 20.2).

Die hier bereits beabsichtigte Einführung des § 129b Strafgesetzbuch (StGB), also die Erweiterung des Anwendungsbereichs der §§ 129, 129a StGB auf kriminelle und terroristische Vereinigungen weltweit, blieb in der Koalition lange strittig und wurde erst am 30. August 2002 wirksam.

2.2.2 Sicherheitspaket II – Terrorismusbekämpfungsgesetz – Referentenentwurf aus dem BMI vom 12. Oktober 2001

Dieser Entwurf, den ich eher als ein Diskussionspapier angesehen habe, vermittelte nicht nur bei Datenschützern den Eindruck, als ob hier alle nur denkbaren und gesetzestechnisch machbaren Möglichkeiten aufgelistet worden seien, teilweise ohne realen Bezug zur Terrorismusbekämpfung. Insbesondere berücksichtigte der Entwurf die in weiten Teilen im Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 formulierten datenschutzrechtlichen Vorgaben an Gesetze nicht. Er enthielt vielmehr sehr pauschale, nicht zielgenau auf konkrete Gefährdungssituationen im terroristischen Bereich ausgerichtete neue Eingrifsbefugnisse und begegnete damit zu Recht, auch innerhalb der Bundesregierung, vielfältiger Kritik. Datenschutzrechtlich problematisiert habe ich insbesondere folgende Defizite dieses ersten Entwurfs:

- Keine Befristung der neuen Befugnisse der Sicherheitsdienste;
- keine Verpflichtung zur Evaluierung;
- keine Benachrichtigungspflicht an den Betroffenen bei Auskunftsbegehren der Nachrichtendienste gegenüber Kreditinstituten, Anbietern von Postdiensten, Telekommunikations- und Telediensten sowie Luftfahrtunternehmen;
- keine Konkretisierung der biometrischen Daten im Gesetz, die in Pässe und Personalausweise aufgenommen werden sollten. Dies sollte durch Rechtsverordnung des BMI im Benehmen mit dem AA erfolgen;
- Initiativ-Ermittlungsbefugnis des BKA zur Verdachtsgewinnung.

2.2.3 Gesetzentwurf zur Bekämpfung des internationalen Terrorismus vom 15. November 2001 (Terrorismusbekämpfungsgesetz – Bundestagsdrucksache 14/7386)

Der Entwurf in der Fassung der Vorlage, der das Bundeskabinett am 7. November 2001 zugestimmt hat und der als Gesetzentwurf der Bundesregierung wortgleich mit dem Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN zur Bekämpfung des internationalen Terrorismus vom 15. November 2001 (Terrorismusbekämpfungsgesetz – Bundestagsdrucksache 14/7386) war, enthielt dann jedoch gegenüber dem vorgenannten Referentenentwurf erste wesentliche datenschutzrechtliche Verbesserungen, wie beispielsweise die

- Streichung der Initiativ-Ermittlungsbefugnis des BKA;
- Befristung der Neuregelungen im Bundesverfassungsschutzgesetz (BVerfSchG), MAD-Gesetz, BND-Gesetz, Artikel 10-Gesetz (G10) und im Sicherheitsüberprüfungsgesetz (SÜG) auf fünf Jahre;

- Evaluierung der weiteren Befugnisse in der Begründung zu Artikel 22 des Entwurfs;
- Einführung einer Berichtspflicht bei Auskunftsbegehren des BfV gegenüber Kreditinstituten, Finanzdienstleistungsinstituten, Finanzunternehmen und Luftfahrtunternehmen, (nicht jedoch bei Post-, Telekommunikations- und Teledienstean bietern);
- erste Schritte in Richtung einer Benachrichtigung der Betroffenen über die durchgeführten Maßnahmen;
- Festlegung der Anordnungsbefugnisse auf der Ebene Behördenleitung bzw. zuständiges Ministerium;
- Einführung einer Zweckbindungsregelung bei Auskunftsbegehren des BfV gegenüber Kreditinstituten und Luftfahrtunternehmen;
- Konkretisierung der biometrischen Daten, die in Pässe und Personalausweise aufgenommen werden können, im Gesetzentwurf. Weitere Einzelheiten sollten einem künftigen Bundesgesetz vorbehalten bleiben.

2.3 Datenschutzrechtliche Verbesserungen „in letzter Minute“

Es verblieben dennoch eine Reihe erheblicher datenschutzrechtlicher Defizite, die ich in meiner Stellungnahme vom 21. November 2001 für die am 30. November 2001 durchgeführte Anhörung zum Entwurf des Terrorismusbekämpfungsgesetzes und in meiner Stellungnahme vom 7. Dezember 2001 vor allem den Mitgliedern des zuständigen Innenausschusses des Deutschen Bundestages näher erläutert habe.

Meine Kritikpunkte waren im Wesentlichen folgende:

2.3.1 Evaluierung und strukturierte Berichtspflichten

Der Gesetzentwurf selbst enthielt – im Gegensatz zur Berichtspflicht bei Auskunftsbegehren des BfV – noch keine Verpflichtung zu einer Evaluierung der weit reichenden neuen Befugnisse der Nachrichtendienste bei Auskunftsbegehren gegenüber privaten Stellen/Wirtschaftsunternehmen wie Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen (§ 8 Abs. 5 BVerfSchG), Postdienstunternehmen (§ 8 Abs. 6 BVerfSchG), Luftfahrtunternehmen (§ 8 Abs. 7 BVerfSchG) sowie Anbietern von Telekommunikations- und Telediensten (§ 8 Abs. 8 BVerfSchG). Gerade bei solch tiefen Eingriffen in die Persönlichkeitsrechte der Bürgerinnen und Bürger, etwa bei Auskünften durch Banken ohne einen konkreten strafrechtlichen Anfangsverdacht, sind aber Ergebnisse über die Effizienz der vom Parlament verliehenen Befugnisse von besonderer Bedeutung. Es liegt auf der Hand, dass eine umfassende und ergebnisoffene Erfolgskontrolle nur dann wirksam durchgeführt werden kann, wenn entsprechend detailliertes Datenmaterial zur Verfügung steht. Daher kam es mir darauf an, im Normtext auch inhaltlich geregelt zu wissen, dass die dem Parlamentarischen Kontrollgremium (PKGr) halbjährlich zu liefernden Berichte der zuständigen Ministerien über die Anwendung der neuen Befugnisse umfassende Informationen und Aussagen über Anlass, Umfang, Dauer, Ergebnis und Kosten der im Berichtszeitraum erfolgten Maßnahmen enthalten (vgl. § 100e Strafprozessordnung [StPO], der die Berichtspflicht für Maßnahmen im Zusammenhang mit der akustischen Wohnraumüberwachung normiert). Diese Berichte, darauf habe ich besonders hingewiesen, sollten durch das entsprechend strukturierte Datenmaterial Grundlage für eine Evaluierung durch das PKGr des Deutschen Bundestages rechtzeitig vor Ablauf der fünfjährigen Befristung der neuen Befugnisse der Nachrichtendienste und der Änderungen des SÜG sein. Sie stellen für mich praktisch die datenschutzrechtliche Grundlagenforschung dar, um die Frage nach der verfassungs- und datenschutzrechtlichen Erforderlichkeit und Verhältnismäßigkeit der Maßnahmen beantworten zu können.

Noch nicht vorgesehen in diesem Entwurf war die Pflicht zur halbjährlichen Berichterstattung für Auskünfte von Postdienstleistern, Anbietern von Telekommunikations- und Telediensten sowie für den Einsatz des so genannten IMSI-Catcher, der den Diensten die Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes ermöglichen soll (s. Nr. 17.1 und Nr. 8.2.4); ebenso nicht für die neuen Befugnisse im MAD-Gesetz und – z. T. – im BND-Gesetz.

Der Gesetzgeber hat dann allerdings auf der Grundlage des umfangreichen Änderungsantrages der Koalitionsfraktionen von SPD und BÜNDNIS 90/DIE GRÜNEN vor der für den 12. Dezember 2001 angesetzten „abschließenden“ Beratung des Entwurfs im Innenausschuss detaillierte Berichtspflichten im o. a. Sinne für die neuen Befugnisse der Nachrichtendienste in den Dienstegesetzen (s. z. B. § 8 Abs. 10 BVerfSchG) geregelt und die Evaluierung der neuen Regelungen vor Ablauf der Befristung normiert (s. z. B. § 8 Abs. 10 BVerfSchG – s. Nr. 2.5).

Hinzuweisen ist jedoch darauf, dass § 8 Abs. 10 BVerfSchG mit der Begründung des Gesetzentwurfs nicht vollständig übereinstimmt. Der Gesetzestext, der über Verweisungen auch für die neuen Befugnisse des MAD (s. Nr. 18.1) und des BND (s. Nr. 19.1) gilt, führt aus, dass das PKGr dem Deutschen Bundestag jährlich sowie nach Ablauf von drei Jahren nach In-Kraft-Treten des Terrorismusbekämpfungsgesetzes zusammenfassend zum Zweck der Evaluierung einen Bericht erstattet. In der Begründung (Bundestagsdrucksache 14/7864 vom 13. Dezember 2001) heißt es allerdings, dass das PKGr drei Jahre nach In-Kraft-Treten des Gesetzes einen zusammenfassenden Evaluierungsbericht an den Deutschen Bundestag zu erstatten hat.

Ich gehe davon aus, dass das PKGr die Evaluierung, ggf. mit wissenschaftlicher Begleitung, auf der Grundlage der Berichte der Ministerien durchführen soll (s. auch Nr. 2.4).

2.3.2 Normenklare Regelung im Sicherheitsüberprüfungsgesetz

Die beabsichtigte Einführung eines vorbeugenden personellen Sabotageschutzes mit erweiterten Aufgaben des BfV ging weit über den bisherigen Anwendungsbereich des SÜG, also den personellen Geheimschutz, hinaus.

Um den Kreis der von solchen weit reichenden Überprüfungsmaßnahmen betroffenen Personen und Bereichen der Wirtschaft und des öffentlichen Dienstes einzugrenzen, habe ich gefordert, nach dem Bestimmtheitsgrundsatz die Voraussetzungen für die im Gesetz genannte „sicherheitsempfindliche Stelle“ im Gesetz selbst zu definieren.

Der Gesetzgeber ist dieser Forderung gefolgt; die Regelungen zum vorbeugenden Sabotageschutz sind normenklar

gefasst worden und unterliegen ebenfalls einer Erfolgskontrolle (s. im einzelnen Nr. 20.1).

2.3.3 Bundeskriminalamt als Zentralstelle

Von der angestrebten Ergänzung des § 7 Abs. 2 BKA-Gesetz, einer Art originärer Datenerhebung durch das BKA, habe ich abgeraten: In seiner Funktion als Zentralstelle zur Unterstützung der Polizeien des Bundes und der Länder ist es eine wesentliche Aufgabe des BKA, die von diesen Stellen übermittelten Informationen zu sammeln und auszuwerten (§ 2 BKA-Gesetz). Es ist daher – entsprechend der geltenden Rechtslage – sachgerecht, wenn sich das BKA bei einer notwendigen Ergänzung der übermittelten Informationen zunächst an die ursprünglic he Stelle der Polizeien des Bundes und der Länder wendet, zumal diese wegen der ihnen obliegenden Strafverfolgungszuständigkeit die vorhandenen Informationsdefizite kompetenter ausgleichen können als andere öffentliche oder nicht öffentliche Stellen.

Der Gesetzgeber ist zwar diesen Bedenken nicht gefolgt. Die Neufassung des § 7 Abs. 2 Satz 2 BKA-Gesetz ist jedoch ebenfalls auf fünf Jahre befristet worden und einer Evaluierung zu unterziehen.

Anders als bei den neuen Befugnissen der Nachrichtendienste ist jedoch das Verfahren, vor allem der Inhalt der Berichtspflichten, nicht gesetzlich geregelt worden und somit im Detail noch festzulegen.

2.3.4 Keine Zentraldatei mit biometrischen Daten

Zwar war in diesem Gesetzentwurf insofern bereits eine wesentliche Verbesserung enthalten, als zu den biometrischen Merkmalen auch „die Art ihrer Speicherung, ihrer sonstigen Verarbeitungen und ihrer Nutzung“ durch (Bundes)Gesetz geregelt werden sollten. Ich habe aber nachdrücklich darauf hingewiesen, dass damit die Grundlage zu überregionalen/zentralisierten Referenzdateien bzw. einer Referenzdatei als einer Zentraldatei gelegt worden wäre. Nach meinen Erfahrungen birgt eine solche Datensammlung immer die Gefahr, dass sie nicht allein zu dem ursprünglich gedachten Zweck, hier zur Identifikation von Personen, genutzt, sondern nachfolgend auch von Polizei, Geheimdiensten oder gar zu kommerziellen Zwecken ausgewertet wird. Ich habe daher nachdrücklich vorgeschlagen, die Unzulässigkeit einer solchen Einrichtung im Gesetz ausdrücklich festzulegen.

Dem ist der Gesetzgeber gefolgt und hat eine zentrale Erfassung biometrischer Daten in einer Zentraldatei ausdrücklich gesetzlich ausgeschlossen.

2.3.5 Einbeziehung von Gesundheitsdaten in die Rasterfahndung

Die – zunächst – vorgesehene Änderung des § 68 des Zehnten Buches Sozialgesetzbuch (SGB X) habe ich für zu weitgehend gehalten. Bei den Sozialdaten handelt es sich um personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen (s. § 35 SGB I). Die Sozialdaten umfassen in erheblichem Umfang insbesondere Angaben zur Gesundheit des Betroffenen. Diese sensiblen Daten bedürfen eines besonderen Schutzes, wie er auch in Artikel 8 der EG-Datenschutzrichtlinie zum Ausdruck kommt. Sie sollten nicht in die Rasterfahndung einbezogen werden. Die Polizeigesetze einiger Länder (z. B. Hamburg und Nordrhein-Westfalen) schließen dies ausdrücklich aus.

Der Gesetzgeber ist meinen Bedenken gefolgt.

2.4 Ohne Resonanz blieb folgende Kritik

2.4.1 Online-Zugriff der Nachrichtendienste auf das Ausländerzentralregister

Den in § 22 des Gesetzes über das Ausländerzentralregister vorgesehenen nunmehr uneingeschränkten Online-Zugriff der Dienste auf den gesamten Datenbestand des Ausländerzentralregisters (AZR) habe ich kritisiert. Das AZR hat die Aufgabe, die mit der Durchführung ausländer - oder asylrechtlicher Vorschriften betrauten Behörden und andere Stellen zu unterstützen. Vor diesem Hintergrund habe ich darauf hingewiesen, dass das AZR mit dem o. a. Direktzugriff auch bei einer abstrakten Gefährdungslage eine neue Qualität erhielte; es würde in ein polizei- bzw. nachrichtendienstliches Register verändert.

Der Gesetzgeber ist meinen Bedenken leider nicht gefolgt.

2.4.2 Fingerabdruckdaten von Asylbewerbern

Mit der Neuregelung des § 16 Abs. 5 Asylverfahrensgesetz werden die von Asylbewerbern gemäß § 16 Abs. 1 Asylverfahrensgesetz erhobenen Fingerabdruckdaten, die von der eigentlichen Zweckbestimmung her der Identitätsfeststellung dienen und nur im Einzelfall zur Aufklärung einer Straftat oder zur Gefahrenabwehr herangezogen werden können, den auf der Grundlage des § 81b StPO bzw. der Polizeigesetze der Länder erhobenen Fingerabdrücken von Beschuldigten und Verdächtigen gleichgestellt. Gegen diese Neuregelung habe ich auch aus Gründen der Verhältnismäßigkeit erhebliche Zweifel geäußert.

Der Gesetzgeber ist meinen Bedenken leider nicht gefolgt.

2.5 Fazit und Ausblick

Auch wenn ich – wie dar gelegt – nicht mit allen Ergebnissen zufrieden bin, sehe ich bei dem Vergleich der „Ausgangslage“ im ersten Arbeitsentwurf eines Terrorismusbekämpfungsgesetzes vom 12. Oktober 2001 mit dem am 1. Januar 2002 in Kraft getretenen Gesetzespaket eine hinnehmbare Kompromisslösung mit einer Reihe von erfreulichen datenschutzrechtlichen Fortschritten. Dies gilt in erster Linie für die Evaluierung und Befristung der neuen Befugnisse der Sicherheitsbehörden. Erstmals werden die Voraussetzungen für eine Erfolgskontrolle und die Verpflichtung zur Evaluierung im Sicherheitsbereich gesetzlich geregelt (Artikel 22 Abs. 3). Es gilt der Vorbehalt, dass die entsprechenden Maßnahmen erforderlich, geeignet und verhältnismäßig sein müssen. Dies ist im Rahmen der Evaluierung auf der Grundlage aussagekräftiger Berichte der Bundesregierung zu prüfen, d. h. die gesammelten Erfahrungen müssen gründlich ausgewertet werden.

Es sind nicht wenige, die ihre Skepsis artikulieren, ob denn die Gesetzesevaluierung tatsächlich mit dem erforderlichen Nachdruck durchgeführt werde. Auch das Know-how muss vorhanden sein – schließlich geht es bei der Evaluierung um die Beurteilung und Bewertung der Wirkung staatlicher Programme und Maßnahmen mit wissenschaftlichen Methoden. Zurückgreifen – hoffe ich – könnte man auf die dann

(endlich) vorliegenden Erfahrungen aus dem Forschungsauftrag des BMJ an das Max-Planck-Institut zur Evaluierung der Telefonüberwachung nach § 100a StPO (vgl. auch Nr. 8.3), die Erkenntnisse aus dem – anfangs im Hinblick auf das unzureichende Datenmaterial unbefriedigenden – Berichtsverfahren nach § 100e StPO und die Ergebnisse im Bereich der akustischen Wohnraumüberwachung (vgl. auch Nr. 8.4). Jedenfalls ist im Koalitionsvertrag bekräftigt worden, die Evaluierung „bis Mitte der Legislaturperiode" vorzunehmen.

Die – hoffentlich – vor allem in präventiver Hinsicht greifenden Maßnahmen im Terrorismusbekämpfungsgesetz haben sich nach alledem einer kritischen Begleitung zu stellen. Dies sollte durch die lückenlose Kontrollfunktion der G10-Kommission, des PKGr und meiner Behörde – entsprechende Kontrollinstitutionen gibt es auch auf Länderebene – sowie durch die nunmehr gesetzlich geregelte Berichts- und Evaluierungspflicht möglich sein. Meine Aufgabe sehe ich auch darin, die Öffentlichkeit und die Medien hinsichtlich der Anwendung und des Nutzens der neuen Befugnisse im Terrorismusbekämpfungsgesetz zu sensibilisieren.

Es bleibt abzuwarten, wie die neuen Befugnisnormen greifen. Daher habe ich den neuerlichen Vorstoß einiger Länder, Internetanbieter verpflichten zu wollen, sämtliche Nutzungsdaten ihrer Kunden monate- oder gar jahrelang zu speichern und auf Anforderung an die Polizei, die Staatsanwaltschaft und sogar die Nachrichtendienste herauszugeben, abgelehnt. Mit einer solchen Vorratsspeicherung persönlicher Daten von Millionen rechtstreuer Bürger würde der Grundsatz, dass erst ein Anfangsverdacht bestehen muss bevor die Polizei ermitteln darf, auf den Kopf gestellt.

3 Die notwendige Erneuerung des Datenschutzes

3.1 Weiterentwicklung des Datenschutzrechts

In meinen letzten Tätigkeitsberichten habe ich kontinuierlich über die Weiterentwicklung des Datenschutzrechts berichtet (zuletzt 18. TB Nr. 2). Ständig neue technische Entwicklungen mit zum Teil tief greifender datenschutzrechtlicher Relevanz, Harmonisierungsbemühungen und Anforderungen des internationalen und europäischen Rechts, neue gesellschaftliche und politische Problemstellungen und ein sich wandelndes Bewusstsein der Bürger hinsichtlich ihres Grundrechts auf informationelle Selbstbestimmung bedingen einen permanenten Prozess der Überprüfung, Anpassung und Fortentwicklung des Bundesdatenschutzgesetzes und anderer datenschutzrechtlicher Regelungen. Nur so kann das Schutzniveau für die personenbezogenen Daten der Bürger aufrechterhalten und möglichst noch vergrößert werden. So haben noch vor In-Kraft-Treten der Novelle zum BDSG (s. dazu Nr. 3.2) die Überlegungen zu einer weiteren grundlegenden Reform des Datenschutzrechts (s. dazu Nr. 3.3) begonnen. Daneben waren im Bereich der inneren Sicherheit und der Terrorismusbekämpfung neue gesetzliche Regelungen erforderlich, die eine Neujustierung des Verhältnisses zwischen Sicherheitsbelangen und Datenschutz gebracht haben. In anderen wichtigen Feldern wie der Gentechnologie oder dem Arbeitnehmerdatenschutz sind gesetzliche Regelungen in Vorbereitung.

3.2 Umsetzung der BDSG-Novelle

Im 18. Tätigkeitsbericht habe ich ausführlich den Entwurf der Bundesregierung für ein Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze (Bundestagsdruck-sache 14/4329) vorgestellt (Nr. 2.1.3). Nach eingehenden Beratungen im Deutschen Bundestag und im Bundesrat ist es mit einigen Änderungen und Ergänzungen, aber im wesentlichen Kern unverändert, am 18. Mai 2001 verkündet worden (BGBl. I S. 904) und am 23. Mai 2001 in Kraft getreten. Damit ist endlich nach fünf Jahren zähen Ringens die europäische Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 auf Bundesebene in nationales Recht umgesetzt und das bereits von der Europäischen Kommission eingeleitete Vertragsverletzungsverfahren (vgl. 18. TB Nr. 2.6) in letzter Minute abgewendet worden.

Wenn auch nicht alle Erwartungen und Wünsche erfüllt worden sind, so bringt doch diese Neufassung des BDSG zahlreiche und wichtige Verbesserungen sowohl für den Datenschutz im öffentlichen Bereich als auch für nicht öffentliche Stellen. Neben vielen anderen bedeutenden Änderungen sind mir die neuen Regelungen zu

- Datenvermeidung und Datensparsamkeit (§ 3a),
- Vorabkontrolle (§ 4d Abs. 5 und 6),
- automatisierten Einzelentscheidungen (§ 6a),
- Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen/Videoüberwachung (§ 6b),
- mobilen personenbezogenen Speicher - und Verarbeitungsmedien/Chipkarten (§ 6c),
- Datenschutzaudit (§ 9a)

besonders wichtig, weil sie das Grundrecht auf informationelle Selbstbestimmung in für den Bürger wichtigen Bereichen stärken.

Trotz der langen Vorlaufzeit habe ich aber feststellen müssen, dass die Umsetzung des neuen BDSG vielfach nur sehr schleppend anlief und zu Unsicherheit und Interpretationsschwierigkeiten geführt hat. Für den meiner Zuständigkeit unterliegenden öffentlichen Bereich habe ich mich deswegen im August 2001 schriftlich an alle Ressorts gewandt, auf die geänderte Rechtslage, insbesondere auch was den behördlichen Datenschutzbeauftragten anbelangt, hingewiesen und um Unterstützung gebeten. Gleichwohl kann ich aber auch bei Redaktionsschluss noch nicht feststellen, dass das neue BDSG im öffentlichen wie im nicht öffentlichen Bereich vollständig umgesetzt wäre.

3.2.1 Auditgesetz

Mit dem neuen § 9a enthält das Bundesdatenschutzgesetz erstmals eine Regelung zum Datenschutzaudit. Diese Bestimmung ist mir besonders wichtig, weil sie Ausdruck für einen neuen, modernen Ansatz im Datenschutzrecht ist. Nach ihr können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen zur Verbesserung des Datenschutzes und der Datensicherheit ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Obwohl es sich hierbei um eine Kann-Bestimmung

handelt, die den Gedanken aufgreift, Datenschutz nicht restriktiv als Behinderung zu begreifen, sondern positiv einzusetzen als Mittel des wirtschaftlichen Wettbewerbs, als verkaufsförderndes Plus, das die Sorgen der Anwender und Konsumenten aufgreift und ihnen abhilft, waren im Vorfeld die Widerstände gegen diese Regelung erheblich. Ich bin froh, dass der Anregung des Bundesrats in seiner Stellungnahme vom 29. September 2000 (Bundesratsdrucksache 461/00), diese Vorschrift zu streichen, im weiteren Gesetzgebungsverfahren nicht gefolgt wurde.

Umso bedauerlicher ist, dass die Bestimmung bis heute leer läuft, weil das nach § 9a Satz 2 BDSG erforderliche Ausführungsgesetz fehlt, das die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter regeln soll. Das innerhalb der Bundesregierung hierfür zuständige Bundesministerium des Innern hat zunächst die Verwaltungshochschule Speyer mit einer Gesetzesfolgenabschätzung beauftragt. Der Abschlussbericht sollte im Herbst 2002 vorliegen, stand aber bei Redaktionsschluss immer noch aus. Erst danach soll das Ausführungsgesetz in Angriff genommen werden.

Die durch dieses Verfahren eingetretene Verzögerung bedauere ich sehr und ich befürchte, dass der im Gesetz vorgegebene Ansatz Schaden leiden kann. In der Zwischenzeit wurden und werden von unterschiedlichen Stellen zu unterschiedlichen Zwecken Datenschutzaudits entwickelt und angeboten, bei denen völlig offen ist, ob sie den künftigen gesetzlichen Anforderungen entsprechen werden. Sollte dies nach In-Kraft-Treten des Ausführungsgesetzes zu § 9a BDSG dann nicht der Fall sein, sind nicht nur die entsprechenden finanziellen und personellen Ressourcen vergeblich eingesetzt worden, es droht auch Verwirrung und Enttäuschung bei Unternehmen und Verbrauchern, die die bereits angebotenen Datenschutzaudits mit Blick auf § 9a BDSG einsetzen bzw. darauf vertrauen. Dies kann den richtigen Gedanken der Auditierung datenschutzgerechter Soft- und Hardware und von Datenschutzkonzepten entwerten.

Deswegen erwarte ich, dass das Ausführungsgesetz zu § 9a BDSG jetzt zügig erarbeitet und verabschiedet wird, damit endlich eine Auditierung auf dieser Grundlage beginnen kann.

3.2.2 Videoüberwachung

Bereits in meinem 18. Tätigkeitsbericht (Nr. 2.1.3) habe ich die neue Regelung des § 6b BDSG vorgestellt, die inzwischen mit der Novellierung am 23. Mai 2001 in Kraft getreten ist. Damit ist es erstmals gelungen, eine allgemeine Rechtsgrundlage für die vielfältigen Videoüberwachungen des öffentlich zugänglichen Raumes zu schaffen, die in gleicher Weise für öffentliche wie auch für nicht öffentliche Stellen gilt. Im Gegensatz zu einer vielstimmigen Kritik, die diese neue Vorschrift als zu weit gefasst ansieht und eine stärkere gesetzliche Eingrenzung von Videoüberwachungen fordert, beurteile ich die jetzt geltende Regelung grundsätzlich positiv und sehe in ihr einen angemessenen Interessenausgleich zwischen dem Grundrecht auf informationelle Selbstbestimmung einerseits und den berechtigten Belangen derer andererseits, die eine Videoüberwachung für gesetzlich zugelassene Zwecke einsetzen. Angesichts der fortdauernden kritischen Bewertung ist es aber umso wichtiger, dass die gesetzlichen Vorschriften strikt eingehalten werden. Dabei kommt auch technischen und psychologischen Aspekten große Bedeutung zu (vgl. hierzu Nr. 4.1).

Leider habe ich aber feststellen müssen, dass die Umsetzung der neuen Bestimmung nur schleppend erfolgt. So sind auch anderthalb Jahre nach In-Kraft-Treten bei weitem nicht alle von der gesetzlichen Regelung betroffenen Kameras entsprechend gekennzeichnet. Dies gilt nicht nur für nicht öffentliche Stellen, etwa in Parkhäusern oder vor Geldautomaten, sondern – wie ich auch anlässlich von Kontrollen feststellen musste – vielfach auch für öffentliche Stellen. Wie schwer sich auch diese mit der neuen Regelung tun, veranschaulichen die Antworten der Bundesregierung auf zwei Kleine Anfragen der PDS-Fraktion im Deutschen Bundestag zur Kennzeichnung videoüberwachter Bundesgebäude, von denen die erste (Bundestagsdrucksache 14/7905) von einer unzutreffenden rechtlichen Wertung ausging und auch die zweite (Bundestagsdrucksache 14/8263) nach meiner Bewertung nicht voll dem gesetzlichen Regelungsgehalt entspricht. Ich habe mich deswegen mehrfach an das Bundesministerium des Innern gewandt, das daraufhin die Überwachung des öffentlich zugänglichen Raumes durch Videokameras für seinen Geschäftsbereich durch einen Erlass vom 24. Juni 2002 geregelt hat, bei dessen Ausarbeitung ich beteiligt war.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich im Berichtszeitraum regelmäßig mit dieser Thematik befasst und eine Arbeitsgruppe eingesetzt, die aufgrund der Erfahrungen mit der derzeitigen Regelung Vorschläge für die von der Bundesregierung angekündigte Zweite Stufe der BDSG-Novellierung erarbeiten soll. Ich werde hieran aktiv mitarbeiten und auch in Zukunft mein besonderes Augenmerk auf die Anwendung des § 6b BDSG richten.

3.2.3 Selbstregulierung, § 38a BDSG

Artikel 27 Abs. 1 der europäischen Datenschutzrichtlinie 95/46/EG verpflichtet Mitgliedsstaaten und Kommission zur Förderung der Ausarbeitung von Verhaltensregeln. Dabei liegt das Ziel ausdrücklich darin, die bereichsspezifische Relevanz der aufgrund der Richtlinie erlassenen einzelstaatlichen Vorschriften zu erhöhen. Im Rahmen der Umsetzung dieser europäischen Vorgaben sollen nach § 38a BDSG Verhaltensregeln von Berufs- und Branchenverbänden als interne Regelungen zur ordnungsgemäßen Durchführung datenschutzrechtlicher Vorschriften beitragen. Die in § 38a Abs. 1 BDSG genannten Verbände und Vereinigungen können von ihnen erarbeitete Verhaltensregeln der Datenschutzaufsichtsbehörde unterbreiten, die dann nach § 38a Abs. 2 BDSG die Vereinbarkeit der ihr unterbreiteten Entwürfe mit dem geltenden Recht überprüft.

Infolge dieser neuen Möglichkeit haben im Berichtszeitraum eine Reihe von Verbänden und Konzernen im Wege der Selbstregulierung entsprechende Verhaltensregeln ausgearbeitet und den jeweils zuständigen Aufsichtsbehörden vorgelegt. Dabei haben sich in der Praxis Unsicherheiten und Schwierigkeiten ergeben, die sich nicht ohne weiteres und unmittelbar anhand des Gesetzestextes lösen ließen und die auch den Düsseldorfer Kreis beschäftigt haben. Im Wesentlichen ging es dabei um den möglichen Inhalt, die Verbindlichkeit solcher Regelungen und um den Prüfmaßstab der Aufsichtsbehörden.

Aus den maßgeblichen gesetzlichen Bestimmungen ergibt sich, dass verbands- oder konzerninterne Verhaltensregelungen weder das Gesetz ersetzen noch von ihm abweichen können. Ziel ist vielmehr, die Durchführung datenschutzrechtlicher Bestimmungen zu fördern. Ausreichend ist mithin nicht lediglich eine Wiederholung des Gesetzes. Das Gesetz eröffnet durch eine Selbstbindung des Verbandes, der Branche oder des Konzerns die Möglichkeit, ein Mehr als das gesetzlich Notwendige zur Förderung des Datenschutzes und dies auf freiwilliger Basis zu schaffen, aber auch die Vorgaben des Gesetzes verbands-, branchen- oder konzernspezifisch zu präzisieren.

Zu den Verbindlichkeiten solcher von den Datenschutzaufsichtsbehörden geprüften Verhaltensregeln sagt das Gesetz indes nichts. Meines Erachtens kann die Aufsichtsbehörde nach geltendem Recht für ihre Kontrolltätigkeit immer nur die Vorschriften des BDSG bzw. einschlägiger Spezialgesetze zugrunde legen. Verstöße gegen präzisierende oder gar weiter gehende Verhaltensregeln können kein Einschreiten der Aufsichtsbehörde auslösen. Entsprechendes gilt erst recht für die Feststellung von Ordnungswidrigkeiten oder Straftatbeständen. Ob die Verhaltensregeln mit verbands- oder konzerninternen Sanktionen bei Verstößen hiergegen zu belegen sind, bleibt im Ermessen derer, die diese Regeln beschließen. Zwingend erforderlich ist dies nach dem Gesetz nach meiner Auffassung nicht.

Auch die in § 38a Abs. 2 BDSG vorgesehene Überprüfung durch die Datenschutzaufsichtsbehörde kann sich meines Erachtens immer nur auf die Vereinbarkeit mit dem geltenden Recht beziehen, nicht aber darauf, ob die Verhaltensregeln sinnvoll und praktikabel erscheinen oder ob es wünschenswert wäre, noch weitere Bestimmungen zu treffen, die über das gesetzlich Gebotene hinausgehen.

Die Erörterungen im Düsseldorfer Kreis sind noch nicht abgeschlossen. Sollte im Zuge der zweiten Stufe der BDSG-Novellierung entsprechend den Gutachtervorschlägen auch die branchenspezifische Selbstregulierung und Selbstkontrolle (vgl. Nr. 3.3) ausgebaut werden, wären gesetzliche Präzisierungen zu den aufgetretenen Fragen überlegenswert.

3.2.4 Drittstaatenübermittlungen nach §§ 4b, 4c BDSG

Die Regel-Ausnahme-Kombination der §§ 4b und 4c BDSG beantwortet – in Umsetzung von Artikel 25 und 26 der EG-Datenschutzrichtlinie (s. 16. TB Nr. 2.1, 17. TB Nr. 2.1.1, 18. TB Nr. 2.1.2) – die Frage, inwieweit von Deutschland ausgehende Datenübermittlungen nach materiellem Recht zulässig sind. Die mit der Novellierung des BDSG in das Gesetz eingestellten Vorschriften wurden in den Ersten Abschnitt eingefügt, der die allgemeinen und gemeinsamen Bestimmungen enthält. Damit ist klargestellt, dass die §§ 4b und 4c entsprechend den Vorgaben der Richtlinie als einheitliche Regelungen für den öffentlichen wie für den nicht öffentlichen Bereich gelten.

3.2.4.1 Beurteilung der Angemessenheit des Schutzniveaus und Verantwortung für die Zulässigkeit der Übermittlung

Die europäische Datenschutzrichtlinie bezweckt, dass die Europäische Union zu einem einheitlichen informationellen Großraum wird, innerhalb dessen offene Grenzen und ein gleicher Datenumgang sichergestellt sind (s. 16. TB Nr. 2.1.1). Das BDSG stellt daher den innergemeinschaftlichen Datenverkehr dem inländischen gleich (§ 4b Abs. 1) und gewährleistet damit unionsweiten „freien" Datenverkehr. Diese Regelung umfasst neben den Mitgliedsstaaten der Europäischen Union auch die anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (EWR), d. h. Norwegen, Island und Liechtenstein sowie die Organe und Einrichtungen der Europäischen Gemeinschaften. Im Hinblick auf letztere wird durch die gesetzliche Regelung der durch den Vertrag über die Europäische Union von Amsterdam in den Vertrag zur Gründung der Europäischen Gemeinschaft eingefügte Artikel 286 berücksichtigt, durch den die Geltung der Richtlinie für die Organe und Einrichtungen der Europäischen Gemeinschaften verbindlich gemacht wurde (s. 18. TB Nr. 2.3).

Schon heute lässt sich sagen, dass der unionsweite „freie" Datenverkehr für die Praxis eine große Erleichterung gebracht hat. Auch wenn multinationale Unternehmen weiterhin über die nach wie vor unterschiedlichen Kontrollverfahren – insbesondere bei der Anmeldung – klagen, wird doch allgemein anerkannt, dass die offenen Grenzen einen großen Fortschritt darstellen.

Hinsichtlich der Datenübermittlungen an Stellen außerhalb der Union und des EWR, also an Drittstaaten, hat die Novellierung des BDSG zwar formell eine neue Regelung gebracht (§ 4b Abs. 2), die allerdings inhaltlich weitgehend der alten Rechtslage entspricht. Ihr materieller Kern besteht darin, dass eine Übermittlung zu unterbleiben hat, soweit ihr ein schutzwürdiges Interesse des Betroffenen entgegensteht (was schon bisher galt), und präzisiert dies dahin gehend, dass dies der Fall ist, wenn bei dem Empfänger „ein angemessenes Datenschutzniveau" nicht gewährleistet ist (§ 4b Abs. 2 Satz 2). Die Feststellung, ob ein angemessenes Datenschutzniveau besteht, ist Sache der übermittelnden Stelle; sie trägt auch dafür die Verantwortung (§ 4b Abs. 5).

Bei der Beurteilung, ob das Datenschutzniveau angemessen ist, ist nicht einzig auf die für den Empfänger geltenden Rechtsnormen abzustellen, sondern auch auf „die für ihn geltenden Standesregelungen und Sicherheitsmaßnahmen", darüber hinaus auf alle Umstände, die bei der Datenübermittlung von Bedeutung sind, wie insbesondere die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung und das Endbestimmungsland (§ 4b Abs. 3). Die Beurteilung erfolgt also nicht global für alle Empfänger des betreffenden Landes und alle Übermittlungen, die an diese gerichtet sind, sondern nach den Umständen des Einzelfalls bzw. der Fallgruppe.

Da die Feststellung des angemessenen Schutzniveaus mit großen Aufwendungen verbunden sein kann, ermächtigt Artikel 25 Abs. 6 der EG-Datenschutzrichtlinie die Europäische Kommission, mit für alle EU-Mitgliedsstaaten bindender Wirkung allgemein festzustellen, dass ein Drittland angemessenes Datenschutzniveau gewährleistet. Dies ist für die Schweiz, Ungarn und die Vereinigten Staaten von Amerika (vgl. 18. TB Nr. 2.2, Nr. 32.2.1 und Nr. 32.2.2) sowie für Kanada geschehen (Entscheidung der Kommission vom 20. Dezember 2001, ABl. 2/13 vom 4. Januar 2002). Wie schon im Falle der Vereinigten Staaten von Amerika wurde dabei der Geltungsbereich der Feststellung eingegrenzt. Sie gilt nur für den Anwendungsbereich des kanadischen Personal Information Protection and Electronic Documents Act (s. auch unter 32.4).

3.2.4.2 Ausnahmen vom Grundsatz der Angemessenheit durch allgemeine Regelungen und Einzelgenehmigungen

Die in § 4b BDSG enthaltene Grundsatzregelung wird gem. § 4c BDSG durch zwei Gruppen von Ausnahmen durchbrochen. Die eine greift in katalogartiger Auflistung unmittelbar zugunsten der verantwortlichen Stelle ein, während die andere Ausnahmengruppe sich auf einzelfallbezogene Genehmigungsmöglichkeiten bei Gewährleistung ausreichender Garantien durch die verantwortliche Stelle bezieht.

Bei den in § 4c Abs. 1 Satz 1 Nr. 1 bis 6 angeführten Tatbeständen handelt es sich nicht um eine kumulativ zu berücksichtigende Aufzählung, sondern es genügt, wenn mindestens eine der genannten Ausnahmen vorliegt. Die Tatbestände zeichnet aus, dass sie konkret beschriebene Fallgestaltungen enthalten, in denen eine Gefährdung des Grundrechts auf informationelle Selbstbestimmung nicht zu erwarten ist. Dies kann durch die Bedingungen der Datenübermittlung oder die Zusammenhänge, in denen diese stattfindet, begründet sein. Im Einzelnen sieht die Regelung folgende Ausnahmetatbestände vor:

- Einwilligung,
- Vertragserfüllung und vorvertragliche Maßnahmen,
- Vertrag im Betroffeneninteresse,
- wichtiges öffentliches Interesse und Rechtsansprüche,
- lebenswichtige Interessen,
- öffentliche Register.

Für den Fall, dass eine der vorgenannten Katalogausnahmen nicht eingreift, kann die verantwortliche Stelle gleichwohl ein solches auf andere Weise garantieren. Diesbezügliche Garantien können sich nach § 4c Abs. 2 „insbesondere“ aus Vertragsklauseln und verbindlichen Unternehmensregelungen ergeben, die der Aufsichtsbehörde zur Genehmigung vorzulegen sind.

Solche vertragliche Verpflichtungen sind nur dann ausreichende Garantien, wenn der durch sie verbürgte Schutz des Betroffenen nach Abschluss des Vertrages nicht mehr zur Disposition der die Daten exportierenden verantwortlichen Stelle und des Datenimporteurs im Drittland steht. Ebenso wichtig ist, dass der Datenexporteur die Einhaltung der ihm durch Vertrag gemachten Zusagen überwacht und diese nötigenfalls beim Vertragspartner einfordert. Auch muss sichergestellt sein, dass die Vertragsklauseln im Empfängerland wirksam sind. Kommt die Datenschutzaufsichtsbehörde zu dem Ergebnis, dass die beigebrachten Garantien auf vertraglicher Grundlage im Hinblick auf die festgestellten Risiken als ausreichend anzusehen sind, kann sie die beabsichtigte Datenübermittlung genehmigen.

Mit Bezug auf das Genehmigungsverfahren hat der Düsseldorfer Kreis ein Abstimmungsverfahren vereinbart. Ein Garantievertrag ist seitens der verantwortlichen Stelle zunächst der für sie zuständigen Aufsichtsbehörde vorzulegen, die diesen einschließlich ihres Votums an den als „Clearingstelle“ agierenden Berliner Beauftragten für Datenschutz und Akteneinsicht weiterleitet. Von diesem werden die anderen obersten Datenschutzaufsichtsbehörden unterrichtet. Falls keine Einwände geäußert werden, kann die zuständige Aufsichtsbehörde nach ihrem Votum entscheiden. Anderenfalls wird der Sachverhalt in der entsprechenden Arbeitsgruppe des Düsseldorfer Kreises besprochen und, falls nötig, dem Plenum vorgelegt. Die zuständige Aufsichtsbehörde entscheidet dann eigenverantwortlich unter Berücksichtigung des in der Arbeitsgruppe bzw. im Plenum des Düsseldorfer Kreises gefundenen Ergebnisses.

Die Verwendung von Standardvertragsklauseln mit ausreichenden Schutzgarantien könnte zu einer wesentlichen Erleichterung für das aufsichtsbehördliche Genehmigungsverfahren – wie auch für die beteiligten Vertragsparteien – beitragen. Die Anerkennung bestimmter Standardvertragsklauseln als ausreichende Garantien ist nach Artikel 26 Abs. 4 i. V. m. Abs. 2 der EG-Datenschutzrichtlinie der Europäischen Kommission vorbehalten. Eine entsprechende Entscheidung erließ die Europäische Kommission am 15. Juni 2001 (http://europa.eu.int/comm/internal_market/en/dataprot/news/1539de.pdf). Die unter wesentlicher Beteiligung der Gruppe nach Artikel 29 der EG-Datenschutzrichtlinie erarbeiteten Standardvertragsklauseln enthalten rechtlich durchsetzbare Verpflichtungserklärungen und darauf gegründete Garantien des Datenexporteurs und des Datenimporteurs. Der Vertrag wirkt zugunsten der Betroffenen, die mithin eigene Rechte aus der Vereinbarung geltend machen können. Die europäischen Standardvertragsklauseln enthalten ferner Verpflichtungen der Vertragsparteien zu gesamtschuldnerischer Haftung und zum Ausschluss der Kündigung der eingegangenen Verpflichtungen. Eine weitere, seit dem 3. April 2002 geltende Kommissionsentscheidung (http://www.datenschutz-berlin.de/doc/eu/kommission/standard271201.pdf) befasst sich mit Standardvertragsklauseln im Rahmen der Auftragsdatenverarbeitung.

Neben allgemeinen Vertragsklauseln nennt das BDSG in § 4c Abs. 2 auch verbindliche Unternehmensregelungen als Mittel zur Begründung ausreichender Garantien. Unternehmensregelungen sind für international operierende Unternehmen wesentlich leichter zu handhaben und passen besser zu ihrer Struktur als Vertragsklauseln. Mehrere internationale Unternehmen haben diesen Weg eingeschlagen und stehen mit den deutschen Datenschutzaufsichtsbehörden in engem Kontakt, um sich über den Inhalt ihrer Regelungen und das Verfahren ihrer Einführung zu verständigen. Zwischen den Beteiligten besteht Übereinstimmung, dass der wirksamen praktischen Durchsetzung hierbei die größte Bedeutung zukommt und dass Konzerndatenschutzbeauftragten dabei eine Schlüsselstellung zukommt.

3.2.5 Behördliche Datenschutzbeauftragte in der Bundesverwaltung

Seit dem In-Kraft-Treten des novellierten BDSG am 23. Mai 2001 sind alle Behörden im Anwendungsbereich des Gesetzes zur Bestellung eines behördlichen Beauftragten für den Datenschutz verpflichtet. Je nach Struktur der öffentlichen Stelle genügt auch die Bestellung eines Beauftragten für mehrere Bereiche. Im August 2002 habe ich mir mit einer Umfrage (s. Anlage 26) für den Bereich der Bundesverwaltung einen ersten Überblick über die Umsetzung dieser Regelung verschafft. Bis auf das BMI haben alle Obersten Bundesbehörden für ihren eigenen Bereich sowie – soweit vorhanden – den Geschäftsbereich geantwortet.

Das BMI teilte mit, dass dort eine Neugestaltung der Funktion des Datenschutzbeauftragten auch im Zusammenhang mit einem Personalwechsel geplant sei. Erst nach dieser

Neuorganisation solle die Beantwortung der Fragen für das BMI und den nachgeordneten Bereich erfolgen. Ich begrüße sehr, dass das Amt des Datenschutzbeauftragten im BMI gestärkt werden soll. Anderthalb Jahre nach In-Kraft-Treten der Neuregelungen im BDSG muss aber eine zügige Umsetzung erwartet werden, insbesondere dort, wo noch Nachbesserungsbedarf besteht.

Als Ergebnis der Umfrage ist festzuhalten, dass alle Obersten Bundesbehörden entsprechend der gesetzlichen Verpflichtung Datenschutzbeauftragte bestellt und dies auch ihren Beschäftigten bekannt gegeben haben. Ganz überwiegend gilt dies auch für die nachgeordneten Geschäftsbereiche, wo nur in Ausnahmefällen die Umfrage erst den Anstoß gegeben hat, Datenschutzbeauftragte zu bestellen und die dazu erforderlichen organisatorischen Begleitmaßnahmen vorzunehmen. Während der jeweilige Datenschutzbeauftragte als Ansprechpartner in den Verwaltungen den Beschäftigten benannt wurde, ergab sich noch ein Nachholbedarf für die Bekanntmachung gegenüber dem Bürger. Denn nach dem Gesetz ist der Datenschutzbeauftragte auch für diese Ansprechpartner und hat sich für die Wahrung von deren Datenschutzrechten in den Behörden einzusetzen. Seine Aufgabe ist unter anderem, über die so genannten Verfahrensverzeichnisse der Verwaltungen für die Bürger Transparenz in der Datenverarbeitung zu schaffen. In den allgegenwärtigen Internetpräsentationen der Behörden und den Bestrebungen zum eGovernment sollte daher auch der Datenschutzbeauftragte als Ansprechpartner für die Bürger deutlich herausgestellt werden.

Die Umfrage hat weiter ergeben, dass bis auf wenige Ausnahmen die Datenschutzbeauftragten ihr Amt nicht hauptamtlich wahrnehmen und mit ihnen in der Regel auch keine Vereinbarung über eine Entlastung von anderen Aufgaben getroffen worden ist. Anders als etwa bei der Gleichstellungsbeauftragten schreibt auch das Gesetz keine Freistellungen fest. Die wirkungsvolle Wahrnehmung der gesetzlichen Aufgaben wird aber in der Zukunft ganz entscheidend davon abhängig sein, ob ihnen trotz knapper Personalressourcen genügend Entlastung eingeräumt wird, um ihr Amt auch ausfüllen zu können.

Um einen fruchtbaren Erfahrungsaustausch zwischen den Datenschutzbeauftragten in den Ressorts zu erreichen und Gelegenheit zu bieten, Rechtsfragen und praktische Probleme gemeinsam zu erörtern, habe ich einen regelmäßig zusammenkommenden Gesprächskreis mit den Datenschutzbeauftragten der Obersten Bundesbehörden eingerichtet. Beginnend im September 2001 fand dieser Austausch inzwischen zweimal statt. Er wurde mit jeweils ca. 30 Teilnehmern aus praktisch allen Obersten Bundesbehörden gut angenommen. Nachdem es zunächst schwerpunktmäßig um die Einführung der neu bestellten Datenschutzbeauftragten in das novellierte BDSG und ihre neugestaltete Aufgabenstellung ging, ergaben sich im Folgenden eine Vielzahl praktischer Fragestellungen etwa über die Gestaltung der neuen Verfahrensverzeichnisse, die Videoüberwachung bis hin zur Erörterung datenschutzrechtlicher Aspekte der eGovernment Initiative BundOnline 2005.

Der Erfahrungsaustausch bietet ein gutes Forum, datenschutzrechtliche Beratung durch mein Haus einzuholen, und zugleich einen Anstoß für die bereits in Gang gekommene Kommunikation zwischen den Datenschutzbeauftragten der Obersten Bundesbehörden. Ich würde es begrüßen, wenn innerhalb der Geschäftsbereiche der Ressorts die Zusammenarbeit zwischen den Datenschutzbeauftragten der einzelnen Behörden in ähnlicher Weise gefördert werden könnte.

3.3 In Vorbereitung: Die zweite Stufe der Datenschutzreform

Wie ich in meinem letzten Tätigkeitsbericht schon dargestellt habe (18. TB Nr. 2.1.4), hat die Bundesregierung bereits lange vor In-Kraft-Treten der aktuellen BDSG-Novelle die Absicht erklärt, in einer zweiten Stufe der Novellierung eine umfassende Neukonzeption des BDSG zu verabschieden. Zur Verwirklichung dieses Zieles, das nach der ursprünglichen Planung noch innerhalb der 14. Legislaturperiode erreicht werden sollte, hat das Bundesministerium des Innern ein großangelegtes Gutachten zur „Modernisierung des Datenschutzrechts“ bei drei renommierten Fachleuten aus den Bereichen Datenschutzrecht und Informatik in Auftrag gegeben, das auf eine Initiative aus dem parlamentarischen Raum hin durch eine Begleitkommission aus namhaften Sachverständigen in enger Abstimmung mit den Gutachtern unterstützt werden sollte. In dieser Kommission, die in zwei Sitzungen im Januar und Juni 2001 zunächst das Gutachtendesign und dann einen Diskussionsentwurf des Gutachtens eingehend erörtert hat, habe ich mitgearbeitet. Auch die Datenschutzbeauftragten der Länder hatten im April 2001 in einem Workshop mit den Gutachtern Gelegenheit, deren Vorstellungen eingehend zu diskutieren, in einer einvernehmlichen Stellungnahme zu bewerten und eigene Vorschläge einzubringen. Auch hieran war ich beteiligt.

Das sehr umfangreiche Gutachten ist dann am 12. November 2001 offiziell übergeben und der Öffentlichkeit vorgestellt worden. Es enthält eine umfassende und tief gehende Analyse des Modernisierungsbedarfs im Datenschutzrecht, zeigt die Richtung für eine grundlegende Reform auf und kommt zu einer Fülle von Anregungen und Vorschlägen, die bei ihrer Verwirklichung zu einer deutlichen Änderung von Recht und Praxis beim Datenschutz in der Bundesrepublik Deutschland führen würden.

Besonders hervorheben möchte ich den Vorschlag, das Datenschutzrecht insgesamt zu vereinfachen. Damit ist nicht nur eine verständliche Sprache und eine übersichtliche Gliederung gemeint, was für sich schon ein lohnendes Ziel wäre, sondern der Versuch, die Flut der spezialgesetzlichen Bestimmungen einzudämmen und das moderne Datenschutzrecht auf ein allgemeines Gesetz zu gründen, das nur in erforderlichem Umfang durch bereichsspezifische Regelungen ergänzt wird. Es soll grundsätzliche und präzise Vorschriften zur Verarbeitung personenbezogener Daten enthalten und möglichst offene Abwägungsklauseln vermeiden. Darüber hinaus soll es allgemeine Regelungen zur Technikgestaltung, zur Datensicherheit, zur Datenschutzorganisation, zur Kontrolle und zur Selbstregulierung vorsehen. Spezialgesetzliche Regelungen sollen also auf das unabdingbar Notwendige beschränkt werden und nur noch die „Ausnahme von den allgemeinen Regelungen enthalten und nur für bestimmte riskante Datenverarbeitungen die Anforderungen verschärfen oder bei unterdurchschnittlich riskanten Datenverarbeitungen Erleichterungen bieten“. Auch Tele-kommunikations- und Teledienstedatenschutz sollen in das BDSG integriert werden.

Ein weiterer wichtiger Punkt des Gutachtens ist nach meiner Einschätzung die Stärkung der Selbstbestimmung. Überall dort, wo nicht auszuschließen ist, dass die Belange des Betroffenen beeinträchtigt werden könnten, und wo nicht im öffentlichen Bereich zwingende Gründe der staatlichen Aufgabenerfüllung vorliegen, soll der Betroffene – ganz im Sinne des Bundesverfassungsgerichts – selbst entscheiden können. Seine Einwilligung ist grundsätzlich für die Verarbeitung seiner personenbezogenen Daten erforderlich, also eine so genannte Opt-in-Lösung, wobei natürlich Ausnahmen möglich bleiben sollen, wenn auch in geringerem Umfang als nach geltendem Recht. Unterstützt soll dies werden durch eine noch bessere Zweckbindung und durch Stärkung der Betroffenenrechte wie Auskunft und Benachrichtigung. Auch die Überlegungen der Gutachter zur gesellschaftlichen Selbstregulierung und zum Datenschutz durch Technik halte ich für besonders zukunftsrelevant. Das ursprünglich verfolgte, sicherlich sehr ehrgeizige Ziel, noch in der 14. Legislaturperiode auf der Grundlage des Gutachtens zumindest einen Gesetzentwurf oder Eckpunkte hierfür vorzulegen, konnte nicht erreicht werden. Dies ist sicherlich auch darauf zurückzuführen, dass die Überlegungen der Gutachter einen sehr grundlegenden Ansatz haben, der weniger auf Einzelregelungen im BDSG als auf eine grundsätzliche Umsteuerung abzielt. Die Umsetzung dieser neuen Prinzipien und Strukturen in dem bereits sehr umfangreich kodifizierten Datenschutzrecht wird deswegen nicht leicht sein. Erforderlich ist weiter eine Einpassung des Vorhabens in den europäischen Rahmen.

Der Deutsche Bundestag hat aber sowohl in seiner Entschließung zu meinem 18. Tätigkeitsbericht (Bundestagsdrucksache 14/9490 Nr. 2) als auch in seinem Beschluss „Umfassende Modernisierung des Datenschutzrechtes voranbringen“ (Bundestagsdrucksache 14/9709) die Erwartung zum Ausdruck gebracht, dass die Bundesregierung zügig einen Gesetzentwurf zur grundlegenden Modernisierung des Bundesdatenschutzgesetzes erarbeitet. Die Bundesregierung hat ihrerseits in der Koalitionsvereinbarung für die 15. Legislaturperiode eine entsprechende Absicht bekundet. Ich bin deswegen sicher, dass die Arbeiten an der zweiten Stufe der BDSG-Novellierung fortgesetzt werden, und werde diese beratend begleiten.

3.4 Informationsfreiheitsgesetz

Der freie und voraussetzungslose Zugang jeden Bürgers zu den bei der Verwaltung vorhandenen Akten, Unterlagen und Informationen wird zunehmend als wichtige Voraussetzung für die Teilhabe am demokratischen Prozess und die Kontrolle der Staatsverwaltung angesehen. Deswegen haben bereits – teilweise seit langem – viele demokratisch verfasste Staaten, die Europäische Union und innerhalb der Bundesrepublik Deutschland die Länder Berlin, Brandenburg, Schleswig-Holstein und Nordrhein-Westfalen entsprechende gesetzliche Regelungen. Dem stehen aus Sicht des Datenschutzes, der selbst auf den Prinzipien der Transparenz und freien Selbstbestimmung des Bürgers fußt, keine grundlegenden Bedenken entgegen, wenn die Privatsphäre der Betroffenen sowie Betriebsgeheimnisse gesetzlich geschützt bleiben und die anzuwendenden Regelungen entsprechende Schutzmechanismen enthalten. Dies hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom März 2001 (Anlage 9) noch einmal bekräftigt.

Im Berichtszeitraum hat es auch auf Bundesebene Bemühungen gegeben, eine gesetzliche Grundlage für den freien Zugang des Bürgers zu den Informationen der Bundesbehörden zu schaffen. Bereits in der Koalitionsvereinbarung für die 14. Legislaturperiode vom 20. Oktober 1998 war vereinbart worden, ein Informationsfreiheitsgesetz vorzulegen. Im Jahr 2001 wurde dann vom federführend zuständigen BMI ein Gesetzentwurf im Internet veröffentlicht, der sich in einer Reihe von Vorschriften um ein ausgewogenes Verhältnis zwischen Informationszugang einerseits und Schutz personenbezogener Daten und von Betriebsgeheimnissen andererseits bemühte und – vergleichbar mit den bereits geltenden Landesgesetzen – das Amt eines Bundesbeauftragten für Informationsfreiheit vorsah, das von mir neben meiner Funktion als Bundesbeauftragter für den Datenschutz wahrgenommen werden sollte. Zu einer abschließenden Abstimmung dieses Entwurfs innerhalb der Bundesregierung ist es dann aber in der letzten Legislaturperiode nicht mehr gekommen. Die Bundesregierung beabsichtigt jedoch entsprechend der Koalitionsvereinbarung für die laufende Legislaturperiode weiterhin, ein Informationsfreiheitsgesetz vorzulegen.

Bei den Beratungen über den Gesetzentwurf war ich in den vergangenen Jahren beteiligt und habe dabei mit meinen Vorschlägen zu einem ausgewogenen Verhältnis zwischen Informationsfreiheit und Datenschutz beitragen können. Ich werde auch die neuen Bemühungen um ein Informationsfreiheitsgesetz aufmerksam begleiten.

3.5 Verbraucherinformationsgesetz

Als Konsequenz aus einer in der Öffentlichkeit und den Medien engagiert geführten Debatte um den Schutz der Verbraucher hat das Bundesministerium für Verbraucherschutz, Ernährung und Landwirtschaft im Januar 2002 einen ersten Entwurf eines Verbraucherinformationsgesetzes vorgelegt, mit dem den Verbrauchern Zugang zu den bei den Behörden des Bundes, der Länder und der Gemeinden vorhandenen Informationen über Lebensmittel und Bedarfsgegenstände eröffnet und zugleich geregelt werden sollte, unter welchen Voraussetzungen Behörden die Öffentlichkeit über marktrelevante Vorkommnisse unterrichten können. Im Zuge der Erörterungen wurde auch die Frage aufgebracht, ob nicht durch die Einsetzung eines Beauftragten für Verbraucherinformation ein Instrument geschaffen werden könnte, das der interessierte Verbraucher bei Widerständen und Hindernissen in Behörden im Vorfeld einschalten kann, ohne gleich den Verwaltungsrechtsweg beschreiten zu müssen. Für die Bundesverwaltung wurde hierfür parallel zu Überlegungen im Bereich der Informationsfreiheit an den Bundesbeauftragten für den Datenschutz gedacht. Meinerseits bestanden und bestehen gegen die Übernahme einer solchen neuen Aufgabe keine Bedenken, wenn der Gesetzgeber dies wünscht und die neue Funktion mit meiner Unabhängigkeit und bisherigen Aufgabenstellung und Arbeitsweise vereinbar ist. Der dem Deutschen Bundestag zugeleitete Gesetzentwurf vom 8. April 2002 (Bundestagsdrucksache 14/8738) sah dann in § 8 vor, dass jedermann den Bundesbeauftragten für den Zugang zu Verbraucherinformationen anrufen kann, soweit Bundesbehörden betroffen sind und er sich in seinem Recht auf freien Zugang zu Informationen im Sinne des

Gesetzes verletzt fühlt. Die Aufgabe sollte von mir wahrgenommen werden, wobei die Ausgestaltung dieser Funktion sich nach den entsprechenden Vorschriften des Bundesdatenschutzgesetzes und des Entwurfs eines Informationsfreiheitsgesetzes richtete. Die Länder sollten Einrichtung und Aufgaben eines Beauftragten für den Zugang zu Verbraucherinformationen für ihren Bereich regeln.

Nachdem der Deutsche Bundestag das Verbraucherinformationsgesetz am 17. Mai 2002 verabschiedet hatte, versagte der Bundesrat am 21. Juni 2002 seine erforderliche Zustimmung.

In der Koalitionsvereinbarung für die laufende Legislaturperiode vom 16. Oktober 2002 ist im V. Abschnitt vorgesehen, mit einem Verbraucherinformationsgesetz die Informationsrechte der Verbraucher gegenüber Behörden und Anbietern nachhaltig zu verbessern. Es bleibt abzuwarten, ob in diesem Zusammenhang an dem Gedanken festgehalten wird, mir das Amt eines Beauftragten für den Zugang zu Verbraucherinformationen zu übertragen.

3.6 Europäische Harmonisierung in der Praxis

Das wichtigste Forum zur Harmonisierung der Datenschutzpraxis in den Mitgliedsstaaten der Europäischen Union ist nach wie vor die Gruppe nach Artikel 29 der EG-Datenschutzrichtlinie. Ihre Arbeit wurde im Berichtszeitraum intensiviert, was sich sowohl an der Intensität der Sitzungen – pro Jahr fünf zweitägige Sitzungen der Gruppe und je drei bis vier Sitzungen der vier bis fünf Fach-Arbeitsgruppen – als auch an Quantität und Qualität der Ergebnisse zeigt. Im Jahr 2001 wurden 14 Papiere, im Jahr 2002 zwölf Papiere verabschiedet. Der Themenkreis ist weit gespannt: Er umfasst zunächst informative bis analytische Papiere, wie die jährlichen Berichte über die Entwicklung in der Gemeinschaft, den Mitgliedsstaaten und Drittstaaten, oder eine Untersuchung über Erscheinungsformen und Probleme schwarzer Listen. Ferner betraf er rechtliche Ausarbeitungen, etwa zum adäquaten Schutzniveau in Drittstaaten, zu Mustervertragsklauseln für Drittlandsübermittlungen oder zur Anwendbarkeit der Datenschutzgesetze der Mitgliedsstaaten auf internationale Datenverarbeitungen im Internet. Weiter ging es um Positionen zu den Problemen bestimmter Sektoren, wie dem Arbeitnehmerdatenschutz in Zeiten zunehmender Überwachung und zu international abgestimmten Methoden zur Bekämpfung der Cyber-Kriminalität, bis hin zu den aktuellen internationalen Problemen im Gefolge des 11. September 2001, etwa auf dem Gebiet der Luftfahrt (Zusammenstellung der von der Arbeitsgruppe angenommenen Dokumente s. Anlage 8). Ständige Arbeitsgruppen bestehen zurzeit zu den Themen Internet, Mustervertragsklauseln, internationale Verhaltensregelungen und Arbeitnehmerdatenschutz.

Die Arbeitsgruppe hat beschlossen, die Transparenz ihrer Arbeit gegenüber der europäischen Öffentlichkeit zu verbessern. Zu diesem Zweck soll ein fortzuschreibender Arbeitsplan mit den aktuellen Themen ins Internet gestellt werden. Außerdem soll interessierten Personen und Stellen die Gelegenheit gegeben werden, sich im Rahmen einer Internetkonsultation zu Entwürfen der Arbeitsgruppe zu äußern, bevor diese abschließend beraten und angenommen werden. Für Anfang 2003 ist eine erste derartige Konsultation zu einem Papier zur Videoüberwachung geplant.

3.7 Zwischenbilanz zum Safe Harbor

Anfang 2002 hat die EU-Kommission eine erste bewertende Bestandsaufnahme des Safe-Harbor-Arrangements zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten von Amerika vorgenommen (vgl. 18. TB Nr. 2.2.2). Sie entsprach damit einem Anliegen des Europäischen Parlaments und der Datenschutzbeauftragten der Mitgliedsstaaten. Probleme wurden vor allem in zweierlei Hinsicht festgestellt:

Zum einen lässt die Resonanz innerhalb der amerikanischen Wirtschaft zu wünschen übrig. Auch zum Jahresende 2002 lag die Anzahl der dem Safe Harbor beigetretenen Unternehmen nur knapp über 300. So erfreulich es einerseits ist, dass die Großen der amerikanischen IT-Industrie fast geschlossen beigetreten sind, so deutlich ist das Zögern in den anderen Wirtschaftsbereichen. Immerhin sind aus mehreren Wirtschaftsbranchen einzelne Großunternehmen beigetreten, so etwa eine Hotelkette, ein Mischkonzern, ein Wirtschaftsinformationsdienstleister und ein Automobilhersteller (US-Tochter eines deutschen Unternehmens). Dies deutet darauf hin, dass die Anforderungen des Safe Harbor grundsätzlich annehmbar sind und dass daher die Aussicht besteht, dass der Safe Harbor künftig wesentlich mehr Zulauf erhält. Damit wäre wohl insbesondere zu rechnen, wenn die Datenschutzaufsichtsbehörden in den Europäischen Mitgliedsstaaten die Zurückhaltung, um die sie von amerikanischer Seite während der Anfangszeit gebeten worden waren, aufgäben und ihre Aufmerksamkeit stärker auf den Datenaustausch mit amerikanischen Unternehmen wendeten, die dem Safe Harbor nicht beigetreten sind.

Zum anderen hat die Kommission auf der Grundlage einer Studie hinsichtlich der Umsetzung der Anforderungen des Safe Harbor in den beigetretenen amerikanischen Unternehmen festgestellt, dass vor allem bei der Transparenz verbreitete Defizite bestehen. Bei vielen dieser Unternehmen kann der Bürger nur feststellen, dass sie dem Safe Harbor angehören, aber nicht, welche Rechte ihm daraus erwachsen und in welcher Weise er sie geltend machen kann. Viele Unternehmen geben zwar ihre privacy policy auf ihrer Internetseite bekannt, berücksichtigen dabei aber nicht die besonderen Anforderungen des Safe Harbor. Die Federal Trade Commission hat in diesem Zusammenhang versichert, dass sie ungeachtet dieser Mängel gegen ein Unternehmen vorgehen kann, das die Safe-Harbor-Regeln nicht beachtet. Unabhängig davon hat die amerikanische Seite zugesagt, auf mehr „visible compliance“ hinzuwirken.

Als positiv kann bewertet werden, dass bisher keine Beschwerdefälle bekannt geworden sind, die nicht von den betroffenen Unternehmen zur Zufriedenheit der Betroffenen beigelegt wurden.

3.8 Bestellung des Europäischen Datenschutzbeauftragten überfällig

Die Einrichtung des Europäischen Datenschutzbeauftragten hat sich weiterhin verzögert. Erst im Juli 2002 gelang es dem Europäischen Parlament, dem Rat und der Kommission, sich auf die notwendigen Regelungen zum Ernennungsverfahren, zum Sitz und zu den dienstrechtlichen Verhältnissen des Europäischen Datenschutzbeauftragten zu einigen und damit die in der Datenschutzverordnung zunächst offen gelassenen Fragen zu beantworten (vgl. 18. TB

Nr. 2.3). Ergänzend zum Ernennungsverfahren (Vorschlag einer Kandidatenliste aufgrund öffentlicher Ausschreibung durch die Kommission, gemeinsame Entscheidung über den Datenschutzbeauftragten und seinen Stellvertreter durch Europäisches Parlament und Rat) sieht die Regelung eine Veröffentlichung der Bewerberliste vor (die inzwischen erfolgt ist) und ermöglicht eine Anhörung der Kandidaten durch das Europäische Parlament. Mit der Bestellung des Europäischen Datenschutzbeauftragten wird im ersten Halbjahr 2003 gerechnet.

3.9 Die Konferenz der Datenschutzbeauftragten der Europäischen Union

Die Frühjahrskonferenz der unabhängigen europäischen Datenschutzbehörden vom 9. bis 11. Mai 2001 in Athen hat ihre auf der Vorkonferenz in Stockholm (vgl. 18 TB Nr. 2.5) gefasste Entschließung zur Aufbewahrung von Verkehrsdaten durch Internet Service Provider (Retention of traffic data bei Internet Service Providers, s. Anlage 6) bekräftigt. Darin äußern die Datenschutzbeauftragten erneut ihre nachhaltigen Bedenken gegenüber Vorhaben, nach denen Provider Verkehrsdaten routinemäßig über die Zwecke der Abrechnung hinaus für Möglichkeiten behördlicher Rechtsverfolgung aufbewahren sollen.

Die Konferenz von Athen befasste sich außerdem mit aktuellen Fragen zur Kriminalität im Cyberspace, zur Telekommunikation, zum Internet und zum E-Commerce. Bei dem Thema „Einwilligung als Rechtsgrundlage der Datenverarbeitung“ standen die Gefahren einer Kommerzialisierbarkeit der Einwilligungserteilung im Mittelpunkt des Interesses. Neben Fragen des Arbeitnehmerdatenschutzes bildeten Erscheinungsformen und rechtliche Einordnung „Schwarzer Listen“ in den Bereichen Kreditinformation, Versicherungswesen, Fernmeldeverkehr und in Mietrechtsangelegenheiten weitere Beratungsschwerpunkte.

Im Lichte der durch die Europäische Grundrechtecharta erneut bestätigten Grundrechtsqualität des Datenschutzes (vgl. 18. TB Nr. 2.4) verabschiedete die Konferenz eine weitere Entschließung, in der sie das „Europäische Modell“ eines grundrechtlich verankerten Datenschutzes begrüßt und ihn als wesentlichen Bestandteil einer „E-Citizenship“ versteht. Dieses europäische Datenschutzmodell soll als Richtschnur für alle Einrichtungen der Europäischen Union bei der Überprüfung des gegenwärtigen Rechtszustandes, bei der Ausarbeitung neuer Regelungen sowie in der Ausgestaltung des Verhältnisses zu Drittländern dienen (Declaration on Article 8 of the EU Charter of Fundamental Rights, s. Anlage 7).

Zur Frühjahrskonferenz am 25. und 26. April 2002 konnte ich die Datenschutzbeauftragten der EU-Mitgliedsstaaten und des Europäischen Wirtschaftsraumes (Norwegen, Island), der Beitrittskandidaten Polen, Tschechische Republik und Ungarn sowie die der Schweiz und der Kanalinsel Guernsey in Bonn begrüßen. Den wichtigsten Beratungsgegenstand bildeten die Erfahrungen nach den Terroranschlägen in den USA vom 11. September 2001, wobei insbesondere die unterschiedlichen Reaktionen in den Teilnehmerstaaten – zum Handeln sah sich einerseits der Gesetzgeber u. a. in Griechenland, Großbritannien, Italien, Schweden und Deutschland veranlasst, als ausreichend wurde andererseits die Gesetzeslage in Frankreich, den Niederlanden und Portugal angesehen – und ihre datenschutzrechtlichen Auswirkungen erörtert wurden. Aus der Vielzahl weiterer behandelter Themen sind die Fragen zur Auditierung und Zertifizierung von Konzepten für besseren Datenschutz und Datensicherheit hervorzuheben sowie die Vorträge und Diskussionen über Verfahren biometrischer Identifizierung. Zu letzterem Thema bestand Konsens dahin gehend, dass biometrische Daten vorrangig auf der Grundlage freiwilliger Entscheidungen der Betroffenen verwendet werden sollen und stets der Grundsatz der Verhältnismäßigkeit zu beachten ist.

3.10 Die Umsetzung der Datenschutzrichtlinie 95/46/EG in den Mitgliedsstaaten der Europäischen Union

Die Kommission hat mit der Erarbeitung des Berichts über die Durchführung der EG-Datenschutzrichtlinie begonnen, den sie dem Europäischen Parlament und dem Rat binnen drei Jahren nach Ablauf der Umsetzungsfrist (1998) zu erstatten hat (Artikel 33 Abs. 1). Die Ausgangslage ist insofern schwierig, als viele Mitgliedsstaaten die Richtlinie nur mit erheblicher Fristüberschreitung umgesetzt haben und zwei Mitgliedsstaaten auch zum Jahresende 2002 noch keinen Vollzug melden konnten (Frankreich, Irland).

Zur Vorbereitung des Berichts hat die Kommission nicht nur bei den Regierungen und den Datenschutzbehörden der Mitgliedsstaaten mittels umfangreicher Fragenkataloge Informationen zusammengetragen, sondern darüber hinaus eine große Internetkonsultation durchgeführt, die sich – mit unterschiedlichen Themenschwerpunkten – einerseits an datenverarbeitende Stellen, also an Unternehmen, Verbände und sonstige Organisationen, wendete, andererseits an Betroffene, also an Individuen, Bürgerrechts- und Verbraucherschutzorganisationen und vergleichbare Einrichtungen. Die Umfragen zeigten – auch bei den datenverarbeitenden Stellen – eine außerordentlich positive Einstellung zum Datenschutz. Es wird ein strenger Datenschutz gefordert und die geltenden Regelungen werden grundsätzlich akzeptiert, wobei die Betroffenen den bestehenden Schutz nur als das notwendige Minimum betrachten. Kritisiert werden allerdings die immer noch erheblichen Unterschiede zwischen den Mitgliedsstaaten und es wird eine stärkere Beratung durch die Datenschutzbehörden gewünscht.

Sowohl bei den datenverarbeitenden Stellen als auch bei den Betroffenen kamen fast die Hälfte der Antworten aus Deutschland. Auch unter Berücksichtigung der unterschiedlichen Bevölkerungszahlen kann dies als Bestätigung für die wichtige Rolle Deutschlands im europäischen Datenschutz gewertet werden.

Im Herbst 2002 hat die Kommission eine zweitägige internationale Konferenz mit Interessenvertretern und Experten auch aus den USA und anderen Drittländern durchgeführt. In einer Reihe von Arbeitskreisen bestand die Gelegenheit zur vertieften Diskussion wichtiger Konzepte und Anwendungsgebiete der Richtlinie. Das Interesse war unerwartet groß. Die Kommission hatte 400 Teilnehmer eingeplant und musste ebenso vielen Interessenten absagen. Kommissar Bolkestein konnte zum Abschluss der Konferenz feststellen, dass die Richtlinie bei aller Diskussion zu vielen Einzelfragen von niemandem als unpraktikabel oder ungeeignet bezeichnet wurde. Die Überlegungen der Kommission zielten

gegenwärtig weniger in Richtung auf eine Änderung der Richtlinie als vielmehr auf deren verbesserte Anwendung. Als relevante Punkte nannte er dabei die Vereinfachung des Meldeverfahrens, die weitere Angleichung zwischen den Mitgliedsstaaten, verstärkte Anstrengungen im Bereich der Privacy Enhancing Technologies, mehr Flexibilität bei der Drittlandsübermittlung und eine stärkere Rolle der Selbstregulierung.

Im Hinblick auf die noch begrenzten Anwendungserfahrungen ist diese Position der Kommission durchaus nachvollziehbar. Auf der anderen Seite bin ich überzeugt, dass die in Deutschland teilweise vollzogene, teilweise geplante Modernisierung des Datenschutzes auch auf der europäischen Ebene ihre Entsprechung finden muss. Bei manchen Themen kann dies ohne Novellierung der Richtlinie gelingen. So zeigte der Arbeitskreis „Bild- und Tonverarbeitung", dass mehrere Mitgliedsstaaten auch ohne Gesetzesänderung zu einer Handhabung gelangt sind, die der im neuen § 6b BDSG vorgeschriebenen weitgehend entspricht. Grundsätzlich sollte die Kommission aber eine Novellierung nicht ausschließen, wenn die sachliche Notwendigkeit evident ist und für eine umfassende und zügige freiwillige Koordination der Mitgliedsstaaten nur geringe Aussichten bestehen.

4 Technologischer Datenschutz

4.1 Neue Regelungen im BDSG: Videoüberwachung

4.1.1 Grundsätzliches

Ich habe es sehr begrüßt, dass der Gesetzgeber mit den neuen Regelungen des § 6b BDSG endlich klare Rechtsnormen für die Videoüberwachung geschaffen hat (s. o. Nr. 3.2.2). Zweifellos hat sich hiermit die Rechtsposition der betroffenen Bürgerinnen und Bürger verbessert. Neben den rechtlichen gibt es aber auch technische und psychologische Aspekte zu beachten. Die Aufstellung neuer Videokameras im öffentlichen Raum führt immer wieder zu – häufig kontroversen – Diskussionen in der Öffentlichkeit und in den Medien und die verunsicherten Bürger fragen, ob das denn sein muss, was eigentlich aufgezeichnet wird und was damit geschieht.

Unabhängig von einer datenschutzrechtlichen Bewertung zeigt sich damit vielfach ein gravierendes Versäumnis der verantwortlichen Stelle: Seit Jahren weise ich immer wieder darauf hin, dass unerlässliche Voraussetzung für einen wirkungsvollen – und von den Bürgerinnen und Bürgern akzeptierten – Einsatz von Videoüberwachung die frühzeitige und angemessene Beteiligung der Betroffenen ist. Das kann damit beginnen, dass ein beabsichtigtes Projekt in angemessener Form – auch mithilfe der Medien – bekannt gegeben und den Betroffenen Gelegenheit gegeben wird, sich hierzu zu äußern. Bereits in dieser Phase könnten Mängel erkannt und bestehende Besorgnisse durch die Gestaltung des Systems behoben werden. Die Inbetriebnahme des fertigen Systems sollte ebenfalls frühzeitig und in angemessener Form bekannt gemacht werden. Von besonderer Bedeutung ist auch die in § 6b Abs. 2 BDSG geforderte Kenntlichmachung der Videoüberwachung: Wer sich in einen überwachten Bereich begibt oder sich in ihm aufhält, muss über diesen Umstand unmissverständlich und deutlich informiert werden.

4.1.2 Datenschutz durch Technik

Bei der Videoüberwachung muss in besonderer Weise dem Grundsatz der Datensparsamkeit und Datenvermeidung Rechnung getragen werden, wie er nach der Novellierung des BDSG in § 3a geregelt ist. Für die technische Ausgestaltung eines Videoüberwachungssystems ergeben sich hieraus eine Reihe von Anforderungen:

Grundsätzlich unzulässig ist – über die Beobachtung hinaus – eine permanente Aufzeichnung aller gewonnenen Bildsequenzen oder auch nur der Bildsequenzen einzelner Kameras. Die Aufzeichnung ist nur zulässig, „wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist (§ 6b Abs. 3 BDSG)". In diesem Sinne muss der Umfang der gespeicherten Daten technisch – gegebenenfalls durch „menschliche Mitwirkung" – auf das Unerlässliche begrenzt werden. Dies kann z. B. dadurch geschehen, dass der Aufzeichnungszeitraum für eine bestimmte Kamera auf einen kurzen Zeitraum, z. B. 30 Minuten, begrenzt wird, wonach die gespeicherten Daten automatisch durch die Daten der danach folgenden Bildsequenzen überschrieben werden. Als Alternative bietet es sich an, erst im „Alarmfall" mittels Knopfdruck eine Aufzeichnung zu starten.

Für die Wahrung des Persönlichkeitsrechts der Betroffenen ist es von besonderer Bedeutung, dass der Aufnahmewinkel der Kameras bzw. die dadurch bestimmten Bildausschnitte sich strengstens am Zweck der Videobeobachtung orientieren. Dabei dürfen Sichtwinkel und Brennweite der Kameras keineswegs einen Einblick in Wohn- und Geschäftsräume ermöglichen, der eine Identifikation der dort wohnenden bzw. arbeitenden Menschen erlaubt.

Besonders beeindruckt hat mich das Konzept eines deutschen Anbieters von Videobeobachtungssystemen, wonach die Gesichter der beobachteten Personen in der Aufzeichnung grundsätzlich durch eine computergestützte Bildbearbeitung unkenntlich gemacht werden: Das eingesetzte Programm erkennt in den Videobildern mit hoher Zuverlässigkeit menschliche Gesichter und verdeckt diese mit einem geometrischen Muster, wie wir dies – allerdings von Menschen gesteuert – bereits aus dem Fernsehen etwa beim Interview von Personen kennen, die nicht erkannt werden wollen. Die Unkenntlichmachung kann durch eine erneute Bearbeitung der Aufzeichnung wieder aufgehoben werden, etwa durch den Warenhausdetektiv, wenn durch die Videobeobachtung ein Diebstahl aufgezeichnet wurde. Die Unkenntlichmachung der Gesichter der Kaufhauskunden kann von ihm jedoch nur dann aufgehoben werden, wenn er dafür einen kryptographischen Schlüssel benutzt, der Unbefugten nicht zur Verfügung steht.

Durch intensive Kontakte zu Anbietern und Mitarbeit in verschiedenen Gremien von Anbietern und wissenschaftlichen Einrichtungen setze ich mich für datenschutzfördernde Maßnahmen bei der Videotechnik ein.

4.2 Mehr Sicherheit mit Biometrie?

„Password oder PIN vergessen?" oder „Handelt es sich wirklich um die Person, für die sie sich ausgibt?".

Wer kennt nicht das Problem? Sicherheit – angefangen von Zugangsschutz zu Gebäuden oder Einrichtungen bis hin zur Anmeldung am PC – bekommt einen immer größeren Stellenwert in unserer Gesellschaft. Nicht erst seit dem 11. Sep-

tember 2001 ist der Ruf nach mehr Sicherheit gestiegen. Die Verfahren zur Identifikation bzw. Verifikation von Personen werden bei höheren Sicherheitsanforderungen und den damit verbundenen zusätzlichen Kontrollen zur Überprüfung von Personen personal- und kostenintensiv . Unterstützung bei der Feststellung der Identität von Personen kann die „Biometrie“ leisten. Bei dieser Technik werden unterschiedliche individuelle Merkmale des menschlichen Körpers wie Iris, Fingerabdruck, Stimme oder Gesichtsform mithilfe elektronischer Verfahren zur Identifikation bzw . Verifikation von Personen genutzt. Die zu bestimmenden Ausprägungen der Körpermerkmale werden dabei erfasst, gespeichert und automatisiert mit dem Original ver glichen. Damit wird der eigene Körper zum Schlüssel.

Zu den momentan auf dem Markt befindlichen biometrischen Systemen, die unterschiedliche biometrische Merkmale nutzen, liegen derzeit hinsichtlich eines Masseneinsatzes nur wenig aussagefähige Erfahrungswerte vor . Dies schließt deren Genauigkeit, Fehlerquote und praktische Nutzbarkeit ein. Auch werden Missbrauchsmöglichkeiten der biometrischen Informati onen diskutiert und die Entwicklung der einzelnen Verfahren ist noch nicht abgeschlossen. Dadurch, dass Missbrauchsmöglichkeiten bei einzelnen Anwendungen nicht ausgeschlossen werden können, werden biometrische Daten als hoch sensibel eingestuft.

Je nach Sicherheitsanforderung kann bereits jetzt der Einsatz von auf dem Markt vorhandenen Produkten sinnvoll sein. Dabei besteht auch durchaus die Möglichkeit eines datenschutzgerechten Einsatzes. Für die jeweilige Anwendung sind dazu das entsprechend den Sicherheitsanforderungen infrage kommende biometrische V erfahren, die Einsatzumgebung und die Randbedingungen zu untersuchen. Eine grundsätzliche Aussage über die Datenschutzkonformität der einzelnen Verfahren lässt sich nicht tref fen; hier fehlen derzeit noch vergleichende Erkenntnisse.

Maßstab für eine Anwendung im Sinne des Datenschutzes sollte z. B. sein, dass

- nur solche Verfahren zum Einsatz kommen, die eine Benachteiligung bestimmter Pe rsonengruppen weitgehend ausschließen;
- nur die für den späteren V ergleich notwendigen Merkmale und keine Überschussinformationen aufgenommen und gespeichert werden;
- eine strenge Zweckbindung der Daten sichergestellt ist;
- die Datensätze nur in einer gesicherten Umgebung (Netzwerk, Datenbank) verarbeitet werden;
- nach Möglichkeit auf eine zentrale Speicherung der Daten verzichtet wird, z. B. durch Speicherung der Daten auf einer Chipkarte oder einem Ausweis;
- nur kooperative biometrische Verfahren eingesetzt werden (die zu überprüfende Person muss aktiv in die Überprüfung einbezogen werden, keine verdeckte Erfassung);
- eine umfassende Informat ion über die gesamte Anwendung beim beteiligten Personenkreis erfolgt bzw . eine gesetzliche Regelung für den Einsatz vorliegt und
- eine sofortige Löschung der Daten vor genommen wird, sobald ein Betrof fener nicht mehr an der Anwendung teilnimmt.

Bei einem datenschutzfreundlichen Verfahren werden schon beim „enrolment“ – der ersten Datenerhebung – vom System nur die für einen späteren Vergleich notwendigen Daten erfasst und gespeichert. Eine Speicherung der vollständig erhobenen Daten ist in der Regel nicht notwendig.

Da wir erst am Anfang der Nutzung biometrischer Verfahren stehen, bleibt abzuwarten, ob mit der Zuordnung eines biometrischen Merkmals zu ei ner Person eine ausreichend sichere Verifikation oder Identifizierung vorgenommen werden kann.

Das Bundesamt für Sicherheit in der Informationstechnik prüft in Zusammenarbeit mit dem Bundeskriminalamt derzeit verschiedene biometrische Verfahren auf ihre Eignung.

So wird u. a. die Möglichkeit der Aufnahme von maschinenlesbaren biometrischen Merkmalen in Ausweisdokumenten und die Einführung eines vereinfachten Grenzkontrollverfahrens untersucht. Vor einer Einführung derartiger Systeme müssen jedoch noch die gesetzlichen Grundlagen geschaffen werden.

Ob und wann damit das Auswendiglernen von PIN-Nummern und Passwörtern der V ergangenheit angehört, bleibt abzuwarten.

4.3 Protection Profile – Sicherheitsanforderungen auf den Nenner gebracht

In der V ergangenheit wurde versucht, die Sicherheit und Vertrauenswürdigkeit von IT-Systemen durch die Zertifizierung nach dem europäischen Kriterienkatalog „ **I**nformation **T**echnology **S**ecurity **E**valuation **C**riteria (ITSEC)“ nachzuweisen. Der Kriterienkatal og enthält vordefinierte Funktionalitätsklassen, sodass Antragsteller ihr System oder Produkt einer Evaluation gemäß dieser Klassen unterziehen können. Die Anwendung der ITSEC- Kriterien ist sehr zeit- und kostenintensiv und berücksichtigt anwendungsspezifische Forderungen beispielsweise des Datenschutzes nicht. Da sich die ITSEC-Kriterien nur schwer am Markt durchsetzen ließen, wurde ein neuer Kriterienkatalog die „ **C**ommon **C**riteria for Information T echnology Security Evaluation (CC)“ erarbeitet und ve röffentlicht: Diese Kriterien sind eine W eiterentwicklung und Harmonisierung der ITSEC, des Orange Book und der Sicherheitskriterien Kanadas. Nach beiden Kriterienkatalogen ist eine Prüfung und Bewertung sowohl der Funktiona lität als auch der V ertrauenswürdigkeit eines Systems möglich, wobei die CC detailliertere Funktionalitätskriterien bieten als die ITSEC. Die CC sind für die Bewertung der Sicherheitseigenschaften aller informationstechnischer Systeme und Produkte geeignet. Die Standardisierungsorganisation ISO hat die Federführung bei der Entwicklung übernommen und die CC zum international genormten Standard (ISO/IEC 15408) geführt. Sie bestehen im Wesentlichen aus vier Teilen:

Einführung und allgemeines Modell,

- funktionale Sicherheitsanforderungen,
- Anforderungen an die Vertrauenswürdigkeit und
- Schutzprofile.

Aus datenschutzrechtlicher Sicht ist besonders die Möglichkeit interessant, für bestimmte Anforderungen, beispielsweise die Informationsflusssteuerung, Schutzprofile (Protection

Profiles) zu definieren und dies e registrieren zu lassen. Im Beschreibungsteil der Schutzprofile können die Sicherheitsziele anwendungsspezifisch und damit datenschutzgerecht beschrieben werden. Dies erhöht die bislang vermisste Flexibilität. Nach der Registri erung von solchen Profilen steht es Anbietern frei, ihre Produkt e auf die Einhaltung der Anforderungen der Schutzprofile prüfen zu lassen. Ich habe mich darum entschlossen, in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bayerischen Landesbeauftr agten für den Datenschutz die Möglichkeiten der flexiblen Gestaltung von Schutzprofilen für die Beschreibung einer Informationsflusssteuerung zu nutzen.

Das Schutzprofil „Benutzerbestimmbare Informationsflusskontrolle“ definiert Sicherheitsanforderungen für den Betrieb von IT-Anwendungen an Arbeitsplätzen, auf denen personenbezogene Daten verarb eitet werden. Das Konzept entstand aufgrund von Überlegungen, den Informationsfluss auf Arbeitsplatzrechnern gezielt steuern zu können. Hierzu wurden Anforderungen definiert, die es gestatten, die Zulässigkeit eines Informationsflusses auf einem Arbeitsplatzrechner gemäß definierbarer Regeln zu kontrollieren. Das Schutzprofil unterstützt besonders IT-Anwender mit geringer Fachkompetenz in der Durchsetzung des Schutzes von personenbezogenen Informationen. Die Einsatzmöglichkeiten des Schutzprofils liegen in folgenden Bereichen:

– E-Commerce (Data Warehouse etc.),

– eGovernment (Auftragsvergabe, Antragswesen etc.),

– Gesundheitswesen (elektronische Patientenakte etc.),

– Tele- und Mediendienste.

Jedem einzelnen Informati onsfluss kann eine seinem Schutzbedarf entsprechende Kombination von Sicherheitsmechanismen zugeordnet werden. Für die kontrollierten Informationen gewährleisten diese Mechanismen selektiv den Schutz

– der Integrität durch elektronische Signatur,

– der Vertraulichkeit durch Verschlüsselung und

– der Authentizität durch elektronische Zertifikate.

Es ist das erste Datenschutzprofil in Deutschland und wurde vom BSI evaluiert und am 1. Oktober 2002 zertifiziert. Am 12. November 2002 wurde es mir als Auftraggeber vom Präsidenten des BSI über geben. Die genauen Beschreibungen können auf meiner Homepage (http://www.bfd.bund.de/technik/protection_profile.html) eingesehen werden.

Der Einsatz nach dem Schutzp rofil zertifizierter Software bietet sich in verschiedenen Bereichen an: z. B. elektronischen Bezahlvorgängen, bei der Speicherung von medizinischen Daten oder bei Ba nkgeschäften mit Buchungstransaktionen. Das Schutzprofil selbst abstrahiert die datenschutzrechtlichen Anforderungen an eine Software so weit von technischen Details, dass eine Realisierung für eine breite Palette untersc hiedlicher IT-Umgebungen möglich ist.

4.4 Offene Software im Kommen

Nach meinem letzten Tätigkeitsbericht (siehe 18. TB Nr. 8.8) hat die Bereitschaft zum Eins atz offener Software (Open Source Software – OSS) in der Verwaltung weiter zugenommen:

– So hat der Ältestenrat des Deutschen Bundestags auf Vorschlag der IuK-Kommis sion am 14. März 2002 beschlossen, im Deutschen B undestag auf allen Servern das Betriebssystem Linux und auf den Clients W indows XP – wahlweise auch hier Linux – einzuführen. Als Verzeichnisdienst soll OpenLdap – ein freier Server auf der Grundlage des Lightweight Directory Access Protocol (LDAP), der eine einheitliche Basis für Personendaten wie E-Mail-Adresse und Fax-Nummer bietet – eingeführt werden. W ie der V orsitzende des Ältestenrats, Dr. Uwe Küster, auf dem Linuxtag 2002 ausführte, ist das eine richtungsweisende Entscheidung und ein Signal sowohl für die öf fentliche Verwaltung als auch für die Wirtschaft, verstärkt OSS einzusetzen.

– Bundesinnenminister Otto Schily unterzeichnete am 3. Juni 2002 zusammen mit dem IBM-Chef Erwin Staudt einen Kooperationsvertrag über die Förderung von OSS in der öf fentlichen Verwaltung. Damit werden OSS, Hardware und die erforderliche Unterstützung für Bund, Länder und Kommunen zu besonders günstigen Konditionen angeboten. Das Bundesministerium des Innern strebt eine Erhöhung des OSS-Anteils vor allem bei Servern an und rechnet für 2003 und 2004 im Serverbereich mit einer erheblichen Verschiebung hin zum Betriebssystem Linux.

– Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein Förderprogramm aufgelegt, mit dem OSS-Projekte in der Bunde sverwaltung unterstützt werden, bei denen Linux am Arbeitsplatz erprobt wird. Weiter hat das BSI mit dem Projekt „Ägypten“ erstmals ein Entwicklungsvorhaben nach den Grundsätzen der freien Softwareentwicklung durchgeführt. Mit dieser Software werden Verschlüsselung und Signatur für freie E-Mail-Systeme bereitgestellt. Weitere Informationen zu diesem Projekt sind im Internet unter http://www .gnupg.org/aegypten/index.de.html zu finden.

– Auch die Europäische Kommission befasst sich mit dem Einsatz von OSS (s. z. B. http://europa.eu.int/comm/enterprise/library/enterprise-europe/news-updates/new-economy/20020708.htm).

Für einen Umstieg gibt es also gute Gründe. So ist bei vielen Behörden die Ablösung vera lteter Hardware notwendig oder die eingesetzte Software wird von Anbietern bzw. Herstellern nicht mehr unterstützt. Für den Datenschutz sind besonders die hohe V erfügbarkeit und Sicherheit sowie die leichte Wartung vorteilhaft. Da s dabei gelegentlich vor gebrachte Argument hoher Schulungskosten bei den Anwendern berücksichtigt nicht, dass auch bei herkömmlicher , proprietärer Software Schulungsmaßnahmen notwendig sind, da sich dort die neuen Produkte oft erheblich von den eingesetzten Produkten unterscheiden (zur Umstellung in meiner Dienststelle s. Nr. 33.8).

Schließlich stellt die bei OSS übliche vollständige Of fenlegung des Quelltextes von Programmen für die IT-Sicherheit und den Datenschutz eine große Chance dar, insbesondere um verdeckte Programmfunktionen besser erkennen zu können. Prüfungen sind allerdings nur dann sicher , wenn der Quelltext auch tatsächlich von kompetenten Personen untersucht wird und die Programme auf einem ver-

trauenswürdigen Weg (z. B. durch Signaturen) bereitgestellt werden.

Bei der Nutzung der OSS-Produkte gibt es keinen „Zwang“ zur Registrierung und der damit verbundenen Übermittlung personen- oder organisationsbezogener Daten an den Hersteller, so wie es bei vielen proprietären Produkten der Fall ist. Vielmehr besteht bei OSS die Möglichkeit, diese im Sinne des Datenschutzes weiterzuentwickeln, um z. B. zu besseren Techniken der Datenvermeidung und Datensparsamkeit oder prüfbarer Sicherheit zu gelangen.

4.5 Programm zur „freiwilligen Selbstkontrolle“ einer Internetseite

Die Gestaltung einer Internetseite sowie die Erbringung von Zusatzdiensten muss sich im Rahmen der gesetzlichen Bestimmungen bewegen. Regelungen zum Datenschutz, die bei der Erstellung von Internetseiten zu beachten sind, finden sich beispielsweise in folgenden Bestimmungen:

– Teledienstegesetz

– Teledienstedatenschutzgesetz

– Mediendienstestaatsvertrag

– Telekommunikationsgesetz

– Fernabsatzgesetz

– Bundesdatenschutzgesetz

– Signaturgesetz.

Eine umfassende manuelle Prüfung von bestehenden Internetseiten auf die Einhaltung der gesetzlichen Regelungen scheitert in vielen Fällen allein schon an der Größe des Angebotes. Internetseiten können aus datenschutzrechtlicher Sicht zum Teil sehr unterschiedlich ausfallen. Dabei soll hier nicht besonderer Wert auf das Design oder die Form gelegt werden; vielmehr soll ausschließlich das Vorhandensein datenschutzrechtlicher Anforderungen wie Impressum, Datenschutzhinweise und Formulargestaltungen geprüft werden.

Vor diesem Hintergrund wurde in Zusammenarbeit mit der Fachhochschule Bonn-Rhein-Sieg die Möglichkeit einer automatisierten Datenschutzprüfung von Internetseiten entwickelt. Nach Abschluss der Arbeiten besteht mit dem Dienst „System zur automatisierten Datenschutzprüfung (SaD)“ nunmehr für Unternehmen und Behörden die Möglichkeit, in Form einer freiwilligen Selbstkontrolle ihre Internetauftritte automatisiert auf die Einhaltung von gesetzlichen Datenschutzforderungen hin zu überprüfen. Das Verfahren gestattet es den Verantwortlichen in Behörden und Unternehmen, datenschutzrechtlich bedenkliche Inhalte zu erkennen und zu beseitigen. Zur Prüfung selbst muss keine Software geladen werden. Hierzu reicht der Aufruf von SaD über die Internetseite http://sad.inf.fh-rhein-sieg.de/. Dort wird die Adresse der zu überprüfenden Seite hinterlegt und eine eigene „Ergebnis“-E-Mail-Adresse angegeben. SaD übernimmt nach dieser Eingabe die Überprüfung selbst. Hierzu wird zunächst die komplette Internetseite der angegebenen Adresse auf den SaD-Server heruntergeladen. Sobald dieser Ladevorgang abgeschlossen ist, beginnt SaD mit der Prüfung der Seite. Dies erfolgt beispielsweise über die Suche von Schlüsselwörtern. So wird das Impressum über die Suche der Worte „Impressum“, „Wir über uns“ usw. gesucht. Findet SaD entsprechende Eintragungen, wird davon ausgegangen, daß entsprechende Inhalte vorhanden sind. Das Testen von Formularen erfolgt über die Suche von entsprechenden Schlüsselcodes in der HTML-Programmierung. Auch die näheren Inhalte der Formulare können über Schlüsselwörter abgeprüft werden. So geht SaD davon aus, dass das Wort „Beruf“ vor einem Formularfeld die Eingabe einer Berufsbezeichnung im Formular erfordert. Die Ergebnisse dieser Untersuchungen speichert SaD in einer Datenbank. Nach Abschluss der Prüfung wird an die „Ergebnis“-E-Mail-Adresse ein Abschlussreport gesendet. Die heruntergeladenen Internetseiten werden dann gelöscht.

SaD ist modular aufgebaut, d. h. pro geprüftem Kriterium gibt es ein Prüfskript, sodass eine Erweiterung von SaD jederzeit sichergestellt ist. Auch „prangert“ SaD keine Mängel an, sondern will durch einen Hinweis den Anbieter der Internetseite auf mögliche Mängel nur aufmerksam machen. Es bleibt dem Anbieter überlassen, ob er dem Hinweis von SaD folgt und die Gestaltung nochmals kritisch hinterfragt.

Eine Zielsetzung von SaD war die Bereitstellung eines Dienstes zur freiwilligen Selbstkontrolle. Um diesem Ziel gerecht zu werden, mussten Sicherheitsfunktionen im Verfahren berücksichtigt werden; u. a. sollte auf keinen Fall eine Überprüfung von Seiten anderer Behörden oder Unternehmen möglich sein. Dies wurde dadurch realisiert, dass vor dem Start der Prüfung fest gestellt wird, ob die „Ergebnis“-E-Mail-Adresse aus der Domäne stammt, die zu überprüfen ist. Ferner wird an diese Adresse eine E-Mail gesendet, in der eine Zufallszahl genannt wird, unter der das Ergebnis abrufbar ist. Nur durch die Bestätigung des Erhalts dieser Zufallszahl kann das Ergebnis von SaD abgerufen werden. Die Überprüfung anderer Internetseiten als der eigenen ist somit weitgehend ausgeschlossen.

Um zu verhindern, dass es durch mehrmaliges Aufrufen von SaD zu einer Überlastung der Internetseite kommt, wird der Startauftrag ebenfalls in eine Datenbank eingetragen. Erfolgt eine zweite Prüfanforderung innerhalb kurzer Zeit, wird diese abgelehnt.

SaD steht derzeit kostenlos für Behörden und Unternehmen zur Verfügung.

4.6 Nur ein Programmfehler verhinderte Ausspionieren von Kollegen

Immer wieder beweist es sich, dass keine Kontrolle wie die andere verläuft und man niemals davon ausgehen kann, weit verbreitete und scheinbar hinlänglich bekannte IT-Systeme wirklich zu kennen. Anlässlich der Kontrolle einer Behörde, die ein lokales Netzwerk mit den zurzeit häufig anzutreffenden Systemkomponenten Novell in Verbindung mit Windows NT auf Server- und Clientseite betreibt, wurden stichprobenartig auch einige Standard-Arbeitsplatzcomputer im Bereich der Zentralabteilung einer genaueren Überprüfung unterzogen.

Hierbei ergab sich aus Sicht einer bestimmten Nutzergruppe der Eindruck, dass über die Option ‚Netzlaufwerk verbinden‘ unter ‚Extras‘ im Windows-Explorer problemlos eine Verbindung zu Netzlaufwerken anderer Mitarbeiter hergestellt werden konnte mit der Folge, dass hier scheinbar ein Zugriff auf die personenbezogenen Daten dieser Mitarbeiter

möglich war. Im Wesentlichen handelte es sich hierbei um Daten, die bei der Nutzung des Internetexplorers anfallen (temporäre Internetdateien usw.). Nach Überprüfung der systemseitigen Einstellungen der betroffenen PC sowie Server ergab sich folgendes Bild: Alle Benutzer der betreffenden Organisationseinheit, die auf einem bestimmten Server eingerichtet waren und die Möglichkeit zum Zugriff auf Netzlaufwerke hatten, konnten in den Fällen, bei denen auf dem Server die Nutzereinstellungen im Systemobjekt „Public“ auf ‚Read‘ und ‚File-Scan‘ gesetzt waren, die Verzeichnisnamen aller auf diesem Server befindlichen Nutzer erkennen.

Der angezeigte Inhalt in diesen Verzeichnissen war allerdings lediglich mit dem Inhalt der eigenen gleichlautenden Unterverzeichnisse identisch; eine tatsächliche Kenntnisnahmemöglichkeit von Inhalten anderer Nutzer fand also nicht statt. Dies war aber nur dem glücklichen Umstand zu verdanken, dass im Windows-Dateimanager ein Fehler vorlag. Dieser herstellerseitig nicht dokumentierte Fehler besteht darin, dass bei Ablage der Profildaten auf einem Netzlaufwerk zwar die angelegten Verzeichnisnamen, nicht aber deren Inhalte angezeigt werden. Gesteuert durch clientseitige Systemeinträge erfolgt der Zugriff immer auf die lokalen Daten. Ohne diesen Fehler wäre der Zugriff auf die Daten der anderen Nutzer aufgrund der eingestellten Rechte auf dem Server tatsächlich möglich gewesen.

Aus datenschutzrechtlicher Sicht lag hier an sich ein schwerwiegender Mangel in der Rechteverwaltung vor, der für sich allein schon Grund für eine Beanstandung nach § 25 BDSG gewesen wäre. Aufgrund besonderer Umstände sowie der Zusage der Behörde, die Konfiguration unverzüglich zu ändern und die nutzerspezifischen Profildaten nicht mehr auf Netzlaufwerken, sondern lokal abzulegen, habe ich von einer Beanstandung abgesehen.

4.7 Datenschutzgerechtes eGovernment

Infolge der zunehmenden elektronischen Kommunikation verändern sich auch die Verwaltungsvorgänge. Umständliche Behördengänge, eingeschränkte Sprechzeiten und oftmals lange Wartezeiten vor Ort sollen zukünftig weitestgehend vermieden werden, indem z. B. An- und Abmeldungen, Anträge, ja sogar Verwaltungsakte elektronisch versandt und empfangen werden können. In diesem Zusammenhang wird der Begriff Electronic-Government (eGovernment) verwendet. Man spricht aber nicht nur von eGovernment, wenn es sich um das Außenverhältnis der Verwaltung handelt, also zur Wirtschaft und zum Bürger, sondern man spricht auch von eGovernment, wenn innerhalb der Verwaltung Verfahren der Vorgangsbearbeitung den neuen Kommunikationstechniken angepasst werden, um diese auch sinnvoll zu nutzen. Als Beispiel für das Außenverhältnis der Verwaltung seien die Ausschreibung für die Beschaffung stellvertretend für die Beziehung Verwaltung-Wirtschaft und das Verfahren zur elektronischen Steuererklärung ELSTER für die Beziehung Verwaltung-Bürger genannt.

Gesetzliche Rahmenbedingungen hierfür wurden u. a. mit dem Telekommunikationsgesetz, dem Teledienstedatenschutzgesetz, dem Mediendienstestaatsvertrag, dem neuen Signaturgesetz und dem überarbeiteten Verwaltungsverfahrensgesetz geschaffen.

Aus der Sicht des Datenschutzes sind bei eGovernment-Anwendungen u. a. folgende Aspekte zu beachten:

- Datenvermeidung und Datensparsamkeit (z. B. Pseudonymisierung);
- sichere Transaktionen über das öffentliche Netz;
- Transparenz der Verfahren (Datenschutzinformationen, elektronische Auskunft, Berichtigung, Löschung);
- Beachtung der Zweckbindung und anderer datenschutzrechtlicher Vorschriften sowie
- datenschutzgerechte Internetangebote (nur zulässige Daten ins Internet, rechtzeitige Löschung von Verbindungsdaten, Anbieterkennzeichnung, Reduzierung von Cookies, Anonymität von Statistiken).

Insbesondere die Anbindung der Verwaltung an das Medium Internet erfordert eine sichere und vertrauliche Kommunikation sowie einen angemessenen Schutz personenbezogener Daten. Aus datenschutzrechtlicher Sicht muss gewährleistet sein, dass keine Unberechtigten personenbezogene Daten erlangen oder gar verfälschen können. Hier gilt es, geeignete Sicherheitsmaßnahmen wie Verschlüsselung und elektronische Signatur einzusetzen. Überall da, wo es auf die Integrität und Authentizität einer Willenserklärung ankommt, bietet sich der Einsatz der elektronischen Signatur an. Eine vertrauliche Kommunikation erfordert die Verschlüsselung der zu übertragenden Informationen. Ohne hinreichende Sicherheit werden die Anwender den neuen technischen Möglichkeiten nur bedingt vertrauen und sie darum auch nicht nutzen.

Die Bundesregierung plant, im Rahmen der Initiative BundOnline 2005 bis zum Jahr 2005 alle internetfähigen Dienstleistungen der Bundesverwaltung auch über das Internet online bereitzustellen. Zur Förderung der Initiative BundOnline 2005 wurde von Seiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ein eGovernment-Handbuch erarbeitet, welches erstmalig öffentlich auf der CeBit 2001 vorgestellt wurde. Dieses Handbuch wird modular im Internet (www.bsi.bund.de) veröffentlicht und aktualisiert. Es enthält sowohl methodische Hinweise für planmäßiges Vorgehen als auch praktische Lösungsansätze. Des Weiteren soll die Initiative MEDIA@KOMM der Bundesregierung diese Entwicklung in den Städten und Gemeinden gezielt unterstützen und die Einführung von eGovernment-Dienstleistungen beschleunigen.

Die Datenschutzbeauftragten des Bundes und der Länder haben im Oktober 2000 die Entschließung „Vom Bürgerbüro zum Internet – Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung“ verabschiedet. In dieser Entschließung erklären sie ihre ausdrückliche Bereitschaft, solche Entwicklungsprozesse konstruktiv zu begleiten. Die 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 8. und 9. März 2001 beschlossen, eine Arbeitsgruppe „eGovernment“ einzurichten, dessen Federführung Niedersachsen übernommen hat und an der auch ich beteiligt war. Als Ergebnis dieser Arbeitsgruppe ist die Broschüre „Datenschutzgerechtes eGovernment“ entstanden, die als Handreichung für den Praktiker in der Verwaltung gedacht ist; sie steht jedoch auch für alle anderen Interessenten zum Abruf auf den Internetseiten des virtuellen Datenschutzbüros (www.datenschutz.de) bereit.

5 Deutscher Bundestag – Datenschutzordnung für den parlamentarischen Bereich

Zu den Themen, die seit vielen Jahren immer wieder Gegenstand in meinen Tätigkeitsb erichten waren, gehört die Schaffung einer Datenschutzordnung für den Deutschen Bundestag (vgl. 17. TB Nr. 3.1; 16. TB Nr. 35, dort Nr. 1; 15. TB Nr. 2; 14. TB Nr . 3.1). Von der Novellierung des Bundesdatenschutzgesetzes im Jahre 2001 hatte ich erhoff t, dass hiervon auch neue Impulse für den Erlass einer Datenschutzordnung des Deutschen Bundestages ausgehen würden. Tatsächlich waren die Ge spräche mit dem Deutschen Bundestag zu diesem Thema am Ende der ver gangenen Legislaturperiode sehr intensiv. Besondere Probleme für eine tragbare Lösung, die insbesondere auch den besonderen Status der Abgeordneten und des Parlaments berücksichtigen muss, bereiteten insbesondere eine Schadensersatzregelung entsprechend den §§ 7 und 8 BDSG, Regelungen für eine Datenübermittlung ins Ausland, Benachrichtigungspflichten nach § 19a BDSG und Auskunftspflichten.

Eine Untersuchung von Datenschutzordnungen für den parlamentarischen Bereich im Ausland und bei den Ländern ergab folgendes: Zwar besteht lediglich in Schweden ein eigenes Gesetz für das Informationssystem Rixlex des Reichstags. In den anderen 13 Ländern, die auf meine Anfrage geantwortet haben, gilt – abgesehen von Dänemark und der Schweiz – für die dortigen Parlamente das jeweilige nationale Datenschutzgesetz, zum Teil mit geringen Anpassungen an die Besonderheiten des parlamentarischen Bereichs. In Deutschland haben mittlerweile die Landesparlamente von sechs Ländern (Bremen, Hambur g, Hessen, Niedersachsen, Rheinland-Pfalz und Schleswig-Holstein) eine für sie geltende Datenschutzordnung erlassen, die sich an einem entsprechenden Musterentwurf orientiert, den die Konferenz der Präsidentinnen und Präsidenten der deutschen Landesparlamente bereit s Mitte der Neunzigerjahre vorgelegt hat. In elf Ländern gibt es in den Landesdatenschutzgesetzen Regelungen zum Datenschutz im parlamentarischen Bereich und nur in vier Ländern wurden bislang datenschutzrechtliche Regelungen für das Landesparlament nicht getroffen.

Zu meinem Bedauern war am Ende der Legislaturperiode die Zeit zu knapp, um die erfo rderlichen Änderungen des Bundesdatenschutzgesetzes und eine Datenschutzordnung für den Deutschen Bundestag zu beschließen. Ich würde es begrüßen, wenn sich der Deutsche Bundestag in dieser Legislaturperiode eine Datenschutzordnung gibt.

6 Auswärtiges Amt

6.1 Das Programm VISA 2000

Nach der Ausländerdateien-Verordnung (AuslDatV) führen die Auslandsvertretungen eine Datei über die erteilten V isa und Transit-Visa (Visadatei – § 7 AuslDatV) und eine Datei über die Versagungen von Visa (Visa-Versagungsdatei – § 8 AuslDatV). Geführt werden diese Dateien in den Botschaften und Generalkonsulaten zu rzeit noch überwiegend mithilfe herkömmlicher Datenbanken (siehe auch 18. TB Nr. 4.3.5).

Bei einem Generalkonsulat habe ich mir im Berichtszeitraum das Programm VISA 2000 angesehen, das keine reine Datenbank mehr ist, sondern ein datenbankbasiertes automatisiertes Verfahren zur Durchführung des V isa-Verfahrens (vgl. Abbildung 1). Obwohl derzeit noch zusätzlich Papierausdrucke aus dem System gemacht werden, wird das Verwaltungsverfahren durch das Programm bestimmt. W esentliches Ziel ist es, dem Antragsteller möglichst noch am gleichen Tag das Visum auszuhändigen. Beim herkömmlichen Verfahren vergehen in der Regel zwei bis vier T age zwischen der Stellung eines sc hriftlichen Antrags und der Ausstellung des V isums. Auf die Stellung eines schriftlichen Antrags soll demgegenüber beim System VISA 2000 zukünftig grundsätzlich verzichtet werden. Dazu werden die für das Visa-Verfahren erforderlichen Daten am Visa-Schalter erfragt und direkt in das System VISA 2000 eingegeben. Dies hat zur Folge, dass die Bearbeitung des Antrags am Schalter nunmehr etwas länger dauert, dafür aber andererseits die Bearbeitung des V isumantrags in der publikumsfreien Zeit erheblich kürzer wird. Insbesondere können die erforderlichen Anfragen beim Ausländerzentralregister (AZR) im Bundesverwaltungsamt (BV A) sofort online erfolgen, wenn die Pflichtfelder im Programm VISA 2000 ausgefüllt sind. Es ist bereits angedacht, den Erfassungsaufwand am Schalter dadurch erheblich zu reduzieren, dass den Antragstellern das Antragsformular nicht nur – wie bereits seit einiger Zeit – im Internet zum Ausdrucken zur V erfügung gestellt wird, sondern darüber hinaus ermöglicht wird, das Formular online auszufüllen und an die Auslandsvertretung über Internet zu versenden. Bei der Abholung des V isums müssten dann die Daten ggf. nur noch ergänzt werden, da eine Vorabprüfung bereits nach der Online-Übermittlung in der publikumsfreien Zeit erfolgen könnte. Hinzu kommt, dass einige Verfahrensschritte (z. B. Berechnung der Dauer der Gültigkeit des Visums oder von Gebühren, Ausdrucken des Visa-Etiketts) automatisiert erfolgen und die Zeit der Bearbeitung des Antrags hierdurch erheblich verkürzt wird. Auch im Falle der Verweigerung des Visums hilft das System weiter, indem es für die wesentlichen V ersagungsgründe Textbausteine sowohl in der deutschen als auch in der jeweiligen Landessprache bereit hält.

Das Programm VISA 2000 ist derzeit noch in der Erprobungsphase. Es wird künftig im Zusammenspiel von Auslandsvertretungen und BVA bei der Erteilung von Visa eine zentrale Rolle spielen. Die in das System VISA 2000 einfließenden Daten des Antragstellers werden in absehbarer Zeit dem AZR im BVA online zur Verfügung gestellt. Dies gilt sowohl für die beim Antragsteller erhobenen Daten – einschließlich von biometrischen Merkmalen, wie z. B. Passbildern – als auch für die Daten über die Entscheidung des Antrages.

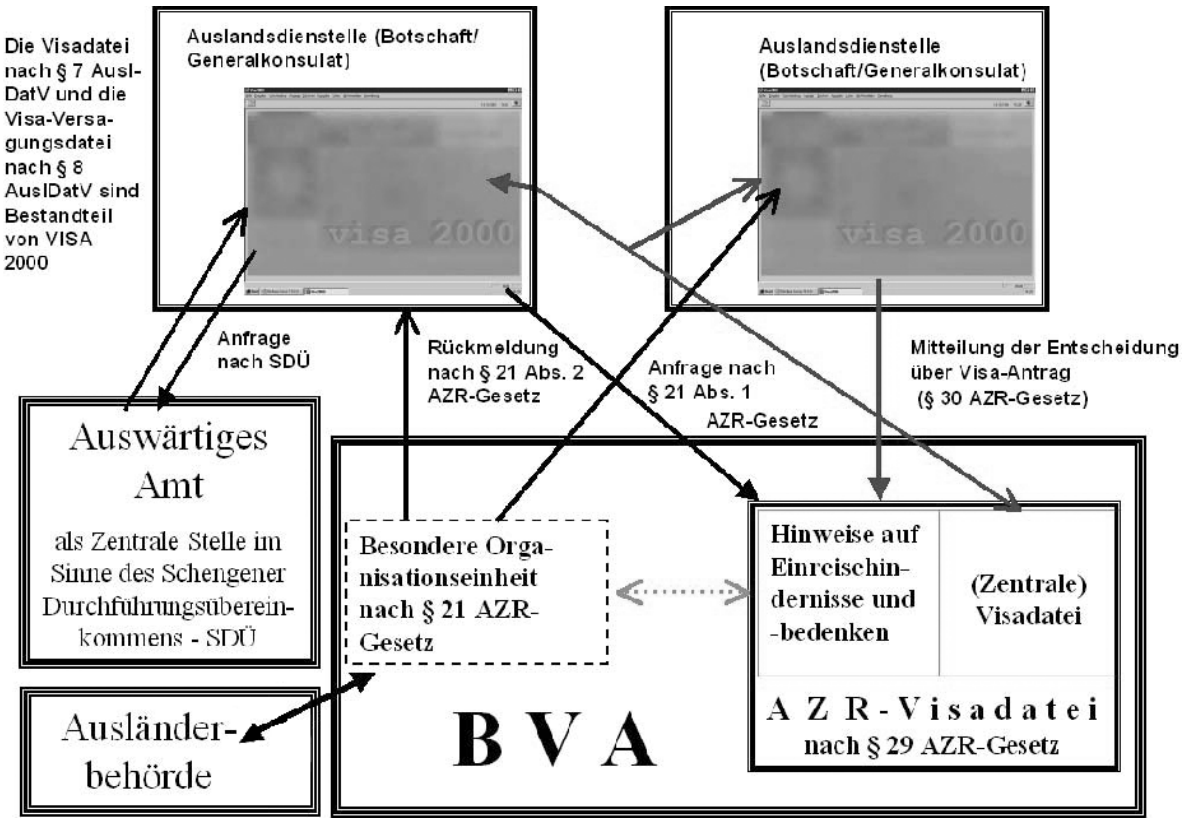
Bisher wurde von den Auslandsvertretungen lediglich beim BVA nachgefragt, ob dem Visumantrag des Ausländers Einreisehindernisse oder -bedenken entgegenstehen. Nach den Änderungen durch das Terrorismusbekämpfungsgesetz wird sich das Verfahren insoweit ändern, als nicht nur in den Auslandsdienststellen nach den §§ 7 und 8 AuslDatV das Ergebnis des Visumsverfahrens in der Visa- bzw. Visa-Versagungsdatei festgehalten wird, sondern darüber hinaus auch im AZR nach § 29 Ausländerzentralregistergesetz eine zentrale Datei geführt wird, die die Entscheidung über einen Visumantrag enthält. Dabei kann die Auslandsvertretung erfahren, ob der Antragsteller bereits von einer anderen Auslandsvertretung ein V isum erhalten hat oder dieses abgelehnt wurde und aus welchen Gründen. Hierfür muss die

Auslandsdienststelle ihre Entscheidung nicht nur dem Antragsteller, sondern auch dem AZR mitteilen. Über das System VISA 2000 dürfte es darüber hinaus zukünftig auch möglich sein, digitale Passbilder des Visa-Antragstellers an die Visa-Datei des AZR zu übermitteln. Die Aufnahme eines Passbildes ist derzeit im Programm VISA 2000 (noch) nicht vorgesehen, technisch aber machbar.

Das Programm VISA 2000 ist ein neuer Ansatz, V erwaltungsverfahren (möglichst) ohne Papier durchzuführen. Grundsätzliche datenschutzrechtliche Bedenken habe ich gegen dieses System nicht. Allerdings ist ihm anzumerken, dass Ausgangspunkt der Überlegungen die Durchführung des Verfahrens und nicht die Erfüllung gesetzlicher Normen ist. Dies wird zum Beispiel dadurch deutlich, dass in einem Evaluierungsbericht für das System gefordert wird, es solle eine Visa-Versagungsdatei nach § 8 AuslDatV implementiert werden. Tatsächlich ist diese Funktion – wenn auch etwas versteckt – im System vorhanden, und auch in der Systembeschreibung wird auf die Löschungsregelungen der §§ 7 und 8 AuslDatV hingewiesen. Allerdings wird dort lediglich das Verfahren beschrieben, wie bei Ablauf der Löschungsfristen des § 7 Abs. 4 AuslDatV (ein Jahr nach Ablauf der Geltungsdauer des V isums) bzw. § 8 Abs. 3 Nr . 2 AuslDatV (fünf Jahre nach Ablehnung des Antrags) der Datensatz per Hand gelöscht werden kann. Nicht nur , dass in der derzeitigen Erprobungsphase im besuchten Generalkonsulat noch kein Datensatz gelöscht wurde; aufgrund bisheriger Erfahrungen bei Kontrollen, wie mit den bisherigen Dateien nach §§ 7 und 8 AuslDatV umgegangen wird, erwarte ich, dass auch künftig nur sehr selten Datensätze gelöscht werden. Dies gilt insbesondere für Auslandsvertretungen, in denen sehr viele V isa erteilt bzw. verweigert werden. Gegenüber dem Auswärtigen Amt habe ich daher gefordert, dass diese Löschfunktion unbe dingt automatisiert werden muss. Eine Antwort steht hierzu allerdings noch aus.

Abbildung 1 (zu Nr. 6.1)

Das Programm Visa 2000



6.2 Der „Internationale Personaldatenpool“

Im Berichtszeitraum wurde das Auswärtige Amt vom Bundeskabinett beauftragt, eine Datenbank („Internationaler Personaldatenpool“) zu schaffen, mit deren Hilfe die deutschen Interessen bei der Besetzung von Stellen in internationalen Organisationen besser gewahrt werden können. Die Bundesregierung verfolgt mit dieser Datenbank das politische Interesse, die Zahl Deutscher in internationalen Organisationen zu erhöhen. Dieser Auftrag an das Auswärtige Amt hat folgenden Hintergrund: Zwar arbeiten ca. 3 500 Deutsche (vergleichbar höherer Dienst) derzeit in internationalen Organisationen, davon ca. 1 000 in den Organen der EU. Trotz ihrer hohen Bevölkerungszahl und ihrer im Durchschnitt ansehnlichen finanziellen Leistungen an die internationalen Organisationen ist die Bundesrepublik Deutschland damit jedoch im Vergleich zu ihren westlichen Partnerstaaten personell in vielen Organisationen nicht so vertreten, wie es aus deutscher Sicht wünschenswert wäre. Gemeinsam mit dem Büro Führungskräfte zu internationalen Organisationen (BFIO) der Bundesanstalt für Arbeit sieht das Auswärtige Amt seine Rolle in der Information über Aufgabengebiete und Wirkungsweise der internationalen Organisationen, in der Schaffung erleichterten Zugangs zu Stellenausschreibungen sowie in der Unterstützung von Bewerbungen, die in ein konkretes Stadium getreten sind.

Bei der Erfüllung dieser Aufgabe hat mich das Auswärtige Amt frühzeitig beteiligt. Die von ihm gefundene Lösung halte ich aus datenschutzrechtlicher Sicht für sehr gelungen. Der potenzielle Bewerber bei internationalen Organisation pflegt seine Personaldaten (Werdegang, berufliche Qualifikation etc.) selbst und erhält automatisch einen Abgleich aus dem korrespondierenden „internationalen Stellenpool“ mit eventuell für ihn geeigneten Stellenausschreibungen. Der „Internationale Personaldatenpool“ ist lediglich ein, wenn auch sehr gutes Hilfsmittel für eine Bewerbung bei einer internationalen Organisation. Da diese Stellen ihrerseits keinen Zugriff auf die Datenbank haben, muss sich der Interessierte letztendlich selbst bei der internationalen Organisation bewerben. Er kann allerdings dank des „Internationalen Personaldatenpools“ des Auswärtigen Amtes seine Aussichten für eine erfolgreiche Bewerbung realistisch einschätzen. Die vom Bewerber dort eingegebenen Daten werden nur von Mitarbeitern des „Koordinators für internationale Personalpolitik“ im Auswärtigen Amts gelesen. Keine andere deutsche oder internationale Organisation hat ohne Einverständnis des Betroffenen Zugriff. Um dies sicherzustellen, werden die Daten auf den Seiten des Auswärtigen Amtes im Internet mit einer zertifizierten SSL-Verschlüsselung versehen.

Der Personaldatenpool ist mittlerweile unter der Adresse http://www.auswaertiges-amt.de/www/de/aamt/job/jobs_io/personalpool_html ins Internet eingestellt worden.

7 Innere Verwaltung, Statistik

7.1 Asylrecht

7.1.1 Wer kontrolliert Eurodac?

In meinem 17. TB (Nr. 5.7) habe ich ausführlich über die Regelungen des geplanten **Euro**päischen **dac**tyloskopischen Fingerabdrucksystems Eurodac berichtet. Über das Entstehen der Eurodac-Verordnung, die im Dezember 2000 in Kraft getreten ist, habe ich im 18. TB (Nr. 5.2.3) informiert. Seitdem war es Aufgabe der Bundesrepublik Deutschland, die technischen und organisatorischen Voraussetzungen für die nationale Umsetzung dieser Verordnung zu schaffen. Unter anderem waren ergänzende nationale Regelungen im Asyl- und Ausländerrecht sowie in der Asylzuständigkeitsverordnung erforderlich, um die angestrebte Aufnahme des Eurodac-Verfahrens in der Zentraleinheit in Luxemburg Anfang 2003 verwirklichen zu können. Bei der Vorbereitung dieser Regelungen, an denen mich das BMI beteiligt hat, konnte ich datenschutzrechtliche Verbesserungen erreichen. So wird z. B. das Bundesamt für die Anerkennung ausländischer Flüchtlinge ab der Realisierung des Zugriffs auf die nationale Eurodac-Datenbank keine Fingerabdruckblätter von Asylbewerbern mehr vorhalten bzw. in seinem IT-System MARIS (vgl. Nr. 7.1.2) speichern.

Einen weiteren Schwerpunkt bildeten die begleitenden Arbeiten zur Errichtung der gemeinsamen Kontrollstelle, die nach Artikel 20 der Eurodac-Verordnung vorgesehen ist. Sie setzt sich aus Vertretern der nationalen Kontrollstellen zusammen, deren Aufgabe es ist, die Tätigkeit der Zentraleinheit daraufhin zu kontrollieren, ob durch die Verarbeitung oder Nutzung der bei ihr vorhandenen Daten die Rechte der betroffenen Personen verletzt werden. Darüber hinaus kontrolliert sie die Rechtmäßigkeit der Übermittlung personenbezogener Daten an die Mitgliedsstaaten durch die Zentraleinheit. An der Gestaltung der Geschäftsordnung der gemeinsamen Kontrollstelle habe ich intensiv mitgewirkt. Dabei habe ich erreicht, dass diese eine ähnliche Ausgestaltung erhalten hat, wie sie bereits die Geschäftsordnungen der Kontrollinstanzen für Europol und Schengen besitzen.

Über die Aufnahme des Wirkbetriebs und erste Praxiserfahrungen werde ich in meinem nächsten Tätigkeitsbericht informieren.

7.1.2 Systems MARIS im Bundesamt für die Anerkennung ausländischer Flüchtlinge eingeführt

Bereits in meinem letzten Tätigkeitsbericht (Nr. 5.2.2) habe ich über das Workflowsystem **M**igration **A**syl **R**e**I**ntegrations**S**ystem (MARIS, früher IT-2000) beim Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl) berichtet. MARIS, das weitestgehend papierlos arbeitet, hat das bisherige System ASYLON abgelöst, da dieses nicht mehr den gestiegenen Anforderungen entsprach. Während der Evaluierungsphase wurde das System in fünf Außenstellen des BAFl (Hamburg, Berlin, Lebach, Zirndorf, Dortmund) im Echtbetrieb getestet. Seit Herbst 2002 ist es flächendeckend eingeführt, d. h. alle Arbeitsplätze sind nunmehr angeschlossen. Im Juli 2002 habe ich mich in der Außenstelle Zirndorf über den Sachstand bei der Einführung von MARIS informiert. Ich konnte mich davon überzeugen, dass meine datenschutzrechtlichen Forderungen umgesetzt worden sind. Insbesondere die vorgesehene Protokollierung aller Zugriffe nach einem mit mir abgestimmten Zufallsprinzip entspricht den Belangen des Datenschutzes (s. auch 7.1.3).

Darüber hinaus ist ein Projekt mit Verwaltungsgerichten und Ausländerbehörden geplant, das den elektronischen Datenaustausch mittels qualifizierter digitaler Signatur vorsieht.

Die digitale Signatur soll auch in MARIS übernommen werden. Die gescannten Dokumente werden dabei mit der digitalen Signatur versehen und haben dann denselben Beweiswert wie Papierdokumente.

7.1.3 Telearbeitsplätze von Einzelentscheidern im Bundesamt für die Anerkennung ausländischer Flüchtlinge – unter engen Voraussetzungen vertretbar

Nach einer Absprache zwischen dem Präsidenten des BAFl und mir ist – zunächst im Rahmen eines Pilotprojektes – 15 Einzelentscheidern des BAFl in diesem besonders sensiblen Arbeitsbereich Telearbeit unter bestimmten, engen Voraussetzungen angeboten worden. Das Pilotprojekt war auf zwei Jahre befristet und endete mit Ablauf des Jahres 2002. Danach soll das BAFl absprachegemäß über seine Erfahrungen berichten, bevor über das weitere Verfahren entschieden wird. Ich werde die Entwicklung auch in Zukunft begleiten.

Die Kontrolle solcher Telearbeitsplätze ist einer der Schwerpunkte meiner letzten Informations- und Kontrollbesuche beim BAFl im Juli und November 2002 gewesen. Dabei habe ich sowohl die technischen Rahmenbedingungen als auch den eigentlichen Arbeitsablauf am Büro- und am Telearbeitsplatz kontrolliert. Grundlage für die Arbeit des Einzelentscheiders am Telearbeitsplatz sind die in der „Dienstanweisung Einzelentscheider“ festgelegten Kriterien, die auch von mir positiv bewertet werden. Darüber hinaus ist u. a. eine umfangreiche Protokollierung vorgesehen. So werden sowohl die Zugriffe des Einzelentscheiders auf die Datenbank MARIS an seinem Telearbeitsplatz als auch die Zugriffe des Referatsleiters auf die elektronischen Arbeitskörbe des Einzelentscheiders zu 100 % protokolliert. Alle weiteren Zugriffe werden nach einem mit mir abgestimmten Zufallsprinzip festgehalten.

7.1.4 Bundesbeauftragter für Asylangelegenheiten trennt sich von seinen Altakten

Im Frühjahr 2001 habe ich beim Bundesbeauftragten für Asylangelegenheiten (BBfA) einen datenschutzrechtlichen Kontroll- und Informationsbesuch durchgeführt. Der nach § 6 Asylverfahrensgesetz beim BAFl seit 1965 eingerichtete Bundesbeauftragte kann sich an den Asylverfahren vor dem Bundesamt und an Klageverfahren vor den Verwaltungsgerichten beteiligen und gegen Entscheidungen des Bundesamtes klagen. Schwerpunkt meiner Kontrolle war der Verfahrensablauf innerhalb der Dienststelle sowie die Verwaltung des Aktenbestandes, der bis Mitte 1995 in Papierform und danach auf elektronischem Weg erfasst worden ist. Zu den Arbeitsabläufen in den Fachreferaten waren Bemerkungen und Anregungen aus datenschutzrechtlicher Sicht nur in geringem Umfang erforderlich. Hingegen musste ich feststellen, dass zum Zeitpunkt meiner Kontrolle der gesamte seit Errichtung der Dienststelle entstandene Aktenbestand noch erhalten war. Zwar bestehen für die Dauer der Aufbewahrung von Asylverfahrensakten, mit Ausnahme der Regelungen für erkennungsdienstliche Unterlagen, keine weiteren einschlägigen Vorschriften, gleichwohl hat das BAFl verwaltungsinterne Aufbewahrungs- und Löschungsfristen vorgegeben. Vergleichbare Regelungen bestanden beim BBfA aber nicht. Da auf den Altaktenbestand praktisch nicht mehr zugegriffen wird und weil sich ein Vergleich mit BAFl-Akten ähnlichen Inhalts anbietet, habe ich eine an den Vorgaben des BAFl orientierte Vernichtungsregelung gefordert. Der BBfA hat daraufhin in einem ersten Schritt die gesamten Aktenbestände vernichten lassen, die bis zum 31. Dezember 1985 angelegt worden sind. Akten späterer Jahrgänge werden sodann schrittweise der Vernichtung zugeführt. Eine solche Vorgehensweise halte ich für sachgerecht.

7.2 Neues Sicherheitsmerkmal für Pässe und Personalausweise – das Identigramm

Auch nach dem Verkauf der Bundesdruckerei GmbH an ein privates ausländisches Unternehmen im Dezember 2000 besteht meine umfassende Kontrollzuständigkeit für die Einhaltung datenschutzrechtlicher Vorschriften bei der Herstellung von personalisierten Dokumenten durch die Bundesdruckerei GmbH fort.

Bei einem Informations- und Kontrollbesuch im März 2002 habe ich schwerpunktmäßig den (technischen) Ablauf der Fertigung von so genannten Identigrammen kontrolliert, die seit Oktober 2001 generell auf Personalausweisen und Pässen aufgebracht werden (vgl. Abbildung 2).

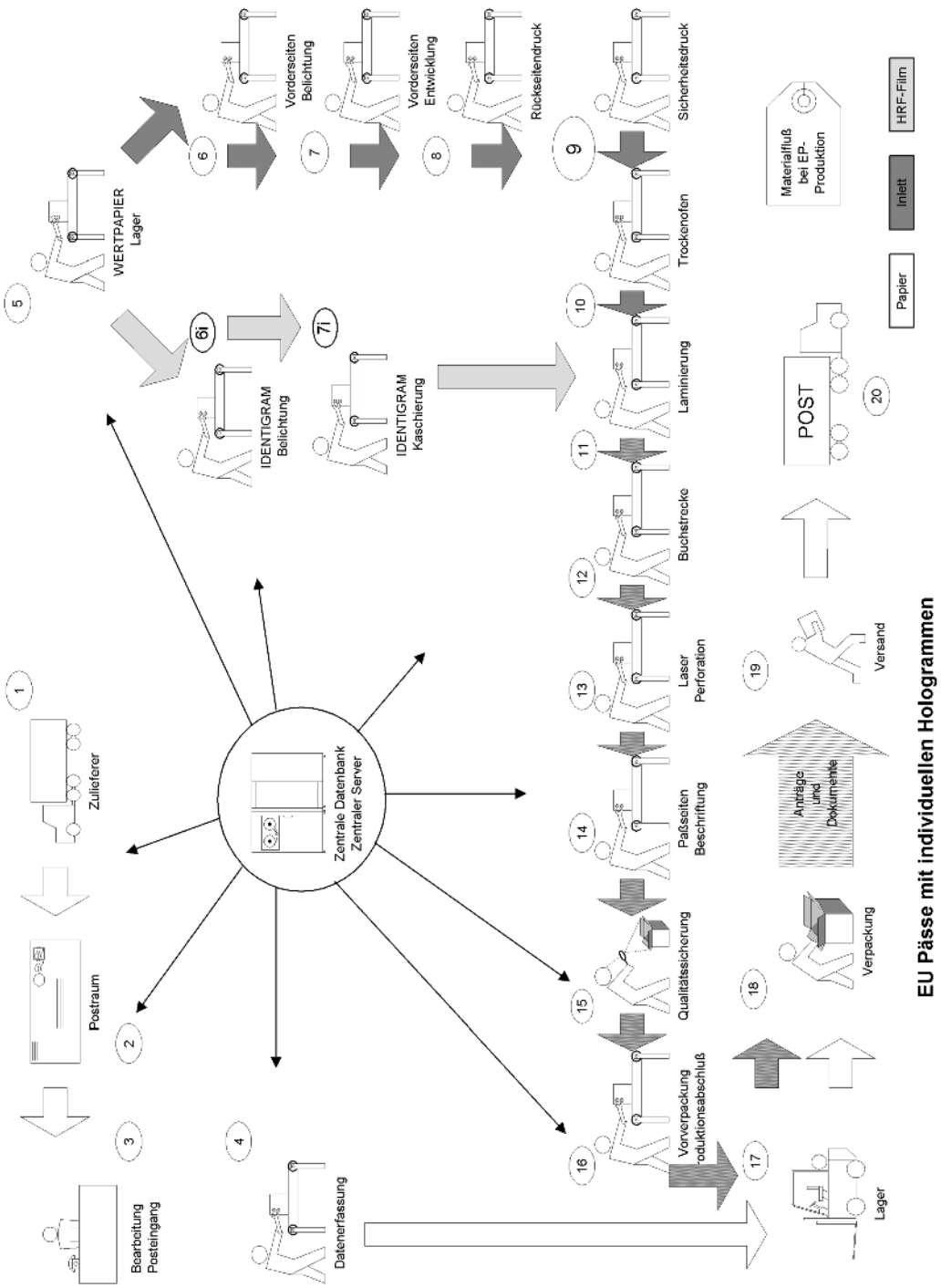
Ein Identigramm ist ein Sicherheitsmerkmal, durch das Teile der Pass- oder Ausweiskarte holographisch wiedergegeben werden. Durch die Einführung dieses Sicherheitsmerkmals soll die Fälschungssicherheit der Pass- sowie Ausweiskarte weiter erhöht werden. Neben Bewegungsstrukturen, die über dem herkömmlichen Lichtbild angebracht sind, enthält das Identigramm zudem eine maschinenlesbare Struktur (so genannter roter Punkt), die neben dem maschinellen Lesen der Ausweise zur Unterstützung der Sichtkontrolle auch eine maschinelle Echtheitsprüfung ermöglicht. Die Struktur beinhaltet weder personen- noch dokumentenbezogene Daten. Hervorzuheben ist, dass das Identigramm nicht kopiert werden kann. Bei der Kontrolle konnte ich mich davon überzeugen, dass die Fertigung (insbesondere die technische Ausgestaltung und der Ablauf des Verfahrens) datenschutzrechtlichen Anforderungen entspricht.

7.3 Novellierung des Melderechtsrahmengesetzes – kein datenschutzrechtlicher Fortschritt

Über meine Forderungen zur Novellierung des Melderechtsrahmengesetzes habe ich bereits in meinem 18. TB (Nr. 5.7) informiert. Nach Vorlage des Entwurfs eines Dritten Gesetzes zur Änderung des Melderechtsrahmengesetzes durch das BMI hat sich auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit den vorgesehenen Änderungen befasst und eine Entschließung (s. Anlage 10) verabschiedet. Darin wurden u. a. Bedenken zum geplanten Zusammenschluss mehrerer Melderegister, zur Möglichkeit einer einfachen Meldregisterauskunft über das Internet sowie zur Risikoabwägung bei einer Auskunftssperre erhoben, wenn eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange des Betroffenen glaubhaft gemacht wird. Weiterhin wurde die Abschaffung der Hotelmeldepflicht und bei Auskünften an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen anstelle der bisherigen Widerspruchslösung die Einwilligung des Betroffenen gefordert.

Abbildung 2 (zu Nr. 7.2)

Produktion von individuellen Hologrammen am Beispiel der Personalausweise



Obwohl als ein Ziel der Novellierung ausdrücklich die Verbesserung des Datenschutzes aufgeführt war, wurden die vorgenannten Datenschutzforderungen überwiegend nicht erfüllt. Lediglich der geplante Zusammenschluss mehrerer Melderegister wurde fallen gelassen und bei Melderegisterauskünften mithilfe des Internets die Mindestforderung der Datenschutzbeauftragten – nämlich die Widerspruchsmöglichkeit des Betroffenen – berücksichtigt. Selbst die vom BMI zunächst vorgesehene Abschaffung der Hotelmeldepflicht wurde nicht realisiert. Damit bleibt diese millionenfache Datenerhebung weiterhin unverändert bestehen, obgleich sie in der Vergangenheit nicht zu nachweisbarem Nutzen geführt hat.

Das Gesetz zur Änderung des Melderechtsrahmengesetzes und anderer Gesetze wurde vom Bundestag mit Zustimmung des Bundesrates beschlossen und am 3. April 2002 im Bundesgesetzblatt (BGBl I S. 1186) verkündet.

Ich bedauere, dass der datenschutzrechtliche Standard des Melderechtsrahmengesetzes nach wie vor wenig befriedigend ist. Gerade in diesem Bereich gibt es besonders viele Beschwerden der Bürger, die sich insbesondere gegen die Auskünfte an Parteien sowie gegen die einfache Melderegisterauskunft an jedermann richten, weil die Bürger hierdurch ihre informationelle Selbstbestimmung – nämlich grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Daten zu bestimmen – gefährdet sehen.

7.4 Datenschutzgesetz für die Suchdienste – eine endliche Geschichte?

Aufgrund meiner Hinweise auf fehlende Datenschutzregelungen hat die Bundesregierung bereits im Sommer 1998 ihre Bereitschaft erklärt, die Verarbeitung und Nutzung personenbezogener Daten durch den Suchdienst des Deutschen Roten Kreuzes und die kirchlichen Suchdienste sobald wie möglich gesetzlich zu regeln. In meinem 18. TB (Nr. 5.4) habe ich über einen ersten Entwurf eines Suchdienstedatenschutzgesetzes berichtet, der aber noch nicht mit den Ressorts und den betroffenen Organisationen abgestimmt war. Auch im Berichtszeitraum ist es dem BMI trotz zahlreicher Gespräche und Abstimmungen mit meinem Hause nicht gelungen, dem Parlament entsprechende gesetzliche Regelungen vorzulegen. Vielmehr ist der Gesetzentwurf wegen BMI-interner Abstimmungsschwierigkeiten noch nicht in die Ressortabstimmung gelangt. Das BMI hat mich Ende September 2002 darüber unterrichtet, dass das Gesetzesvorhaben nunmehr in dieser Legislaturperiode in Verbindung mit einem wichtigen Datenschutzprojekt verwirklicht werden soll. Ich werde über die Fortentwicklung berichten.

7.5 Dopingopfer-Hilfe – datenschutzfreundlich geregelt

Im Frühjahr 2002 ist mir vom BMI der Entwurf eines Gesetzes über eine finanzielle Hilfe für Dopingopfer der DDR (Dopingopfer-Hilfegesetz) zur kurzfristigen Stellungnahme zugeleitet worden. Darin ist vorgesehen, Hochleistungssportler und -nachwuchssportler, die im staatlichen Auftrag der ehemaligen DDR gedopt worden sind, aus humanitären und sozialen Gründen finanziell und moralisch zu unterstützen. Zu diesem Zweck soll ein Hilfefonds beim Bundesverwaltungsamt (BVA) eingerichtet werden. Ich habe bemängelt, dass der Entwurf nicht erkennbar macht, in welcher Form das BVA und der beim BMI einzurichtende Beirat die von den Anspruchsberechtigten übermittelten personenbezogenen Daten verarbeiten und nutzen soll. Da es sich bei diesen Daten um sehr sensible Daten handelt, habe ich dringend empfohlen, im Gesetz nähere Regelungen über die Verarbeitung und Nutzung dieser Daten zu treffen. Durch die Einfügung eines eigenen Paragrafen „Datenschutz“ in den Gesetzentwurf hat die Bundesregierung meiner Empfehlung entsprochen. Das Gesetz ist am 25. August 2002 in Kraft getreten (BGBl. I S. 3410).

7.6 Das Stasi-Unterlagen-Gesetz und die Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR

7.6.1 Der „Fall Kohl“ und die Folgen für das Stasi-Unterlagen-Gesetz

In dem von der interessierten Öffentlichkeit und den Medien mit großer Aufmerksamkeit verfolgten Rechtsstreit zwischen dem ehemaligen Bundeskanzler Dr. Helmut Kohl und der Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) hat das Bundesverwaltungsgericht am 8. März 2002 das erstinstanzliche Urteil des Verwaltungsgerichts Berlin bestätigt und entschieden, die BStU dürfe die umstrittenen Unterlagen mit personenbezogenen Informationen über den Kläger nicht für die Forschung, die politische Bildung oder die Verwendung durch die Medien zur Verfügung stellen (BVerwGE 116, 104). Dieses Urteil des Bundesverwaltungsgerichtes ist nach meiner Auffassung – wie schon das Urteil des Verwaltungsgerichts Berlin – überzeugend. Es stellt unmissverständlich klar, dass auch Personen der Zeitgeschichte – sofern sie nicht Mitarbeiter oder Begünstigte der Staatssicherheit waren – eine Herausgabe von Unterlagen mit ihren personenbezogenen Daten nicht hinnehmen müssen, wenn sie insbesondere durch die Art der Beschaffung dieser Unterlagen selbst zu Opfern des DDR-Regimes geworden sind. Angesichts dieses Urteils sah sich die BStU gehindert, ihren Aufgaben hinsichtlich der historischen, politischen und juristischen Aufarbeitung der Tätigkeit des Staatssicherheitsdienstes in dem bisherigen Umfang nachzukommen, soweit dadurch Personen der Zeitgeschichte, Inhaber politischer Funktionen oder Amtsträger betroffen waren. Die Koalitionsfraktionen von SPD und BÜNDNIS 90/DIE GRÜNEN haben deshalb noch im Juni 2002, kurz vor Ende der Legislaturperiode, den Entwurf eines Fünften Gesetzes zur Änderung des Stasi-Unterlagen-Gesetzes (Bundestagsdrucksache 14/9219) eingebracht. Dieser Entwurf beinhaltete folgende Änderungsvorschläge:

– § 32 des Stasi-Unterlagen-Gesetzes (StUG) sollte weitgehend neu gefasst werden, um personenbezogene Informationen über Personen der Zeitgeschichte, Inhaber politischer Funktionen oder Amtsträger für die historische und politische Aufarbeitung der Tätigkeit des Staatssicherheitsdienstes zugänglich zu machen, soweit deren zeitgeschichtliche Rolle bzw. das funktions- oder amtsbezogene Wirken dieser Personen betroffen sind. Das bisherige Verbot der Herausgabe, falls diese Personen zugleich Opfer der Staatssicherheit gewesen sind, sollte aufgehoben und durch eine Abwägungsklausel ersetzt werden.

– Ein neuer § 32a sollte in das StUG eingeführt werden, der die Benachrichtigung des Betroffenen und die Möglichkeit, Einwendungen zu erheben, regelt.

– § 14 StUG und damit der Anspruch von Betroffenen oder Dritten auf Anonymisierung bzw. Löschung von personenbezogenen Informationen sollte gestrichen werden.

Ich habe mich in schriftlichen Stellungnahmen, zwei Anhörungen vor dem Innenausschuss des Deutschen Bundestages und in einer weiteren Anhörung der CDU/CSU-Bundestagsfraktion allgemein zu dem Regelungsbedarf sowie dem konkreten Gesetzentwurf geäußert. Dabei habe ich insbesondere betont, dass ausweislich der in § 1 des Gesetzes aufgelisteten Ziele das StUG in erster Linie ein Opferschutzgesetz ist. In § 5 des Gesetzes ist zudem bestimmt, dass die Verwendung personenbezogener Informationen zum Nachteil der Opfer unzulässig ist. Eine Herausgabe von Informationen gegen den Willen des Betroffenen, insbesondere wenn diese unter Verletzung des Brief-, Post- und Fernmeldegeheimnisses oder unter Verstoß gegen die Unverletzlichkeit der Wohnung gewonnen wurden, sei damit nicht zu vereinbaren. Damit ergäbe sich praktisch kein Spielraum für eine Interessenabwägung zu Ungunsten des Opfers. Die neue Regelung des § 32a über die Unterrichtung des Betroffenen habe ich grundsätzlich begrüßt und darauf hingewiesen, dass Ausnahmen von der Benachrichtigungspflicht nur in sehr eng begrenzten Fällen und auch nur dann in Betracht kommen könnten, wenn Nachteile für die betroffene Person auszuschließen seien. Allerdings habe ich auch zu § 32a des Entwurfs bemängelt, dass die betroffene Person letztlich eine Herausgabe der sie betreffenden Informationen nicht verhindern kann und ihre Einwände lediglich von der BStU im Rahmen einer Interessenabwägung berücksichtigt werden. Zur Streichung des § 14 StUG habe ich darauf hingewiesen, dass nach Absatz 2 dieser Vorschrift eine Anonymisierung auf Antrag der Opfer ohnehin in den Fällen unterbleibt, die in der Begründung des Gesetzentwurfs als Argumente für eine Streichung angeführt wurden (Interessen anderer Personen oder Stellen am Fortbestand der Informationen). Außerdem habe ich eine konkrete Gesetzesformulierung vorgelegt, die in meinen Augen den Rechten der Opfer in angemessener Weise Rechnung getragen und ausgeschlossen hätte, dass sie durch eine Herausgabe gegen ihren Willen ein zweites Mal zu Opfern würden.

Leider ist der Innenausschuss des Deutschen Bundestages meinen Vorschlägen nicht gefolgt und hat beschlossen, den Koalitionsentwurf unverändert dem Bundestagsplenum zur Beschlussfassung vorzulegen.

Erst buchstäblich in letzter Minute wurde zwischen den Koalitionsfraktionen und der FDP-Bundestagsfraktion ein Kompromiss vereinbart, der durch einen gemeinsamen Änderungsantrag für die zweite Lesung des Gesetzentwurfs eingebracht wurde. Dieser Kompromiss, an dem ich ebenfalls mitgewirkt habe, sah vor, in die neu gefasste Abwägungsklausel des § 32 eine Bestimmung aufzunehmen, nach der bei der Abwägung insbesondere zu berücksichtigen sei, „ob die Informationserhebung erkennbar auf einer Menschenrechtsverletzung“ beruhe. In dieser Fassung ist das Gesetz vom Deutschen Bundestag schließlich beschlossen worden. Der Bundesrat hat darauf verzichtet, den Vermittlungsausschuss anzurufen, sodass das Fünfte Gesetz zur Änderung des Stasi-Unterlagen-Gesetzes bereits am 6. September 2002 in Kraft treten konnte (BGBl. I S. 3446).

Ich halte die Änderungen des StUG insgesamt für vertretbar. Die Rechte des Opfers sind durch den im parlamentarischen Verfahren ergänzten Satz gestärkt worden, auch wenn es letztlich bei der Abwägungsklausel verblieben ist. Ich kann mir indessen kaum vorstellen, dass die BStU Unterlagen mit personenbezogenen Informationen gegen den Willen eines früheren Stasi-Opfers herausgibt, die durch Verletzung des Brief-, Post- und Fernmeldegeheimnisses, unter Verstoß gegen die Unverletzlichkeit der Wohnung oder durch eine sonstige Menschenrechtsverletzung gewonnen wurden.

Ob die neue Regelung eine dauerhafte Grundlage für die weitere Arbeit der BStU darstellt, wird entscheidend auch von ihrer praktischen Handhabung abhängen. Diesbezüglich weiß ich aus eigener Anschauung durch zahlreiche Beratungs- und Kontrollbesuche, wie sorgfältig und gewissenhaft in dieser Behörde der Umgang mit besonders heiklen personenbezogenen Daten gepflegt wird.

7.6.2 Weitere Besuche bei der Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR und ihren Außenstellen

Im Berichtszeitraum habe ich sowohl die Zentrale in Berlin als auch zwei Außenstellen der BStU beraten und kontrolliert. Schwerpunkt bei meinen Besuchen in der Zentrale war dabei das Verfahren der BStU im Umgang mit Stasi-Abhörprotokollen. Dabei habe ich Unterlagen von mir ausgewählter Personen der Zeitgeschichte eingesehen, bei denen auf Antrag von Forschern und Medien Stasi-Unterlagen von der BStU herausgegeben wurden. Ich habe dabei den Eindruck gewonnen, dass in der Vergangenheit Stasi-Abhörprotokolle in der Praxis der BStU fast keine Rolle gespielt haben. Allerdings wurden in mehreren Fällen Stasi-Abhörprotokolle in Form von zusammenfassenden Vermerken herausgegeben, was nach meiner Rechtsauffassung nicht zulässig ist. Von einer formalen Beanstandung habe ich wegen des damals laufenden Rechtsstreits mit dem früheren Bundeskanzler Dr. Kohl und der dann erfolgten Änderung des Stasi-Unterlagen-Gesetzes abgesehen.

Bei meinen Besuchen in den Außenstellen der BStU habe ich erneut einen sorgfältigen und gewissenhaften Umgang mit den äußerst sensiblen Unterlagen festgestellt. Der Schwerpunkt meiner Kontrollen war dabei wieder das Verfahren der BStU bei Anträgen auf Auskunft und Einsicht in die Unterlagen des ehemaligen Staatssicherheitsdienstes sowie die automatisierte Datenverarbeitung. Soweit von mir Mängel festgestellt wurden, sind diese umgehend behoben worden.

Für das im letzten Tätigkeitsbericht angesprochene Problem bei der Behandlung von Besuchern bei der BStU wurde folgende Lösung gefunden: Besucher brauchen ihren Personalausweis für die Dauer des Besuches nicht mehr zu hinterlegen. Allerdings besteht die BStU aus Gründen der Sicherheit und des Nachweises weiterhin darauf, dass die Besucher einen – abgespeckten – Besucherschein ausfüllen. Sie hat sich ferner bereit erklärt, die Besucherscheine nach drei Monaten zu vernichten. Die Dauer der Aufbewahrung habe ich nochmals hinterfragt.

Bei meinen Besuchen habe ich auch die Gebäudeüberwachung durch Videokameras überprüft und auf die geänderte Rechtslage nach Einführung des neuen § 6b BDSG im Jahre 2001 hingewiesen (vgl. hierzu auch Nrn. 3.2.2 und 4.1). Auch hier ist die BStU meinen Anregungen gefolgt und hat öffentlich zugängliche Räume mit Hinweisbeschilderung auf

eine Videoüberwachung versehen und sich verpflichtet, Videoaufzeichnungen nach spätestens 24 Stunden zu löschen, wenn sie nicht zur Klärung eines Vorfalls benötigt werden.

7.7 Staatsangehörigkeitsdatei – immer noch keine Rechtsgrundlage

In meinem 16. TB (Nr. 5.7) hatte ich ausführlich über die beim Bundesverwaltungsamt geführte Staatsangehörigkeitsdatei berichtet und in den folgenden 17. TB (Nr. 5.14) und 18. TB (Nr. 5.9) jeweils die hierfür erforderliche Rechtsgrundlage angemahnt. Leider ist auch in dem abgelaufenen Berichtszeitraum noch keine gesetzliche Regelung getroffen worden, weil bei der Neustrukturierung der Staatsangehörigkeitsdatei der Abstimmungsprozess mit den Ländern noch nicht abgeschlossen werden konnte. Hierfür wurde bei dem federführend zuständigen BMI eine Arbeitsgruppe eingerichtet, um alle Staatsangehörigkeits- und Einbürgerungsfragen zu klären. An dieser Arbeitsgruppe bin auch ich beteiligt. Aufgrund der dort bis jetzt erzielten Ergebnisse gehe ich davon aus, dass ich im nächsten Tätigkeitsbericht endlich über einen positiven Abschluss dieses datenschutzrechtlichen Problems berichten kann.

7.8 Wahlen

7.8.1 Bundeswahlgesetz – jetzt endlich datenschutzfreundlicher

Durch das Fünfzehnte Gesetz zur Änderung des Bundeswahlgesetzes, das am 4. Mai 2001 verkündet wurde (BGBl. I S. 698) und inzwischen in Kraft getreten ist, hat sich endlich meine langjährige Forderung erfüllt, die öffentliche Auslegung des Wählerverzeichnisses abzuschaffen (zuletzt 18. TB Nr. 5.10.2). Die Auslegung wurde durch das Recht zur Einsichtnahme in das Wählerverzeichnis ersetzt. Falls die Daten anderer Wahlberechtigter eingesehen werden sollen, müssen Tatsachen glaubhaft gemacht werden, aus denen sich eine Unrichtigkeit oder Unvollständigkeit des Wählerverzeichnisses ergeben könnte. Daten von Wahlberechtigten, für die im Melderegister ein so genannter Sperrvermerk eingetragen ist, dürfen nicht eingesehen werden.

Um die Gewinnung von Wahlhelfern zu erleichtern, dürfen ferner die Gemeindebehörden personenbezogene Daten von Wahlberechtigten auch für künftige Wahlen verarbeiten. Der Betroffene kann der Verarbeitung widersprechen und ist über sein Widerspruchsrecht zu unterrichten. Um die Berufung von Wahlhelfern zu erleichtern, können sich die Gemeindebehörden außerdem an Behörden und sonstige juristische Personen des öffentlichen Rechts wenden, die dann verpflichtet sind, aus dem Kreis ihrer Mitarbeiter diejenigen zu benennen, die im Gebiet der ersuchenden Gemeinde wohnen. Die ersuchte Stelle hat den Betroffenen entsprechend zu unterrichten.

7.8.2 Sind Online-Wahlen technisch möglich und erstrebenswert?

Die Bundesregierung prüft seit längerem, inwieweit politische Wahlen elektronisch unterstützt werden können. Hierzu wurde im BMI eine Arbeitsgruppe „Online-Wahlen“ eingerichtet, die im Dialog zwischen Informatikern, Juristen und Wahlorganisatoren die entsprechenden technischen, rechtlichen und organisatorischen Anforderungen erarbeitet und an der ich beteiligt bin. Es wird angestrebt, bis zur Bundestagswahl 2006 die Wahllokale so zu vernetzen, dass die Wahlberechtigten nicht mehr nur in dem Wahlbezirk, in dem sie wohnen, sondern in jedem beliebigen Wahllokal wählen können. Damit soll der zunehmenden Mobilität der Wahlberechtigten aufgrund beruflicher Anforderungen oder persönlicher Wünsche Rechnung getragen werden. Als Fernziel wird die Stimmabgabe vom heimischen PC aus oder per Handy anvisiert.

Für die Stimmabgabe auf elektronischem Wege stellen die rechtlichen Anforderungen des Artikels 38 GG zum Teil hohe Hürden dar, die nicht leicht zu bewältigen sind:

- Die geheime Wahl erfordert eine technische Gestaltung des Wahlvorganges, die es unmöglich macht, die Wahlentscheidung eines Wählers zu erkennen oder zu rekonstruieren. Das bedeutet, dass das Wahlverhalten auch nach der Stimmabgabe dauerhaft geheim bleiben muss. Dies ist bei den heute eingesetzten Verschlüsselungsverfahren nicht zu gewährleisten, da eine zeitlich uneingeschränkte Sicherheitsaussage kaum möglich ist. Völlig ungelöst ist darüber hinaus bei einer Stimmabgabe vom heimischen PC aus oder per Handy die Sicherstellung der unbeobachteten Wahlentscheidung.
- Die freie Wahl meint die Ausübung des aktiven Wahlrechts ohne physischen Zwang oder psychischen Druck. Dies ist u. a. nur dann gewährleistet, wenn die eigentliche Wahlentscheidung ohne direkte Beeinflussung durchgeführt wird.
- Die Gleichheit der Wahl garantiert, dass die Stimme jedes Wählers den gleichen Zählwert hat. Es muss also insbesondere sichergestellt werden, dass Mehrfachabgaben desselben Wählers sicher erkannt und ausgeschlossen werden können.

Außerdem sind folgende Anforderungen technisch zu gewährleisten (vgl. hierzu Nr. 11.1.2):

- Die zur Stimmabgabe gewählte Technik muss am Tag der Wahl absolut sicher verfügbar und funktionsfähig sein.
- Sowohl das Wählervotum als auch die ermittelten Wahlergebnisse müssen bei der Übertragung und bei der anschließenden Speicherung sicher gegenüber Manipulationen sein.
- Derzeit wird der Kreis der Wahlberechtigten über Wählerverzeichnisse festgelegt. Auch bei der Durchführung der Online-Wahl muss es möglich sein zu überprüfen, ob derjenige, der ein Votum abgeben will, auch wahlberechtigt ist.

Eine Wahl über das Internet ist mit der heute verfügbaren Technik und Software kaum vorstellbar. Selbst wenn die technischen Probleme gelöst werden könnten, müssten zuvor Akzeptanz und Vertrauen der Wähler in eine solche Wahl reifen. Schließlich stellt sich noch die Frage, ob eine Online-Wahl vom heimischen PC aus oder per Handy überhaupt in unsere Wahlkultur passt. Es ist fraglich, ob eine derart beiläufige Stimmabgabe der politischen Bedeutung der Wahlhandlung als maßgeblichem demokratischen Element gerecht wird.

7.9 Volkszählungstest – Ist die Bürgerbefragung zukünftig überflüssig?

Auf der Grundlage des Gesetzes zur Vorbereitung eines registergestützten Zensus vom 27. Juli 2001 (BGBl. I S. 1882) wird im Augenblick getestet, ob die Dateien der Verwaltung geeignet sind, bei zukünftigen Volkszählungen die Befragungen der Bürger zu ersetzen.

Ich habe den Über gang zu dieser neuen Methode als T est befürwortet, damit aber zugleich die Beachtung datenschutzrechtlicher Erfordernisse verknüpft (vgl. im Einzelnen meinen 18. TB Nr. 30.1). Meinen Empfehlungen wurde in vollem Umfang entsprochen.

Die Testerhebungen und Auswertungen sind im Gange: Am 5. Dezember 2001 startete der Testlauf mit der Befragung der Bewohner der Auswahlgebäude. Die Testdaten der Melderegister wurden im Januar und Mai 2002 angefordert. Daran schloss sich die Überprüfung der Mehrfachfälle (z. B. wegen mehrerer oder unklarer Registereintragungen) an, die im November 2002 abgeschlossen wurde. V on den insgesamt 971 037 Personendatensätzen wurden 57 015 nicht eindeutig identifiziert, von denen blieben wiederum durch mehrfache statistische Überarbeitung nur noch 9 159 Befragungsfälle (knapp 1 %) übrig, die durch schriftliche und telefonische Rückfragen oder durch Erhebungsbeauftragte geklärt wurden. Die anderen Primärerhebungen, d. h. die direkt beim Bür ger durchgeführten Befragungen zur Gebäude- und W ohnungsstichprobe wurden ebenfalls im Herbst 2002 beendet. Bis Ende 2002 liefen die Register - und Verfahrenstests mit den Angaben der Bundesanstalt für Arbeit. Mit dem Kernstück der T estläufe – der Haushaltgenerierung (das ist die statistische Zuordnung von Personen zu Haushalten) – wurde noch in 2002 begonnen. Die statistisch errechneten Haushalte werden im Anschluss daran mit den Angaben aus der Haushaltsstichprobe ver glichen, um die Qualität der statistischen Programme zu überprüfen.

In der Vergangenheit wurden immer wieder Bedenken gegen den Testlauf vorgebracht, weil neben den der statistischen Auswertung dienenden Erhebungsmerkmalen viele Hilfsmerkmale erfasst wurden. Diese Bedenken greifen allerdings nicht, weil die größere Zahl an Hilfsmerkmalen benötigt wird, um Personenangaben aus verschiedenen Beständen zusammenzufassen und personenüber greifende Zusammenhänge, wie den Haushalt, zu ermitteln. Sie sind also – wie die Bezeichnung schon sagt – „technische“ Hilfsgrößen, die zum frühestmöglichen Zeitpunkt wieder gelöscht werden. Unproblematisch ist auch, dass für den Testlauf mehr Hilfsmerkmale als letztlich benötigt herangezogen wurden, weil nur so feststellbar sein wird, welche Angaben sich als „stabil“ erweisen und auf welche Merkmale künftig verzichtet werden kann.

Unabhängig hiervon wurde problematisiert, warum identifizierende Daten nicht gleich zu Anfang verschlüsselt werden. Das Problem ist, da ss Daten von verschiedenen Personen bzw. von einer Person aus verschiedenen Melderegistern im Rahmen der Me hrfachfallprüfung, der Haushaltgenerierung und der Erwe rbstätigenberechnung zusammengeführt werden müssen. Eine V erschlüsselung würde voraussetzen, dass die Angabe n in den Registern immer gleich geschrieben werden, um zu gleichen verknüpfbaren Pseudonymen zu kommen. Diese Bedingung ist jedoch häufig nicht erfüllt, wie aus unter schiedlichen Namensschreibweisen und Buchstabendarstellungen (z. B. „ß“) bekannt ist. Im unverschlüsselten Zustand können solche Mängel mithilfe statistischer V erfahren ausgeglichen werden. Außerdem muss bei der Klärung von Zweifelsfällen eine Rückcodierung in Namen etc. möglich sein. Die V erschlüsselung müsste daher nach einem festen System erfolgen, damit gleicher Name zu gleicher alphanumerischer V erknüpfung führt. Eine solche V erfremdung wäre jedoch leicht zu entschlüsseln; sie brächte keinen verbesserten Datenschutz, zumal das gesamte Auswertungsverfahren im abgeschotteten Bereich der amtlichen Statistik läuft.

Kritisch hinterfragt wurde auch die bestehende Auskunftspflicht für die Befragten. Da die mit der Volkszählung verfolgten Zwecke wie Festlegung der genauen Einwohnerzahlen für Bund, Länder und Gemeinden exakte Daten voraussetzen, um Auswahlgrundlage sowie Hochrechnungsrahmen für weitere Stichprobenerhebungen zu sein, kann nach Feststellung des W issenschaftlichen Beirats bei den Untersuchungen auf die Auskunftspflicht nicht verzichtet werden. Erhebungen auf freiwilliger Basis würden wegen erwiesenermaßen zu geringer T eilnahmequote von 50 bis 60 % zu große Unsicherheitsfaktoren beinhalten. In der amtlichen Statistik ist kein Land bekannt, das eine V olkszählung auf freiwilliger Basis durchführt. Zwischen 1985 und 1994 erfolgten weltweit 241 Volks- und Wohnungszählungen, mit denen 95 % der geschätzten W eltbevölkerung erfasst wurden. Die Zensen fanden in Form von reinen Primärerhebungen (in Frankreich, Griechenland, Schweiz, Japan), reinen Registerauswertungen (in Dänemark, Finnland) oder Kombinationen aus beiden (in Schweden, Belgien), als Vollerhebung mit ergänzender Stichprobe (in den USA, Kanada, Polen) oder als Registerauswertung mit Stichprobe (in den Niederlanden) statt.

Ich habe bisher nur wenige Eingaben zum V olkszählungstest erhalten. Dabei handelt es sich im W esentlichen um Probleme bei der Stichprobenbefragung oder der Mehrfachfallprüfung. Sicherlich wendet sich nicht jeder Bür ger gleich an den Bundesbeauftragten, wenn er sich in seinen schutzwürdigen Belangen verletzt fühlt. Dennoch halte ich die geringe Zahl von Beschwerden für ein Symptom des grundsätzlich vorherrschenden Vertrauens in das neue Testverfahren. Dazu hat sicherlich die kontinuierliche Beteiligung der Datenschutzbeauftragten beigetragen. Ich beobachte und begleite auch die weiteren V erfahrensschritte, wenngleich sich erst nach Abschluss der T estphase die Ergebnisse unter Berücksichtigung der Erfahrungsberichte der Statistischen Ämter einer da tenschutzrechtlichen Gesamtwürdigung unterziehen lassen.

7.10 Wiedergutmachung für NS-Opfer

Im Berichtszeitraum war der BfD mit der datenschutzrechtlichen Begleitung verschiedener Projekte und Verfahren zur Wiedergutmachung für NS-Opfer befasst. Dies betraf zum einen die Stiftung „Erinnerung, V erantwortung und Zukunft“, für die das „Gesetz zur Errichtung einer Stiftung Erinnerung, Verantwortung und Zukunft“ vom 2. August 2000 (BGBl. I S. 1263 f f.) die Grundlage schuf. Zum anderen ging es um ein Projekt zur Nachweisbeschaf fung für NS-Zwangsarbeiter, das ehemalige Zwangsarbeiter bei der Recherche von Nachweisen für eine Entschädigungsberechtigung unterstützt. Auch im Bereich der Entschädigung von Holocaust-Opfern durch die Versicherungswirtschaft waren datenschutzrechtliche Fragen zu klären und zu lösen.

7.10.1 Die Stiftung „Erinnerung, Verantwortung und Zukunft“

Mit Gesetz vom 2. August 2000 wurde die Stiftung „Erinnerung, Verantwortung und Zukunft“ als rechtsfähige Stiftung des öffentlichen Rechtes errichtet.

Zweck der Stiftung ist es, über Partnerorganisationen Finanzmittel zur Gewährung von Leistungen an ehemalige Zwangsarbeiter und von anderem Unrecht aus der Zeit des Nationalsozialismus Betroffene bereitzustellen.

Aus der Tätigkeit der Stiftung ergaben sich eine Reihe datenschutzrechtlicher Fragen, bei denen ich beratend tätig wurde. Insbesondere ging es dabei um die Datenübermittlung durch Unternehmen, die bereits Entschädigungsleistungen an ehemalige Zwangsarbeiter geleistet hatten, sowie den Datenabgleich mit dem österreichischen Versöhnungsfonds sowie den Datenbeständen ausländischer Partneror ganisationen. Im Vordergrund stand dabei stets das Bemühen, mit Blick auf das vielfach sehr hohe Alter der Antragsteller die Auszahlung der Entschädigungsleistungen nicht zu verzögern und dabei gleichzeitig den Schutz des Persönlichkeitsrechts der Antragsteller zu wahren. Aufgrund der gesetzlichen Anrechungsvorschriften im Stiftungsgesetz und der von den Antragstellern in den Antragsformularen erteilten Einverständniserklärungen konnten die für den Nachweis der Leistungsberechtigung erforderlichen Datenabgleiche stattfinden.

Für die Stiftung wurde ein Datenschutzbeauftragter bestellt. Anlässlich einer ausführlichen datenschutzrechtlichen Beratung vor Ort konnte festgestellt werden, dass die technisch-organisatorischen Maßnahmen zur Datensicherheit der Verarbeitung bei der Stiftung angemessen sind. Soweit ein Datenabgleich über das Internet stattfindet, wird dieser über eine sichere Verschlüsselung geschützt.

7.10.2 Projekt zur Nachweisbeschaffung für ehemalige NS-Zwangsarbeiter

Im Rahmen der V erfahren zur W iedergutmachung für NS-Opfer ergab sich für viele antragstellende ehemalige NS-Zwangsarbeiter das Problem, den in § 1 1 Abs. 2 Stiftungsgesetz vorgesehenen Nachweis über die Leistungsberechtigung durch Unterlagen zu erbringen. Der Internationale Suchdienst in Bad Arolsen kann in nur etwa einem knappen Drittel der Fälle den erforderlichen Nachweis führen. Hier setzt das Projekt „Nachweisbeschaf fung für ehemalige NS-Zwangsarbeiter/-innen“ an. Es handelt sich um ein Gemeinschaftsprojekt des Bundesarchivs, des Bundesverbandes Information & Beratung für NS-V erfolgte sowie des Internationalen Suchdienstes, das von der Stiftung „Erinnerung, Verantwortung und Zukunft“ finanziert wird. Auf der Rechtsgrundlage des Stiftungsgesetzes und der Einverständniserklärungen der Antragsteller hilft das Projekt den Antragstellern, deren eigene Recherchebemühungen auch über den Internationalen Suchdienst vorher erfolglos verlaufen sind. An der Recherche durch das Projekt sind 240 staatliche und nicht staatliche Archive beteiligt. Ich habe das Projekt auch in einem Termin vor Ort beraten. Alle Mitarbeiter, die aus dem nicht öf fentlichen Bereich kommen, wurden verschwiegenheitsverpflichtet. Die Prüfung zur Datensicherheit des V erfahrens ergab, dass die getrof fenen Maßnahmen ausreichend und angemessen waren. Insbesondere wird der Datenverkehr über das Internet mit einer 128-Bit-Verschlüsselung geschützt. Inzwischen wurden bereits über 218 000 Anfragen an das Projekt gerichtet. Bei den erledigten Recherchen konnte einem V iertel der Antragsteller, deren Bemühungen zuvor erfolglos geblieben waren, mit einem positiven Ergebnis geholfen werden.

7.10.3 Entschädigung von Holocaust-Opfern durch die Versicherungswirtschaft

Ende der Neunzigerjahre beschlossen verschiedene amerikanische Bundesstaaten Gesetze, so genannte Holocaust Victims Insurance Acts, mit denen bislang nicht durchgeführte Entschädigungsverfahren für V ersicherungspolicen von Holocaust-Opfern vorangetr ieben werden sollten. Nach diesen Gesetzen sollten V ersicherungsunternehmen verpflichtet werden, alle Daten von V ersicherungspolicen aus den Jahren von 1920 bis 1945 in die USA zu übermitteln, damit über einen Abgleich der Daten mit den Listen jüdischer Opferverbände und auch der Opferliste in Y ad Vashem die noch zu entschädigenden Personen ermittelt werden könnten. Soweit Versicherungsunternehmen diese Gesetze nicht beachteten, wurde ein V erlust der Lizenz in dem jeweiligen Bundesstaat angedroht. Nach fast einhelliger Auffassung der Datenschutzaufsichtsbehörden wäre die geforderte Übermittlung sämtlicher Daten aus den V ersicherungspolicen in die USA datenschutzrechtlich unzulässig gewesen. Als eine Lösungsmöglichkeit wurde von den Datenschutzaufsichtsbehörden aufgezeigt, eine neutrale Stelle mit der Erstellung einer Opferliste zu befassen. Im März 2002 erklärte sich das Bundesaufsichtsamt für das V ersicherungswesen in seiner Zuständigkeit als Rechtsaufsicht über die V ersicherungsunternehmen bereit, eine Gesamtliste aus den Daten der verschiedenen betroffenen Versicherungsunternehmen zu erstellen. Nach derzeitigem Stand der V erhandlungen zwischen der Bundesstiftung „Erinnerung, Verantwortung und Zukunft“ und der „International Commission on Holocaust Era Insurance Claims (ICHEIC)“ zeichnet sich ab, dass der Datenabgleich mit der Antragsdatenbank der ICHEIC in Deutschland durch die Bundesanstalt für Finanzdienstleistungsaufsicht als Nachfolgerin u. a. des ehemaligen Bundesaufsichtsamtes für das Versicherungswesen stattfinden soll, wogegen keine datenschutzrechtlichen Bedenken mehr bestehen. Das weitere Verfahren stünde damit unter meiner Aufsicht.

8 Rechtswesen

8.1 Regelungsbedarf im Strafrecht – Heimliche Bildaufnahmen und DNA-Analysen dürfen nicht länger straffrei bleiben

Mit dem Instrumentarium des geltenden Rechts kann strafwürdigen Verhaltensweisen, die durch die rasante Entwicklung des technischen Fortschr itts möglich geworden sind, nicht oder nicht mehr angemessen begegnet werden. Es sind hier Strafbarkeitslücken entstanden, die möglichst bald zu schließen sind. Dies betrif ft vor allem das unbefugte Aufnehmen und V erbreiten von Bildern insbesondere mithilfe der Videotechnik und des Inte rnets sowie die unbefugte Durchführung von Gentests, die durch die Medizintechnik entwickelt wurden.

– Unbefugtes Aufnehmen und Verbreiten von Bildern

  Bereits in meinem 18. TB (Nr . 6.13) habe ich angemahnt, dass dringend Regelungen im Strafgesetzbuch geschaffen werden müssen, die das unbefugte Aufneh-

men und Verbreiten von Bildern anderer Personen unter Strafe stellen. Die geltenden Regelungen (§§ 22 f. des Kunsturhebergesetzes) sind nicht umfassend genug und entsprechen auch nicht dem heutigen Stand der Technik. So betreffen die Vorschriften ausschließlich nicht bewegte Bilder, Filme sind also nicht erfasst. Weiterhin ist nur die unbefugte Verbreitung von Bildnissen, nicht jedoch schon deren Aufnahme, unter Strafe gestellt. Im Zeitalter des Internets und der Webkameras ist es möglich, Bilder von Menschen unbemerkt aufzunehmen und weltweit zu verbreiten, die unter Umständen tief in die Intimsphäre des Einzelnen eingreifen (etwa heimliche Aufnahmen in Umkleidekabinen, Sonnenstudios etc.). Solche Verhaltensweisen können nicht länger straflos hingenommen werden. Ein in der letzten Legislaturperiode hierzu eingebrachter Gesetzentwurf fand leider keine parlamentarische Mehrheit. Ich appelliere daher nochmals dringend an den Gesetzgeber, entsprechende Regelungen in das Strafgesetzbuch aufzunehmen.

– Durchführung unbefugter DNA-Analysen

  Bereits mehrfach habe ich auf das Problem der Durchführung unbefugter DNA-Analysen aufmerksam gemacht (siehe z. B. 18. TB Nr. 25.2). Obwohl ein unbefugt durchgeführter Gentest und die unbefugte Verarbeitung oder Nutzung der aus einem Gentest gewonnenen Ergebnisse tief in die Persönlichkeitsrechte der Betroffenen eingreifen, existiert noch kein strafbewehrtes Verbot. Die Datenschutzbeauftragten des Bundes und der Länder haben anlässlich ihrer 62. Konferenz im Oktober 2001 bereits konkrete Formulierungsvorschläge zur Fassung von entsprechenden Strafvorschriften gemacht (s. Anlage 19; vgl. auch Nr. 28.5). Der Gesetzgeber sollte auch hier möglichst bald tätig werden.

8.2 Änderungen der Strafprozessordnung

8.2.1 Neue Rechtsgrundlage für Auskunft über Verbindungsdaten (§§ 100g, h Strafprozessordnung)

Mit Gesetz vom 20. Dezember 2001 (BGBl. I S. 3879) sind die §§ 100g und 100h in die Strafprozessordnung (StPO) eingefügt wurden. Die Regelungen traten am 1. Januar 2002 in Kraft und stellen nunmehr die Rechtsgrundlage für Auskunftsverlangen der Strafverfolgungsbehörden an die Anbieter von Telekommunikationsdiensten hinsichtlich der Verbindungsdaten dar („wer hat wann mit wem wie lange kommuniziert"). Damit wurde endlich eine Nachfolgeregelung für § 12 des Fernmeldeanlagengesetzes geschaffen. Eine gesetzliche Neuregelung hatte ich wegen der verfassungsrechtlichen Bedenken gegen diese Vorschrift, wie sie etwa in der Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 zum Ausdruck gebracht worden sind (s. Anlage 14 zum 18. TB), in der Vergangenheit bereits mehrfach angemahnt, zuletzt in meinem 18. TB (Nr. 6.4.1).

Zahlreiche der von mir geforderten datenschutzrechtlichen Verbesserungen wurden bei der Neuregelung erfreulicherweise berücksichtigt. Hervorzuheben ist hier in erster Linie, dass jetzt nicht mehr jede Straftat ein Auskunftsverlangen der Strafverfolgungsbehörden rechtfertigt, sondern nur noch eine solche von „erheblicher Bedeutung" oder eine solche, die mittels einer Endeinrichtung im Sinne des § 3 Nr. 3 des Telekommunikationsgesetzes begangen wurde. Weiterhin fällt positiv ins Gewicht, dass bezüglich der Anordnung der Maßnahme im Wesentlichen die formalen Kriterien einzuhalten sind, die auch für eine Anordnung der Überwachung und Aufzeichnung von Inhaltsdaten gem. § 100b StPO gelten. So darf regelmäßig nur der Richter eine Maßnahme nach § 100g StPO anordnen. Lediglich bei Gefahr im Verzug ist hierzu auch die Staatsanwaltschaft befugt, wobei deren Anordnung außer Kraft tritt, wenn sie nicht binnen drei Tagen von dem Richter bestätigt wird (§ 100h Abs. 1 S. 3 i. V. m. § 100b Abs. 1 StPO). Auch sind Art, Umfang und Dauer der Maßnahme in der schriftlichen Anordnung zu bestimmen (§ 100h Abs. 1 S. 3 i.V.m. § 100b Abs. 2 S. 1 und 3 StPO). Richtet sich das Auskunftsverlangen in die Zukunft, ist die Anordnung außerdem auf höchstens drei Monate zu befristen, wobei eine Verlängerung um jeweils nicht mehr als drei weitere Monate zulässig ist, wenn die Voraussetzungen noch vorliegen. Unverändert weiter gilt die Pflicht zur Benachrichtigung der Beteiligten (jetzt § 101 Abs. 1 StPO) sowie zur Vernichtung der Unterlagen (jetzt § 100h Abs. 1 S. 3 i. V. m. § 100b Abs. 6 StPO).

Erfreulich ist außerdem, dass der Schutz der Zeugnisverweigerungsrechte für Geistliche, Verteidiger und Abgeordnete sichergestellt ist (§ 100h Abs. 2 StPO). Er entfällt nur dann, wenn die betreffenden Personen selbst einer Teilnahme an der Straftat oder einer Begünstigung, Strafvereitelung oder Hehlerei verdächtig sind. Hervorheben möchte ich ferner, dass die §§ 100g, 100h StPO bis zum 31. Dezember 2004 befristet sind, da bis zu diesem Zeitpunkt die Ergebnisse von verschiedenen Gutachten vorliegen sollen, die zur Thematik „Überwachung des Fernmeldeverkehrs" vom BMJ in Auftrag gegeben wurden.

Welche Daten von dem Auskunftsanspruch nach §§ 100g, h StPO erfasst werden, ist nunmehr ausdrücklich geregelt, und zwar in § 100 g Abs. 3 StPO, der sich inhaltlich an § 6 der Telekommunikations-Datenschutzverordnung (TDSV) anlehnt. So ist u. a. über die Standortkennung sowie über Berechtigungskennungen und Kartennummern Auskunft zu erteilen. Ich gehe davon aus, dass sich diese Verpflichtung der Diensteanbieter nur auf bei ihnen bereits vorhandene Daten beschränkt. Es verhält sich nämlich so, dass die genannten Daten nach der TDSV zwar gespeichert werden dürfen, dies tatsächlich jedoch nicht immer geschieht. So wird z. B. die Standortkennung bei den Diensteanbietern nur bei einer standortabhängigen Tarifgestaltung gespeichert. Eine andere Interpretation des Gesetzes würde zu einer Verpflichtung der Diensteanbieter führen, Daten auch dann zu speichern, wenn sie von ihnen gar nicht benötigt werden, also nur für Zwecke der Strafverfolgung. Eine solche Verpflichtung sollte jedoch mit der Einführung der §§ 100g, h StPO ausweislich der Begründung des Gesetzentwurfs gerade nicht verbunden sein.

Kritisch möchte ich zu den neu eingefügten Vorschriften bemerken, dass es bezüglich der Übermittlung zukünftiger Verbindungsdaten an einer eindeutigen Regelung darüber fehlt, ob diese in periodischen Abständen oder unmittelbar nach der Verbindung stattzufinden hat. Problematisch ist, dass es für eine unmittelbare Übermittlung der Daten derzeit keine entsprechende Technik bei den verpflichteten Unternehmen gibt. Um hier zu einer Lösung der technischen Umsetzungsprobleme zu gelangen, wurde beim Bundesministerium für

Wirtschaft und Arbeit eine Arbeitsgruppe eingerichtet, an der ich mitwirke.

Insgesamt stellen die neuen Vorschriften jedoch einen ausgewogenen Ausgleich zwischen dem Strafverfolgungsinteresse des Staates und dem Persönlichkeitsrecht des einzelnen Bürgers dar.

8.2.2 Zeugnisverweigerungsrecht von Journalisten erweitert

Am 23. Februar 2002 ist ein Gesetz zur Änderung der Strafprozessordnung in Kraft getreten, mit dem das Zeugnisverweigerungsrecht für Medienmitarbeiter gem. § 53 Abs. 1 Nr. 5 StPO erweitert und zugleich das damit zusammenhängende Beschlagnahmeverbot des § 97 Abs. 5 StPO ausgedehnt wurde (BGBl. I S. 682 f.).

Wie bereits berichtet (s. 18. TB Nr. 6.7 zu dem entsprechenden Gesetzentwurf der Bundesregierung), erstreckt sich das Zeugnisverweigerungsrecht der Journalisten nunmehr auch auf selbst erarbeitete Materialien und berufsbezogene Wahrnehmungen.

Weil es in der Praxis der Medienarbeit nicht immer möglich ist, deutlich zwischen Informationen, die selbst recherchiert wurden und solchen, die von Dritten stammen, zu trennen, habe ich diese Neuregelung aus datenschutzrechtlicher Sicht begrüßt.

Auch gegen die Einschränkung dieses erweiterten Zeugnisverweigerungsrechts bei Verbrechen und bei den in § 53 Abs. 2 S. 2 Nr. 1 bis 3 StPO genannten Straftaten im Interesse einer funktionsfähigen Strafrechtspflege und einer umfassenden Wahrheitsermittlung im Strafverfahren habe ich aus datenschutzrechtlicher Sicht keine Bedenken angemeldet.

Die gesetzliche Neuregelung enthält jedoch aus meiner Sicht einen „Wermutstropfen“, der das mit dem Zeugnisverweigerungsrecht nach § 53 Abs. 1 Nr. 5 StPO zusammenhängende ebenfalls novellierte Beschlagnahmeverbot nach § 97 Abs. 5 StPO betrifft. Hier sieht das Gesetz u. a. dann eine Ausnahme von der Beschlagnahmefreiheit vor, wenn der Medienmitarbeiter im Verdacht einer Tatbeteiligung steht. Bedauerlicherweise hat der Gesetzgeber insoweit meinen bereits im letzten Tätigkeitsbericht dargestellten Bedenken nicht Rechnung getragen. Ich hatte mich hier mit Nachdruck dafür eingesetzt, die Beschlagnahmefreiheit nur dann entfallen zu lassen, wenn gegen den Medienmitarbeiter ein dringender Tatbeteiligungsverdacht besteht. Mit der nun getroffenen Regelung, nach der ein einfacher Verdacht ausreicht, um die genannten potenziellen Beweismittel (Schriftstücke u. Ä.) bei dem betroffenen Medienmitarbeiter zu beschlagnahmen, besteht die Gefahr, dass dessen Zeugnisverweigerungsrecht allzu leicht ausgehebelt werden kann.

8.2.3 Genomanalyse im Strafverfahren

Die DNA-Analyse hat sich binnen weniger Jahre zu einem außerordentlich effektiven kriminalistischen Instrument entwickelt und ist geradezu ein Symbol der Revolution in der Kriminaltechnik geworden. Allerdings sind Feststellung, Speicherung und Verwendung des DNA-Identifizierungsmusters jeweils nicht unerhebliche Eingriffe in das Recht auf informationelle Selbstbestimmung gemäß Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG, wie auch das Bundesverfassungsgericht in mehreren Entscheidungen festgestellt hat (vgl. zuletzt Kammerbeschluss vom 15. März 2001, NJW 2001 S. 2320). Da solche Eingriffe nur auf gesetzlicher Grundlage im überwiegenden Interesse der Allgemeinheit und unter Beachtung des Grundsatzes der Verhältnismäßigkeit zulässig sind, ist der Gesetzgeber seit Jahren damit beschäftigt, die erforderlichen Rechtsgrundlagen für die DNA-Analyse im Strafverfahren zu schaffen und noch verbliebene oder sogar durch die Gesetzgebung selbst entstandene Zweifelsfragen auszuräumen. Ich habe hierüber in den letzten Tätigkeitsberichten berichtet (vgl. zuletzt 18. TB Nr. 6.3). Wer nun geglaubt hätte, nach immerhin vier Gesetzesänderungen in den Jahren 1997 bis 2000 sei der Regelungsbedarf erschöpft, sah sich schon in der letzten Legislaturperiode getäuscht, als der Gesetzgeber durch das Gesetz zur Änderung der Strafprozessordnung vom 6. August 2002 (BGBl. I S. 3018) klarstellte, dass auch die Untersuchung von Spurenmaterial einer unbekannten Person nur durch den Richter angeordnet werden darf (vgl. unten Nr. 8.2.3.1). Damit ist die Wunschliste an den Gesetzgeber aber noch keineswegs am Ende:

8.2.3.1 Klarstellung: Richtervorbehalt auch bei der DNA-Analyse von Spuren

Gegen Ende der 14. Legislaturperiode konnte erfreulicherweise eine schon länger andauernde Meinungsverschiedenheit zwischen Bundesregierung und Bundesrat in einem datenschutzfreundlichen Sinne geklärt werden. Nach § 81e StPO dürfen molekulargenetische Untersuchungen nicht nur an Probenmaterial des Beschuldigten eines Strafverfahrens (Absatz 1), sondern auch an aufgefundenem, sicher gestelltem oder beschlagnahmtem Spurenmaterial, das einem Verursacher noch nicht zugeordnet werden kann (Absatz 2), durchgeführt werden. Die Anordnung der Untersuchung ist gem. § 81f StPO dem Richter vorbehalten, ohne dass zwischen den beiden Alternativen differenziert wird. Einige Landgerichte vertreten dazu allerdings die Auffassung, dass es bei solchen Spuren mangels Eingriffs in das Recht auf informationelle Selbstbestimmung einer bekannten Person keiner richterlichen Anordnung bedarf und die Anordnung durch die Staatsanwaltschaft oder ihre Hilfsbeamten ausreicht.

Der Bundesrat hat angesichts der divergierenden Rechtsprechung einen Gesetzentwurf vorgelegt, mit dem klar gestellt werden sollte, dass die DNA-Analyse von Spuren unbekannter Verursacher nicht durch den Richter angeordnet werden müsse, sondern eine Anordnung durch die Staatsanwaltschaft oder durch ihre Hilfsbeamten ausreiche.

Dieser Gesetzentwurf fand keine Zustimmung. Vielmehr folgte der Deutsche Bundestag einem konträren Gesetzentwurf der Bundesregierung: In dem Gesetz zur Änderung der Strafprozessordnung vom 6. August 2002 (BGBl. I S. 3018) wurde das Erfordernis einer richterlichen Anordnung für die molekulargenetische Untersuchung sowohl in den Fällen des § 81e Abs. 1 als auch in den Fällen des § 81e Abs. 2 StPO nunmehr noch deutlicher als bisher klargestellt.

Hierzu habe ich u. a. in einer Anhörung vor dem Rechtsausschuss des Deutschen Bundestages betont, dass der Einsatz derartiger Untersuchungen im Strafverfahren zu empfindlichen, den Kern der Persönlichkeit berührenden Eingriffen führt. Dass die betroffene Person den Strafverfolgungs-

behörden noch nicht namentlich bekannt ist, ändert daran nichts. Eine Anordnungskompetenz der Staatsanwaltschaft würde der Grundrechtsrelevanz solcher Maßnahmen im Hinblick auf die Möglichkeit der Verknüpfung mit der Gen-Datei des Spurenverursachers nicht gerecht.

8.2.3.2 Ultima ratio zur Aufklärung schwerer Verbrechen: DNA-Massentest

DNA-Massentests gehören schon fast zum Standardrepertoire der Strafverfolgungsbehörden, um einen Täter oder eine Täterin aus einer Vielzahl von in Betracht kommenden Personen herauszufiltern. Solche Massentests können mitunter sehr große Personenzahlen treffen: Bei der bislang wohl größten Reihenuntersuchung im Fall der ermordeten Christina Nytsch 1998 in Niedersachsen wurden beispielsweise insgesamt 17 900 Personen um Speichelproben ersucht.

Ob es im geltenden Recht eine tragfähige Grundlage gibt, solche Massentests zwangsweise durchzuführen, ist umstritten. Zum Teil wird angenommen, es handele sich bei dem betroffenen Personenkreis weitgehend um Beschuldigte, die eine Entnahme und Analyse der Speichelprobe nach § 81e Abs. 1 Satz 1 oder § 81a StPO auch gegen ihren Willen dulden müssten. Dies würde voraussetzen, dass hinsichtlich sämtlicher betroffener Personen ein Anfangsverdacht i. S. v. § 152 Abs. 2 StPO besteht. Davon kann jedoch lediglich in Einzelfällen, bei denen ausnahmsweise hinreichend präzise Anhaltspunkte für einen Tatverdacht einer größeren Personengruppe gegeben sind, ausgegangen werden. In der Regel wird aber kaum ein Anfangsverdacht im Sinne der Strafprozessordnung gegen eine Vielzahl von Personen bejaht werden können, die nichts anderes mit der Tat verbindet als Geschlecht, Alter oder Wohnort. Zwangsweise Tests sind aber auch gegenüber anderen Personen, die keine Beschuldigten sind, für bestimmte Zwecke zulässig, etwa zur Klärung der Frage, ob sich am Körper der Person bestimmte Spuren oder Folgen der Straftat befinden (§ 81e Abs. 1 Satz 2 i. V. m. § 81c Abs. 1 StPO) oder ob aufgefundenes Material vom Beschuldigten oder Verletzten stammt (§ 81e Abs. 1 Satz 2 i. V. m. § 81c Abs. 2 StPO). Mit diesen Zweckbindungen sind aber Massentests, die eine ganz andere Zielrichtung verfolgen, kaum zu vereinbaren. Ich halte deshalb eine zwangsweise Reihenuntersuchung nicht für zulässig. Sie kann nur auf freiwilliger Basis durchgeführt werden. Das heißt, dass jeder einzelne Teilnehmer vor der Abnahme einer Speichelprobe nach einer entsprechenden Belehrung gemäß § 4a BDSG schriftlich seine Einwilligung erklären muss.

Allerdings ist auch die Einwilligung als Rechtsgrundlage für den DNA-Massentest nicht unproblematisch. Die rechtsstaatliche Problematik derartiger molekulargenetischer Reihenuntersuchungen liegt in der Gefahr einer Durchbrechung der Unschuldsvermutung und faktischen Umkehr der Beweislast. Die Strafverfolgungsorgane müssen den Teilnehmern, soweit sie nicht Beschuldigte sind, bis auf ganz allgemeine Kriterien wie vermutete Altersgruppe und Wohnort keine Tatnähe im Sinne eines konkreten Verdachts nachweisen. Umgekehrt geraten aber diejenigen, die – aus welchen Gründen auch immer – nicht an dem Massentest teilnehmen wollen, schon dadurch ins Zentrum der Ermittlungen, nicht selten auch unter sozialen Druck und müssen sich für ihre Ablehnung rechtfertigen.

Angesichts der aufgezeigten Problematik von DNA-Massentests plädiere ich für eine gesetzliche Regelung. Eine solche Bestimmung muss rechtsstaatliche Mindestanforderungen definieren, etwa wie folgt:

1. Massentests müssen ultima ratio der strafprozessualen Ermittlungen bleiben. Es bedarf also einer Subsidiaritätsklausel, wonach die Anordnung erst dann zulässig sein sollte, wenn alle im konkreten Fall einsetzbaren und gesetzlich zulässigen Ermittlungsinstrumente ergebnislos ausgeschöpft sind.
2. Der Grundsatz der Verhältnismäßigkeit gebietet wegen des Eingriffs in die Grundrechte einer Vielzahl von Personen eine Beschränkung auf einen Katalog schwerer Straftaten gegen Leib und Leben sowie die sexuelle Selbstbestimmung.
3. Ein Zwang zur Abgabe einer DNA-untersuchungsfähigen Probe darf nur aufgrund eines konkreten Tatverdachts, also gegen Beschuldigte im Sinne der Strafprozessordnung, ausgeübt werden. Bei allen übrigen Personen darf dies nur auf freiwilliger Basis geschehen, wobei die Verweigerung der Zustimmung nicht als Verdachtsmoment gewertet werden darf.
4. Die Anordnung eines DNA-Massentests muss dem Richter vorbehalten bleiben. Staatsanwaltschaft und Polizei sollten nicht anordnungsbefugt sein. Eine Eilkompetenz ist entbehrlich, weil schon die organisatorische Vorbereitung für einen DNA-Massentest so viel Zeit in Anspruch nimmt, dass eine richterliche Anordnung rechtzeitig herbeigeführt werden kann.

8.2.3.3 Einwilligung ersetzt nicht die Prognoseentscheidung des Richters

Schon in meinem letzten Tätigkeitsbericht habe ich bemängelt, dass § 3 Satz 3 des DNA-Identitätsfeststellungsgesetzes vom 7. September 1998 (BGBl. I S. 2646), der die Speicherung der im laufenden Strafverfahren gewonnenen DNA-Identifizierungsmuster zulässt, nicht auf den Richtervorbehalt in § 81g Abs. 3 StPO verweist. Dies führt dazu, dass in diesen Fällen nicht der Richter über das Vorliegen einer Straftat von erheblicher Bedeutung entscheidet und eine besondere Wiederholungsgefahr prognostizieren muss, sondern die Staatsanwaltschaft oder die Polizei. Im Ergebnis führt dieser Verzicht auf die richterliche Gefahrenprognose leider meistens dazu, dass die Anordnung einer DNA-Analyse im laufenden Verfahren automatisch die Speicherung dieser Daten in der DNA-Analyse-Datei nach sich zieht.

Ebenfalls unter Nr. 6.3 des 18. TB habe ich die Praxis der Strafverfolgungsbehörden einiger Länder angesprochen, auf richterliche Anordnungen zur Entnahme und Untersuchung von DNA-Identifizierungsmustern von Strafgefangenen zu verzichten und diese Maßnahmen stattdessen allein auf die Einwilligung der Betroffenen zu stützen. Diese Handhabung hat sich – jedenfalls in einigen Ländern – offenbar über den Bereich der Strafgefangenen hinaus generell auf die Fälle des § 81g StPO und des § 2 DNA-Identitätsfeststellungsgesetz ausgeweitet (vgl. auch Nr. 13.3, soweit der Bund betroffen ist). In anderen Ländern hält man zwar für die Entnahme einer DNA-Probe die Einwilligung des Betroffenen für ausreichend. Für die Analyse der Probe bleibt es jedoch

in jedem Fall bei der richterlichen Anordnung. Gleichwohl ist auch in diesen Ländern die in § 81g StPO und § 2 DNA-Identitätsfeststellungsgesetz vorgesehene Prognose einer besonderen Wiederholungsgefahr nicht immer Gegenstand einer richterlichen Entscheidung, sondern wird mitunter auch von der Staatsanwaltschaft bzw. sogar der Polizei getroffen. Angesichts dieser m. E. nicht hinnehmbaren Tendenz und der in den einzelnen Ländern unterschiedlichen Praxis halte ich eine Klarstellung durch den Gesetzgeber für geboten. Hierbei sollte eindeutig bestimmt werden, dass DNA-Analysen für Zwecke künftiger Strafverfahren nach § 81g StPO und § 2 DNA-Identitätsfeststellungsgesetz und deren Speicherung nach § 3 DNA-Identitätsfeststellungsgesetz nur aufgrund einer richterlichen Anordnung durchgeführt und nicht durch eine Einwilligung des Betroffenen oder Entscheidungen der Staatsanwaltschaft bzw. der Polizei ersetzt werden dürfen.

In diesem Zusammenhang ist anzumerken, dass das Bundesverfassungsgericht in zwei Kammerbeschlüssen vom 14. Dezember 2000 und vom 18. März 2001 (abgedruckt in NJW 2001 S. 879 und 2320) festgestellt hat, dass § 2 DNA-Identitätsfeststellungsgesetz i. V. m. § 81g StPO verfassungsgemäß ist. Gleichzeitig hat das Gericht aber auch die hohen inhaltlichen Anforderungen an die Prognoseentscheidung und ihre tatsächlichen Grundlagen hervorgehoben. Diesem verfassungsrechtlichen Maßstab wird m. E. nur eine richterliche Anordnung auf der Basis einer individuellen Prognose gerecht.

8.2.3.4 Erweiterung des Anlasstatenkatalogs in § 81g Strafprozessordnung

Die Entnahme von Körperzellen des Beschuldigten eines Strafverfahrens und die Feststellung des DNA-Identifizierungsmusters für künftige Strafverfahren nach § 81g Abs. 1 StPO sind nur zulässig, wenn der Beschuldigte einer Straftat von erheblicher Bedeutung, insbesondere eines Verbrechens, eines Vergehens gegen die sexuelle Selbstbestimmung, einer gefährlichen Körperverletzung, eines Diebstahls in besonders schwerem Fall oder einer Erpressung verdächtig ist. Dieser Straftatenkatalog wird heute vielfach unter Hinweis auf den Schutz der Bevölkerung insbesondere vor Sexualstraftätern als zu eng empfunden. Die parlamentarischen Gremien haben sich im Berichtszeitraum mit Gesetzesvorschlägen mehrerer Bundesländer und der CDU/CSU-Bundestagsfraktion befasst, die darauf abzielen, in den Anlasstatenkatalog einen neuen Tatbestand einzuführen, der eine DNA-Erfassung schon bei jedem Vergehen mit sexuellem Hintergrund erlaubt (Bundesratsdrucksache 517/02; 850/02 sowie Bundestagsdrucksache 15/29). Zur Begründung wird angeführt, durch wissenschaftliche Untersuchungen werde bestätigt, dass oft weniger gewichtige Straftaten der Beginn einer kriminellen Karriere seien, an deren Ende schwerste Straftaten stehen können. Hierzu hat die Bundesregierung allerdings in ihrer Stellungnahme (Bundestagsdrucksache 14/9887) zutreffend darauf hingewiesen, dass eine im Auftrag des Bundesministeriums der Justiz durchgeführte Untersuchung der Universität Göttingen zur Rückfälligkeit von exhibitionistischen Straftätern vom April 2002 für einen Untersuchungszeitraum von vier Jahren zu dem Ergebnis kam, dass in diesem Zeitraum nur rd. 1 bis 2 % der exhibitionistischen Straftäter später wegen eines sexuellen Gewaltdelikts oder einer sonstigen Gewalttat verurteilt wurden. Ich halte deshalb die Vorstellung von einer geradlinigen Karriere vom Exhibitionisten zum Gewalttäter für nicht sehr überzeugend. Überdies würden bei der vorgeschlagenen Erweiterung auf Vergehen mit sexuellem Hintergrund selbst Delikte mit reinem Belästigungscharakter oder auch Beleidigung (§ 185 Strafgesetzbuch) mit sexuellem Inhalt als Anlasstaten ausreichen.

Außerdem sehe ich keinen zwingenden Grund für eine Sonderbehandlung der Sexualdelikte, zumal eine Zunahme solcher Straftaten – anders als die öffentliche Diskussion vermuten lässt – statistisch nicht belegt ist. Ebenso wie die Bundesregierung begrüße ich aber, dass der Entwurf immerhin an dem Erfordernis einer qualifizierten Negativprognose festhält, wonach eine DNA-Analyse nur dann zulässig ist, wenn Grund zu der Annahme besteht, dass gegen den Beschuldigten künftig erneut Strafverfahren wegen einer Straftat von erheblicher Bedeutung zu führen sind.

In diesem Zusammenhang möchte ich anmerken, dass es – insbesondere von Seiten der Länder – auch Vorschläge gegeben hat, auf das Erfordernis einer Straftat von erheblicher Bedeutung als Anlassstraftat zu verzichten und schon bei Verurteilung zu einer Strafe von mindestens einem Jahr Freiheitsentzug von der Annahme auszugehen, dass diese bereits für sich allein eine Negativprognose begründe (vgl. Bundesratsdrucksache 434/01). Dieser Vorschlag hat jedoch schon im Bundesrat keine Mehrheit gefunden. Schließlich ist sogar vorgeschlagen worden, DNA-Identifizierungsmuster von allen Männern ohne besonderen Anlass zu erheben und rein vorsorglich in der DNA-Analyse-Datei zu speichern. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat diesen Vorschlag entschieden als verfassungswidrig zurückgewiesen (s. Anlage 14).

8.2.4 IMSI-Catcher – jetzt auch im Strafverfahren

Ebenfalls in den letzten Wochen der 14. Legislaturperiode ist ein neuer Paragraph 100i in die StPO eingefügt worden. Diese Vorschrift erlaubt den Einsatz technischer Mittel zur Ermittlung der Geräte- und Kartennummer oder des Standorts eines aktiv geschalteten Handys. Über das dafür eingesetzte Gerät, den so genannten IMSI-Catcher, habe ich zuletzt im 18. TB (Nr. 10.4) berichtet. Dieser IMSI-Catcher simuliert eine Funkzelle mit großer Feldstärke, sodass sich alle Handys in einem bestimmten Umkreis nicht bei der echten Funkzelle, sondern bei der des IMSI-Catchers melden.

Ursprünglich enthielt der von der Bundesregierung eingebrachte Entwurf eines „Gesetzes zur Änderung der Strafprozessordnung“, das am 14. August 2002 in Kraft getreten ist, nur eine klarstellende Regelung zum Richtervorbehalt für die Anordnung von DNA-Analysen bei Spurenmaterial (s. Nr. 8.2.3.1). Nahezu unbemerkt von der Öffentlichkeit wurde der Gesetzentwurf um die Regelung über den IMSI-Catcher (§ 100i StPO) aufgrund einer Formulierungshilfe der Bundesregierung im Zuge der Ausschussberatungen des Deutschen Bundestages ergänzt.

Ich habe im Rahmen einer Anhörung und bei der maßgeblichen Beratung des Entwurfs im Rechtsausschuss des Deutschen Bundestages – ebenso wie bei der parlamentarischen Beratung des § 9 Abs. 4 des Bundesverfassungsschutzgesetzes im Rahmen des Terrorismusbekämpfungsgesetzes – Be-

denken gegen die Regelung über den Einsatz des IMSI-Catchers erhoben, da hierdurch notwendigerweise auch immer Unbeteiligte betroffen sind. Darüber hinaus habe ich zu der konkreten Ausgestaltung der Vorschrift folgende Änderungen – leider vergeblich – gefordert:

- Die Ermittlung der Gerätenummer ist meines Erachtens keine geeignete Maßnahme, da sie weder generell bei einem erstmaligen Verkauf des Geräts gespeichert wird noch bei einer späteren Veräußerung oder Verlust des Geräts nachgehalten werden kann. Sie ist damit kein eindeutiges Identifizierungsmerkmal.
- Die Eingriffsschwelle zur Übermittlung des Aufenthaltsortes ist nach meinem Dafürhalten zu niedrig. Für die Standortfeststellung nach § 100i Abs. 2 Satz 2 StPO reicht es nämlich bereits aus, dass die Ermittlung des Aufenthaltsortes des Täters „auf andere Weise weniger erfolgversprechend oder erschwert wäre". Im Hinblick auf den mit dem Einsatz des Geräts verbundenen Grundrechtseingriff bei einer Vielzahl von Personen hatte ich gefordert, dass die Ermittlung auf andere Weise „nicht möglich oder wesentlich erschwert wäre", wie dies zur Vorbereitung einer Abhörmaßnahme nach § 100a StPO gemäß § 100i Abs. 2 Satz 1 StPO vorgeschrieben ist.
- Die Dauer der Maßnahme, die gemäß § 100i Abs. 4 Satz 2 StPO bis zu sechs Monaten angeordnet werden kann, ist nach meiner Auffassung zu lang. Ich hatte stattdessen eine Begrenzung auf drei Monate vorgeschlagen, wie sie bei der Überwachungsmaßnahme gemäss § 100b Abs. 2 StPO vorgesehen ist.

Demgegenüber habe ich begrüßt, dass die Anordnung des Einsatzes eines IMSI-Catchers dem Richter vorbehalten ist.

8.2.5 Erneute Erweiterung des Straftatenkatalogs in § 100a Strafprozessordnung

Die Telefonüberwachung ist unbestreitbar ein wichtiges Hilfsmittel im Kampf gegen die Kriminalität. Es war deshalb durchaus sinnvoll, dass mit Artikel 2 des Sechsten Gesetzes zur Änderung des Strafvollzugsgesetzes vom 5. Oktober 2002 (BGBl. I S. 3954) die Straftaten

- schwerer sexueller Missbrauch von Kindern nach § 176a Abs. 1, 2 oder 4 des Strafgesetzbuches (StGB),
- sexueller Missbrauch von Kindern mit Todesfolge nach § 176b StGB und
- Verbreitung pornographischer Schriften nach § 184 Abs. 4 StGB

in den Katalog der Straftaten in § 100a StPO, bei denen die Überwachung und Aufzeichnung der Telekommunikation angeordnet werden darf, einbezogen wurden. Allerdings ist die Telefonüberwachung auch ein tiefer Eingriff in das Persönlichkeitsrecht des Betroffenen. Deshalb bedarf es in bestimmten Zeitabständen bezüglich des Straftatenkatalogs immer wieder einer sorgfältigen Abwägung zwischen dem Strafverfolgungsinteresse des Staates und der Einschränkung von Grundrechten des Betroffenen. Der Gesetzgeber sollte daher darüber informiert sein, welche Ergebnisse in der Praxis tatsächlich zu verzeichnen sind. Vor diesem Hintergrund begrüße ich das Vorhaben der Bundesregierung, den Anlasstatenkatalog des § 100a Satz 1 StPO einer grundsätzlichen Überprüfung zu unterziehen (vgl. hierzu auch Nr. 8.3). Grundlage hierfür ist die bei dem Max-Planck-Institut für ausländisches und internationales Strafrecht im Auftrag des BMJ gegenwärtig erarbeitete Untersuchung zur „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen". Diese Überprüfung ist vor allem deshalb erforderlich, weil immer wieder neue Vorschläge und Gesetzentwürfe zur Ausweitung des Straftatenkatalogs eingebracht werden. Ich werde die Entwicklung weiter aufmerksam begleiten.

8.3 Was macht das Forschungsvorhaben zur Telefonüberwachung?

Bereits in meinem letzten Tätigkeitsbericht (vgl. Nr. 6.4.2) habe ich über das vom BMJ beim Max-Planck-Institut für ausländisches und internationales Strafrecht in Auftrag gegebene Forschungsvorhaben „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b Strafprozessordnung (StPO) und anderer verdeckter Ermittlungsmaßnahmen" berichtet.

Die Anzahl der nach § 100a StPO angeordneten Verfahren steigt weiterhin. Zum einen steigt die Gesamtzahl der Verfahren mit Telefonüberwachungsmaßnahmen, zum anderen auch die durchschnittliche Zahl der Telefonüberwachungsanordnungen pro Verfahren. Im Mittelpunkt der Untersuchung des Max-Planck-Instituts steht die Bedeutung der Erkenntnisse aus der Telefonüberwachung für das Strafverfahren und die Frage, inwieweit Telefonüberwachungsmaßnahmen wirklich zum Erfolg der staatlichen Strafverfolgung geführt haben. Wichtig für die Studie ist eine möglichst präzise Aufbereitung von Daten, mit denen Entwicklung und Strukturen der Telefonüberwachung nachgewiesen werden können. Neben der Aktenanalyse werden die bei der Anordnung beteiligten Personen, wie Polizisten, Staatsanwälte, Richter und Verteidiger, befragt. Bei der Ablaufplanung der Untersuchung bin ich beteiligt. So ist sichergestellt, dass dabei keine personenbezogenen Daten verarbeitet werden.

Die Vorlage des Schlussberichtes ist nunmehr für März 2003 vorgesehen.

8.4 Wann werden die Berichte über die akustische Wohnraumüberwachung endlich besser?

Mit der Einführung des „Großen Lauschangriffs" im Jahre 1998 wurde die Bundesregierung gem. Artikel 13 Abs. 6 S. 1 Grundgesetz verpflichtet, den Deutschen Bundestag jährlich über die zum Zweck der Strafverfolgung durchgeführten akustischen Wohnraumüberwachungen zu unterrichten (vgl. schon 16. TB Nr. 1.6 und 6.1.1; 17. TB Nr. 6.1 und 6.1.1). Inzwischen liegen die Berichte der Jahre 2000 und 2001 vor. Mit Bedauern muss ich feststellen, dass auch diese, ebenso wie schon die Berichte der Jahre 1998 und 1999, den Anforderungen, dem Parlament eine effektive Kontrolle insbesondere der Angemessenheit und Eignung der durchgeführten Maßnahmen zu ermöglichen, nicht gerecht werden. Die in den Berichten gegebenen Informationen reichen hierzu nicht aus.

Die Datenschutzbeauftragten des Bundes und der Länder hatten bereits im Juni 2000 Wünsche bzw. Empfehlungen zu erweiterten Berichtspflichten formuliert (siehe hierzu die Entschließung vom 26. Juni 2000, Anlage 22 zum 18. TB).

Nicht zuletzt aufgrund dieser Anregung äußerte auch das Kontrollgremium des Bundestages den Wunsch nach „angereicherten Erkenntnissen". Daraufhin prüfte eine Arbeitsgruppe des Strafrechtsausschusses der Konferenz der Justizministerinnen und -minister den Sachverhalt. Aufgrund des als Ergebnis verfassten Berichtes hat die Konferenz im November 2001 dann zwar einige Präzisierungen der Erhebungsbögen sowie Hinweise hierzu beschlossen, die für die Berichte ab dem Berichtsjahr 2002 relevant sein werden. Die Wünsche bzw. Empfehlungen der Datenschutzbeauftragten wurden jedoch nur in sehr geringem Umfang berücksichtigt. Insbesondere soll auch in Zukunft nur die Anzahl der Beschuldigten bzw. der Wohnungsinhaber, auch wenn sie nicht beschuldigt sind, genannt werden. Somit werden Angaben über die Anzahl aller von der Maßnahme betroffenen Personen, also auch z. B. von unverdächtigen Familienangehörigen oder zufälligen Besuchern, weiterhin fehlen.

Nach meiner Auffassung ist dies jedoch, ohne dass ich hier näher auf die mehr gesetzestechnische Begründung der Arbeitsgruppe eingehen möchte, im Ergebnis nicht ausreichend. Sinn und Zweck der Aufnahme von Angaben zu Drittbetroffenen in die Berichte der Bundesregierung ist es, dem „Artikel-13-Gremium" des Bundestages einen Überblick darüber zu ermöglichen, wie viele unbescholtene Bürger von den Überwachungsmaßnahmen betroffen sind, um bedenklichen Entwicklungen ggf. gegensteuern zu können. Die Drittbetroffenen müssen daher jedenfalls in ihrer Gesamtzahl in dem Bericht an das Parlament aufgeführt werden (Umfang der Maßnahme). Ich appelliere deshalb dringend an die Bundesregierung, darauf hinzuwirken, dass die Berichte in Zukunft insoweit erweitert werden und möchte in diesem Zusammenhang auch die sonstigen Anregungen der Entschließung vom 26. Juni 2000 nochmals in Erinnerung rufen.

Unter inhaltlichen Aspekten ist aus meiner Sicht bemerkenswert, dass die Anlasstaten sich wie schon in den Jahren 1998 und 1999 auch im Berichtszeitraum 2000 und 2001 im Wesentlichen auf Mord bzw. Totschlag und Betäubungsmitteldelikte beschränkten. Es scheint sich hier ein andauernder Trend abzuzeichnen. Auffallend ist in diesem Zusammenhang, dass bestimmte Katalogtaten des § 100c Nr. 3 Buchstabe a bis f Strafprozessordnung (StPO) bisher überhaupt noch nicht Anlass einer Überwachungsmaßnahme waren. Hierzu zählen z. B. Delikte wie Geld- oder Wertpapierfälschung, schwerer Menschenhandel, gewerbsmäßige Hehlerei, Bandenhehlerei sowie Straftaten nach dem Außenwirtschafts- und Kriegswaffenkontrollgesetz. Dies hat auch die Bundesregierung in ihrem „Erfahrungsbericht zu den Wirkungen der Wohnraumüberwachung durch Einsatz technischer Mittel" vom 30. Januar 2002 (Bundestagsdrucksache 14/8155 S. 5) konstatiert. Nach ihrer Auffassung erschienen angesichts des geringen Anwendungsgrades der Maßnahme insgesamt Rückschlüsse auf die Erforderlichkeit der Aufnahme dieser Straftaten in den Katalog des § 100c Abs. 1 StPO jedenfalls verfrüht. Diese Aussage erscheint mir jedoch zumindest fraglich. Immerhin sind bereits vier Jahre seit der Einführung des Instrumentes der akustischen Wohnraumüberwachung vergangen. Die Bundesregierung hat in ihrem Erfahrungsbericht (a. a. O., S. 10) selbst darauf hingewiesen, dass die Bedeutung der Maßnahme für die Bekämpfung der Organisierten Kriminalität von den Landesjustizverwaltungen zwar nahezu einhellig betont wird, dies jedoch durch Einzelbeispiele nicht hinreichend belegt werden kann. Die von ihr angekündigte Prüfung, ob eine bessere Erfolgskontrolle, insbesondere durch entsprechende Forschungsaufträge, erreicht werden kann, bleibt abzuwarten (a. a. O., vgl. S. 13). Angesichts der Intensität der Grundrechtseingriffe werde ich darauf hinwirken, dass diese Prüfung möglichst auch zeitnah abgeschlossen wird. Zustimmend zur Kenntnis genommen habe ich, dass die Bundesregierung derzeit zur Einführung des Instrumentes der optischen Wohnraumüberwachung („großer Spähangriff") keinen Handlungsbedarf sieht (a. a. O., S. 11 f.).

8.5 „Cyber Crime Convention" – Übereinkommen des Europarates über Datennetzkriminalität

In meinem 18. TB (Nr. 6.10) habe ich über den Entwurf eines Übereinkommens des Europarates über Datennetzkriminalität berichtet, dem u. a. die Überzeugung zugrunde liegt, dass eine wirksame Bekämpfung der Datennetzkriminalität eine verstärkte und rasche internationale Zusammenarbeit in Strafsachen verlangt. Das Übereinkommen ist am 23. November 2001 in Budapest von 26 Mitgliedsstaaten des Europarates – darunter auch Deutschland – sowie von Kanada, Japan, Südafrika und den USA unterzeichnet worden. In Kraft tritt die Konvention allerdings erst dann, wenn fünf Unterzeichnerstaaten sie ratifiziert haben.

Das BMJ hat mich seit dem Frühjahr 1999 regelmäßig an den Arbeiten zum Konventionsentwurf beteiligt. Erfreulicher Weise sind die – nicht zuletzt aufgrund meiner Stellungnahmen – bereits im Verlauf der Beratungen erreichten inhaltlichen Verbesserungen auch noch in der endgültigen Fassung des Übereinkommens enthalten. Dabei handelt es sich insbesondere um solche bei den Bestimmungen zu Überwachungsmaßnahmen im Bereich der elektronischen Kommunikation. So ist die Befugnis zum „Abfangen" der so genannten Inhaltsdaten, also die Überwachung des Kommunikationsinhalts selbst nach Artikel 21 des Übereinkommens endgültig auf Verfahren bei schwerwiegenden Delikten, die nach innerstaatlichem Recht zu bestimmen sind, beschränkt (für Deutschland vgl. insoweit §§ 100a, 100b Strafprozessordnung – StPO). Hinsichtlich der Verbindungsdaten bestimmt das Vertragswerk, dass eine Erhebung oder Aufzeichnung nur möglich ist, wenn nationale Bestimmungen nicht entgegenstehen. Auf diese Weise ist gewährleistet, dass die hier inzwischen im deutschen Strafverfahrensrecht erreichten Verbesserungen (nicht jedes Delikt rechtfertigt jetzt mehr ein Auskunftsverlangen über Verbindungsdaten an die Telekommunikationsdiensteanbieter, vgl. hierzu die neu eingefügten §§ 100g, 100h StPO, s. o. Nr. 8.2.1) nicht durch Regelungen des Übereinkommens unterlaufen werden. Schon im Entwurfsstadium konnte ich darüber hinaus erreichen, dass Vorschriften bezüglich der Verpflichtung von Telekommunikationsdiensteanbietern zur vorsorglichen Speicherung von Verbindungs- und Nutzungsdaten gestrichen wurden.

Leider wurde meiner Forderung nicht entsprochen, in den Bestimmungen über Verfahren bei Rechtshilfeersuchen (Artikel 27 und 28 des Übereinkommens) die datenschutzrechtlichen Regelungen zu verbessern. Es gab von deutscher Seite hierzu den Vorschlag, Artikel 27 Abs. 4 des Übereinkommens dahin gehend zu ergänzen, dass eine Ablehnung des

Hilfeersuchens auch dann möglich sein sollte, wenn in dem ersuchenden Staat kein angemessenes Datenschutzniveau gewährleistet ist (s. zu dies er Forderung und allgemein zur Schaffung von nationalen und internationalen Regelungen zur Bekämpfung der Datennetzkriminalität auch die Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001, Anlage 11). Allerdings konnte hier im Rahmen der V erhandlungen insofern noch ein Kompromiss erreicht werden, als im erläuternden Bericht zu Artikel 27 die Er gänzung aufgenommen wurde, dass im Rahm en des allgemeinen Rechtshilfeverweigerungsgrundes „wesentlicher Interessen" einer Vertragspartei in Ausnahmefällen über Artikel 28 des Übereinkommens hinaus zusätzliche Gesichtspunkte des Datenschutzes geltend gemacht werden können. Angesichts dieser Tatsache und in Anbetracht des eingeschränkten Anwendungsbereichs der genannten Vorschriften (sie finden i. d. R. nur Anwendung, wenn zwischen den beteiligten V ertragsparteien keine entspreche nden anwendbaren völkerrechtlichen Übereinkünfte bestehen; in den meisten Fällen wird jedoch das „Europäische Übereinkommen über die Rechtshilfe in Strafsachen" sowie dessen Zusatzprotokoll gelten) hält sich nach meiner Auf fassung der „Schaden" in Grenzen, sodass ich insgesamt mit den erreichten V erbesserungen zufrieden bin.

8.6 Änderungen im Strafvollzugsgesetz

Mit dem Sechsten Gesetz zu r Änderung des Strafvollzugsgesetzes vom 5. Oktober 2002 (BGBl I S. 3954 f.) ist eine gesetzliche Grundlage zur elektronischen Speicherung von Lichtbildern von Gefangenen sowie zur Übermittlung von personenbezogenen Daten an Finanzbehörden durch die Vollzugsbehörde geschaffen worden. An den Beratungen war ich beteiligt. Allerdings wurden meine Forderungen nur teilweise berücksichtigt.

Bisher war die Aufnahme von Lichtbildern als erkennungsdienstliche Maßnahme nur zur Sicherung des Vollzuges gemäß § 86 Strafvollzugsgesetz (StV ollzG) zulässig. Nach dem neu eingefügten § 86a StVollzG dürfen Lichtbilder der Gefangenen nunmehr auch zu r Aufrechterhaltung der Sicherheit und Ordnung der An stalt aufgenommen und mit dem Namen der Gefangenen sowie deren Geburtsdatum und -ort gespeichert werden. Berücksichtigt wurde hier zumindest meine Forderung nach einem klarstellenden Hinweis, dass die Lichtbilder nur mit Kenntnis der Gefangenen aufgenommen werden dürfen.

Nach § 86a Abs. 2 StVollzG dürfen die Lichtbilder von Justizvollzugsbediensteten genutzt werden, wenn eine Überprüfung der Identität der Gefangenen im Rahmen ihrer Aufgabenwahrnehmung erforderlich ist. Die Bilder dürfen zudem sowohl an die Polize ivollzugsbehörden des Bundes und der Länder, soweit dies zu r Abwehr einer gegenwärtigen Gefahr für erhebliche Rechtsgüter innerhalb der Anstalt erforderlich ist als auch an die Vollstreckungs- und Strafverfolgungsbehörden, soweit dies für Zwecke der Fahndung und Festnahme eines entwichenen oder sich sonst ohne Erlaubnis außerhalb der Anstalt aufhaltenden Gefangenen erforderlich ist, übermittelt werden. In Abstimmung mit den Datenschutzbeauftragten der Länder hatte ich hierzu – leider vergeblich – gefordert, zumindest eine Bestimmung einzufügen, die einen Schutz vor unbefugten Zugrif fen auf die Lichtbilddatei gewährleistet, z. B. durch eine umfassende Protokollierung der Abrufe und der mit ihnen verfolgten Zwecke, sowie eine Regelung für die or ganisatorische und funktionelle Trennung der Protokolldaten von sonstigen Unterlagen über die Gefangenen, insbesondere der Gefangenenpersonalakten, vorzusehen.

Nach der bisherigen Rechtslage durften aufgrund des § 180 Abs. 5 Satz 1 Nr. 1 StVollzG die Strafvollzugsbehörden u. a. den Finanzbehörden nur Auskunft darüber erteilen, ob sich eine bestimmte Person in Haft befindet, sowie ob und gegebenenfalls wann voraussichtlich ihre Entlassung innerhalb eines Jahres bevorsteht. Mit dem Gesetz wurde nun auch eine gesetzliche Grundlage zur Übermittlung von personenbezogenen Daten durch die V ollzugsbehörde an Finanzbehörden zur Durchführung der Besteuerung geschaffen. Dies halte ich für nicht unproblematisch. W eshalb die Durchsetzung steuerrechtlicher Forderungen gegenüber anderen Forderungen privilegiert sein soll, obwohl die bisherige Rechtslage nicht zu ersichtlichen Unzuträglichkeiten bei der Geltendmachung von Forderungen gegen Strafgefangene geführt hat, leuchtet mir nicht ein.

8.7 Novelle des Bundeszentralregistergesetzes

Das Vierte Gesetz zur Änderung des Bundeszentralregistergesetzes (BZRG) ist weite stgehend am 30. April 2002 in Kraft getreten (BGBl. I S. 1406). Über die Arbeiten zur Novellierung des BZRG habe ich bereits in meinen letzten Tätigkeitsberichten informiert (vgl. 18. TB Nr . 6.11.1). In die intensiven Beratungen wurde ich regelmäßig eingebunden; so sind in den Gesetzentwurf auch zahlreiche meiner Forderungen eingeflossen. Allerdings hat der Bundesrat im Gesetzgebungsverfahren mehrere Änderungsvorschläge unterbreitet, die u. a. auf eine Ausweitung des Kreises der Behörden mit unbeschränktem Auskunftsanspruch aus dem Bundeszentralregister hinausliefen. Dies wurde von mir immer kritisch beurteilt. Eine vollständige Kenntnis der V orstrafen eines Bür gers ist nur ausnahmsweise erforderlich. Daher ist bereits bei der Auswahl der auskunftsberechtigten Stellen und der entsprechenden Zweckbestimmung wegen des damit verbundenen Eingrif fs in das informationelle Selbstbestimmungsrecht restriktiv vorzugehen. Auch der Gesetzgeber ist im BZRG bislang so verfahren, wie etwa an den unterschiedlichen Formen des Führungszeugnisses und deren Behandlung erkennbar wird (vgl. auch 17. TB Nr. 6.9). Zwar sind meine Bedenken und die der Datenschutzbeauftragten der Länder auch in die Gegenäußerung der Bundesregierung zur Stellungnahme des Bundesrates mit eingeflossen. Auf der Grundlage der Beschlussempfehlung des angerufenen Vermittlungsausschusses wurden aber dennoch zwei Änderungsvorschläge des Bundesrates in das Gesetz übernommen:

– Im BZRG war bisher in § 20 Abs. 3 Satz 1 geregelt, dass Auskunft über Eintragungen, die mit einem Sperrvermerk versehen sind, weil der Betroffene schlüssig dargelegt hat, dass die Eintragung unrichtig ist, nur einem Strafgericht oder einer Staatsanwaltschaft für ein Strafverfahren gegen den Betroffenen oder den in § 41 Abs. 1 Nr. 3 genannten Behörden (Geheimdiensten) erteilt wird. Die Auskunftserteilung wurde durch die Novellierung erweitert und sieht nunmehr eine Übermittlung an die in § 41 Abs. 1 Nr . 1, 3 bis 5 genannten Stellen (Gerichte, Geheimdienste, Finanzbehörden, Polizei) vor.

– Die unbeschränkte Auskunft aus dem Bundeszentralregister wird nach der Erweiterung des § 41 Abs. 1 Nr. 9 BZRG nunmehr auch Behörden eingeräumt, die über Erlaubnisse zum Halten gefährlicher Hunde entscheiden müssen.

8.8 Zentrales Staatsanwaltschaftliches Verfahrensregister

Der Betrieb des länderüber greifenden Zentralen Staatsanwaltschaftlichen Verfahrensregisters (ZStV) wurde – wie im 18. TB berichtet (Nr. 6.11.3) – im Frühjahr 1999 aufgenommen. Inzwischen ist die weit überwiegende Mehrheit der Staatsanwaltschaften an das Register angeschlossen, ebenso wie andere berechtigte Benutzer (Bundesamt für Verfassungsschutz und einige Landesämter für Verfassungsschutz). Das Register umfasst derzeit ca. 7,65 Mio. Datensätze. Der endgültige Bestand soll sich auf rund 30 Mio. Datensätze belaufen.

Die Daten vom und zum Register werden im ISDN-Netz (in einer geschlossenen Benutzer gruppe) sowie im TEST A-Overlaynetz der Deutschen T elekom AG übermittelt, bei dem nicht zuletzt auf mein Drängen hin eine zusätzliche Leitungsverschlüsselung eingerichtet wurde. Leider wurde jedoch noch immer nicht die notwendige „Ende-zu-Ende-Verschlüsselung“ realisiert. Ursprünglich war hierzu geplant, Produkte zu verwenden, die eine Verschlüsselung auf Basis des MailTrusT-Standards ermöglichen. Nachdem sich dies aus technischen Gründen nicht umsetzen ließ, wurde seitens des Bundeszentralregisters der V orschlag gemacht, ein so genanntes V irtuelles Privates Netz (VPN) einzusetzen, das den gesamten Datenverkehr hinreichend sicher verschlüsselt. Dieser Vorschlag fand meine Zustimmung, harrt jedoch noch immer der Umsetzung, die hof fentlich in nächster Zukunft erfolgen wird.

In meinem 18. TB habe ich auf einen kontrovers geführten Dialog mit dem BMJ zu Art und Inhalt der nach § 495 Strafprozessordnung (StPO) auf Antrag aus dem ZStV zu erteilenden Auskünfte hingewiesen. Umstritten war und ist nach wie vor, ob aus dem Register Auskünfte auch dann erteilt werden sollen, wenn dort keine Einträge vorhanden sind (so genannte Negativauskünfte). Vonseiten des BMJ und des ZStV wurde die Befürchtung geäußert, eine solcherart praktizierte Auskunftserteilung ermögliche eine Ausforschung des Registers. Sie führe dazu, dass jemand aus der Art der Auskunftserteilung auf das V orhandensein von Eintragungen schließen könne. W erde dem Anfragenden nämlich, etwa wegen Gefährdung des Untersuchungszwecks (§ 495 i. V. m. § 491 Abs. 2 S. 1 StPO), eine Auskunft verweigert, könne er daraus jedenfalls schließen, dass derzeit gegen ihn ermittelt werde, wodurch insbesondere im Bereich der Organisierten Kriminalität Ermittlungserfolge gefährdet werden könnten. Deshalb sei es nöt ig, Auskünfte generell nur über abgeschlossene oder de m Beschuldigten bereits bekannt gewordene Ermittlungsverfahren zu erteilen. Auch eine Negativauskunft müsse eine entsprechende Einschränkung enthalten.

Hiermit war ich nicht einverstanden, da das Gesetz ohne jede Einschränkung eine Einzelfallprüfung vorsieht. Außerdem könne von Ausforschungsgefahren schon aufgrund der jedenfalls bis dahin (Mitte des Jahres 2001) geringen Zahl der Anfragen nicht ausgegangen werden. Meinen Bedenken entsprechend hat das BMJ im Dezember 2001 das ZStV gebeten, Negativauskünfte ohne die genannten Beschränkungen zu erteilen, was erfreulicherweise auch nach wie vor geschieht.

Eine vom BMJ zu der Problematik im Jahr 2002 durchgeführte Länderumfrage hat allerdings er geben, dass die Landesjustizverwaltungen weiterhin die Gefahr einer Ausforschung des Registers sehen. Diese Befürchtung lässt sich zwar nicht durch Fakten belegen und auch das ZStV , das hierzu eigens eine Statistik führt, hat bisher keine konkrete Ausforschungsgefahr festgestellt; eine Umfrage er gab aber trotzdem, dass einige Staatsanwaltschaften wegen der genannten Bedenken dem zentralen Register keine Ermittlungsverfahren aus dem Bereich der Or ganisierten Kriminalität melden. Das führt dazu, dass das ZStV seine Funktion nicht ordnungsgemäß wahrnehmen kann. Bereits in der vergangenen Legislaturperiode wurde deshalb von Seiten der Länder vorgeschlagen, die Vorschrift des § 491 Abs. 2 StPO zu ändern (s. z. B. Entwurf eines Gesetzes zur V erbesserung des strafrechtlichen Instrumentariums für die Bekämpfung des Terrorismus und der Organisierten Kriminalität, Bundesratsdrucksache 1014/01), um den Auskunftsanspruch zu beschränken. Obwohl die Änderungsversuche scheiterten, ist das Thema noch nicht „vom Tisch“, denn es sind weitere Gesetzesinitiativen in diese Richtung zu erwarten.

Ich kann mich den vorgebrachten Bedenken gegen die Erteilung von Negativauskünften nicht gänzlich verschließen. Allerdings darf der Auskunftsan spruch im Falle des nicht abgeschlossenen Verfahrens nicht komplett gestrichen werden. Bei einer Gesetzesänderung muss vielmehr eine ausgewogene Lösung gefunden werden, die sowohl dem Interesse des Staates an einer wirk samen Strafverfolgung Rechnung trägt als auch dem Recht des Einzelnen darauf, zu wissen, ob und welche Daten über ihn gespeichert sind. Über den weiteren Fortgang der Diskussion werde ich berichten.

8.9 Eurojust – europäische Zusammenarbeit der Justiz

Auf der Grundlage einer V ereinbarung des Europäischen Rates in Tampere im Herbst 1999 wurde mit dem Beschluss des Rates der Europäischen Union vom 28. Februar 2002 über die „Errichtung von Eurojust zur V erstärkung der Bekämpfung der schweren Kriminalität“ eine neue, mit eigener Rechtspersönlichkeit au sgestattete Einrichtung der Europäischen Union geschaffen. Diese Einrichtung soll insbesondere im Zusammenwirken mit dem Europäischen Justiziellen Netz und Europol dazu dienen, die justizielle Zusammenarbeit zwischen den Mitgliedsstaaten zu verbessern, vor allem bei der Bekämpfung der schweren bzw . Organisierten Kriminalität.

Eurojust soll u. a. die Koordinierung der nationalen Staatsanwaltschaften fördern und die Erledigung von internationalen Rechtshilfe- und Auslieferungsersuchen erleichtern, wenn Ermittlungen und Strafverfolgungsmaßnahmen bei bestimmten Delikten der schweren bzw . Organisierten Kriminalität (z. B. Delikte aus dem Bereich des T errorismus, des illegalen Drogenhandels, der Computerkriminalität) zwei oder mehr Mitgliedsstaaten betref fen. Ermittlungskompetenzen besitzt Eurojust dagegen nicht. Es kann in diesem Bereich allenfalls unterstützend tätig werden.

Bei den Beratungen zur Einrichtung von Eurojust war ich von Beginn an beteiligt. Ich habe frühzeitig darauf hingewiesen,

dass im Hinblick auf die se nsiblen personenbezogenen Daten, die von Eurojust erhoben, verarbeitet und genutzt werden, und angesichts der eigenen Rechtspersönlichkeit dieser Einrichtung die Notwendigkeit von umfassenden Datenschutzvorschriften besteht. Im Laufe der Beratungen konnte ich die Anforderungen im Detail formulieren. Diese wurden durch eine Entschließung der Datenschutzbeauftragten des Bundes und der Länder anlässlichihrer 62. Konferenz im Oktober 2001 nochmals bekräftigt (s. Anlage 20).

Einigen Forderungen wurde im Beschluss über die Errichtung von Eurojust erfreulicher W eise entsprochen. So sind beispielsweise Regelungen zur Sperrung von Daten und zur Datensicherheit in den Beschluss aufgenommen worden. Als Erfolg ist weiterhin zu werten, dass Betroffene grundsätzlich einen Auskunftsanspruch über die sie betreffenden personenbezogenen Daten haben. Die geforderte Abwägung der gegenläufigen Interessen bei der Entscheidung, ob Auskunft erteilt wird, entfällt allerdings, wenn über den Auskunftsuchenden keinerlei Daten bei Eurojust vorhanden sind. Hier wird nur pauschal mitgeteilt, dass eine Überprüfung stattgefunden habe, ohne dass der Antragsteller hieraus entnehmen kann, ob zu seiner Person Daten vorliegen. Aus meiner Sicht ist diese Regelung im Hinblick auf die Zuständigkeit von Eurojust für Delikte der schweren bzw. Organisierten Kriminalität und mit Rücksicht auf die dem Antragsteller eingeräumte Beschwerdemöglichkeit noch akzeptabel. Besonders hervorzuheben ist ferner, dass eine gemeinsame Kontrollinstanz geschaffen wurde, deren Entscheidungen bindenden Charak ter haben. Diese Instanz wird sich, anders als etwa die entsprechende Einrichtung bei Europol, aus Richtern oder Personen, die aufgrund des ihnen verliehenen Amtes eine vergleichbare Unabhängigkeit besitzen, zusammensetzen. Diese Regelung wurde – vor allem auf französische Initiative – zur W ahrung der Unabhängigkeit von Eurojust als einer justiziellen Stelle getroffen (sie besteht aus Richtern, Staatsanwälten oder Polizeibeamten mit gleichwertigen Befugnissen).

Negativ zu vermerken ist demg egenüber u. a., dass der Katalog der personenbezogenen Daten, die verarbeitet werden dürfen, relativ weit gefasst ist und die Aufnahme einer Öf fnungsklausel – wenn auch stark eingeschränkt – nicht vermieden werden konnte. Auch richtet sich die jeweilige Speicherungsfrist bedauerlicher Weise nicht nach der Frist des Mitgliedstaates, in dem sie am kürzesten ist (eine Umgehung der nationaler Löschungsfristen wäre so vermieden worden), sondern nach derjenigen, die am längsten ist.

Insgesamt bin ich jedoch mit den in den Beschluss aufgenommenen datenschutzrechtlichen Regelungen zufrieden. Ich möchte allerdings daran erinnern, dass innerstaatlich noch Rechtsetzungsbedarf best eht, insbesondere im Hinblick auf Auskünfte an Eurojust über strafrechtliche Ermittlungsverfahren sowie Auskünfte aus dem länderübergreifenden Zentralen Staatsanwaltlichen V erfahrensregister (vgl. auch Nr. 8.8). Hier müssen entsprechende Ermächtigungsgrundlagen geschaffen werden.

8.10 Elektronischer Rechtsverkehr

8.10.1 Elektronischer Rechtsverkehr – Eine neue Herausforderung für die Justiz

Auch die Justiz will sich für elektronische Kommunikationsformen öffnen. Die Justizministerien des Bundes und der Länder versprechen sich von de r Möglichkeit, elektronisch mit den Gerichten zu kommunizieren, nicht zuletzt einen erheblichen Kostenvorteil für die Zukunft.

Elektronische Klageerhebungen sind im Bereich der Finanzgerichtsbarkeit bereits seit August 1999 möglich, als das Finanzgericht Hamburg einen Feldversuch zum elektronischen Rechtsverkehr begann. Ei n weiterer Feldversuch wird beim Finanzgericht Brandenburg durchgeführt. Die 70. Konferenz der Justizministerinnen und -minister (Justizministerkonferenz) hatte am 7./9. Juni 1999 die Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz (Bund-Länder-Kommission) beauftragt zu prüfen, unter welchen rechtlichen Voraussetzungen die Justiz für den elektronischen Geschäftsverkehr geöffnet werden kann und welche gesetzgeberischen Schritte hierfür erforderlich sind. Dabei sollte der Eröffnung des elektronischen Geschäftsverkehrs mit den Register gerichten Priorität eingeräumt werden. Die Bund-Länder -Kommission ihrerseits setzte eine Arbeitsgruppe Elektronischer Rechtsverkehr und eine weitere Arbeitsgruppe ein, die si ch mit dem elektronischen Rechtsverkehr in den Fachgerichtsbarkeiten des öf fentlichen Rechts befasste. Im Berichtszeitraum hat die Bund-Länder-Kommission der Justizministerkonferenz ihren Abschlussbericht vorgelegt. Auf dessen Grundlage hat die Justizministerkonferenz auf ihrer 72. Konferenz im Juni 2001 die Bundesministerin der Justiz gebeten, in Zusammenarbeit mit den Ländern die Erforderlichkeit von Rechtsgrundlagen zur Einführung einer elektronischen Kommunikation und Aktenführung zu prüfen und ggf . zu schaf fen. Auf ihrer 73. Konferenz im Juni 2002 be schloss sie er gänzend, die ebenfalls erarbeiteten organisatorisch-technischen Leitlinien für den elektronischen Rechtsverkehr mit den Gerichten und Staatsanwaltschaften dem Bund und den Ländern als Grundlage für den Erlass von Rechtsverordnungen zur Einführung und zur Anwendung des elektronischen Rechtsverkehrs zu empfehlen.

Besonders erfreulich war in diesem Zusammenhang, dass der Abschlussbericht der Bund-Länder -Kommission auch dem Arbeitskreis Justiz (AK Justiz) der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Datenschutzkonferenz) vorgestellt und fachkundig erläutert wurde. Dieser hat unter meiner Federführung daraufhin eine eigene Arbeitsgruppe Elektronischer Rechtsverkehr eingesetzt, die die Entwicklung in diesem Bereich in den nächsten Jahren aus datenschutzrec htlicher Sicht konstruktiv begleiten wird.

Der Begriff Elektronischer Rechtsverkehr ist weit zu fassen. Er reicht von der Einreichung von Schriftsätzen bei Gericht durch die Verfahrensbeteiligten mithilfe elektronischer Medien, über die Führung elektronischer V erfahrensakten, den Einsatz von V ideotechnik in der mündlichen V erhandlung (zur Einführung der V ideotechnik im Strafprozess siehe meinen 17. TB Nr. 6.5 und im finanzgerichtlichen Verfahren meinen 18. TB Nr. 6.14) bis hin zum Abruf und zur Versendung gerichtlicher Entscheidungen (prozessleitender V erfügungen und Beschlüsse, Urteile etc.) auf elektronischem Wege, einschließlich des Zugangs zu den Datenbanken der Registergerichte.

Gesetzliche Grundlage für die Möglichkeit, Schriftsätze auf elektronischem Wege an ein Gericht zu übermitteln, ist die mit dem Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer V orschriften an den modernen

Rechtsgeschäftsverkehr vom 13. Juli 2001 (BGBl. I S. 1542) in die Prozessordnungen und gerichtlichen Verfahrensgesetze aufgenommene Ermächtigung der Bundesregierung und der Landesregierungen, für ihren jeweiligen Bereich den Zeitpunkt zu bestimmen, von dem an elektronische Dokumente bei den Gerichten eingereicht werden können, und welches die für die Bearbeitung dieser Dokumente geeignete Form ist (§ 130a Zivilprozessordnung, § 46b Arbeitsgerichtsgesetz, § 108a Sozialgerichtsgesetz, § 86a Verwaltungsgerichtsordnung, § 77a Finanzgerichtsordnung, § 21 Gesetz über die freiwillige Gerichtsbarkeit, §§ 73 Abs. 2 und 81 Abs. 3 Grundbuchordnung). Als erstes Land hat Hamburg mit der Verordnung über den elektronischen Rechtsverkehr in gerichtlichen Verfahren vom 9. April 2002 (HmbGVBl. S. 41) von der in § 77a Finanzgerichtsordnung enthaltenen gesetzlichen Ermächtigungsgrundlage Gebrauch gemacht und ab dem 1. Mai 2002 die Einreichung von elektronischen Dokumenten – also Schriftsätzen und Klagen – beim Finanzgericht Hamburg gesetzlich zugelassen.

Auch an den Bundesgerichten ist ein Anfang dieser Entwicklung zu verzeichnen. So habe ich mich beim Bundesgerichtshof über die dort aufgrund der Verordnung über den elektronischen Rechtsverkehr beim Bundesgerichtshof vom 26. November 2001 (BGBl. I S. 3225) geschaffene Möglichkeit informiert, Verfahren bei einem Bundesgericht auf elektronischem Wege zu führen. Dort erstreckt sich die Möglichkeit, Revisionsverfahren elektronisch zu führen, zunächst nur auf wenige der beim Bundesgerichtshof zugelassenen Rechtsanwälte. Ich rechne damit, dass sich diese Form der Prozessführung relativ schnell durchsetzen wird. Desto wichtiger ist es aus datenschutzrechtlicher Sicht im Hinblick auf die Übermittlung sehr sensibler personenbezogener Daten auf elektronischem Wege zwischen den Prozessbeteiligten – wie z. B. in Ehescheidungsverfahren, deren elektronische Abwicklung derzeit bei einem niedersächsischen Amtsgericht getestet wird –, möglichst frühzeitig bei der Einführung dieser neuen prozessualen Möglichkeiten beteiligt zu werden. Umso mehr begrüße ich, dass bei der Entwicklung der technischen Systeme sehr viel Wert auf Sicherheit gelegt wurde.

Ein wesentlicher Aspekt des elektronischen Rechtsverkehrs ist die Möglichkeit, elektronisch auf die Datenbanken der Registergerichte zugreifen zu können, was alle bei Gerichten geführten Register umfasst. Es geht dabei nicht nur um die Möglichkeit, aus diesen Registern im automatisierten Verfahren Informationen abrufen zu können, sondern auch darum, bestimmte Register über das Internet allgemein zur Verfügung zu stellen. Wegen der unterschiedlichen Zielrichtung und der unterschiedlichen Berechtigung, Informationen aus den bei den Gerichten vorhandenen Registern abzurufen, ist es nicht möglich, einheitlich für alle Register geltende Bestimmungen zu finden. Im Berichtszeitraum sind bereits gesetzliche Regelungen getroffen worden, um entsprechende automatisierte Abrufe aus dem Handelsregister (§§ 9 und 9a Handelsgesetzbuch), dem Vereinsregister (§ 79 BGB) und dem Schuldnerverzeichnis (§ 9 Insolvenzordnung, s. hierzu Nr. 10.7) zu ermöglichen. Gesetzesänderungen für die anderen bei den Gerichten geführten Register werden folgen.

Ich werde die Entwicklung verfolgen und darüber weiter berichten.

8.10.2 Zugang der Bürger zum Rechtsverkehr mit den Behörden

Nachdem mit dem Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 13. Juli 2001 (BGBl. I S. 1542) die Möglichkeit geschaffen worden ist, im Zivilrecht verbindliche Rechtserklärungen – z. B. zum Abschluss eines Vertrages – in elektronischer Form abzugeben, bestand diese Möglichkeit im öffentlichen Recht zunächst nicht. Das „Dritte Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften“ vom 21. August 2002 (BGBl. I S. 3322) eröffnet nunmehr die elektronische Kommunikation zwischen Bürger und Verwaltung. Es ist – mit Ausnahme von steuerrechtlichen Vorschriften, die bereits ab dem 1. September 2002 galten – am 1. Februar 2003 in Kraft getreten.

Zentrale Regelung ist dabei der neue § 3a des Verwaltungsverfahrensgesetzes (VwVfG), der die Übermittlung elektronischer Dokumente zwischen Bürger und Verwaltung erlaubt, „soweit der Empfänger hierfür einen Zugang geschaffen hat“. Die Bundesregierung hat in der Begründung zu dieser Vorschrift (Bundestagsdrucksache 14/9000 S. 30 f.) deutlich hervorgehoben, dass nur dann, wenn eine Behörde, ein Unternehmen oder ein Rechtsanwalt – d. h. Institutionen, die berufsmäßig am Rechtsverkehr teilnehmen – eine E-Mail-Adresse angeben, damit konkludent die Bereitschaft erklärt wird, auf diesem Wege Dokumente und Erklärungen anzunehmen. Diese Institutionen haben in diesem Fall den Empfang elektronischer Post durch organisatorische Maßnahmen sicherzustellen, z. B. dadurch, dass ihre E-Mail-Postfächer regelmäßig abgefragt werden. Will eine Institution trotz Angabe ihrer E-Mail-Adresse Erklärungen nicht elektronisch annehmen, muss sie dies auf ihrer Internetseite oder in ihrem Schreiben an die Behörde ausdrücklich erklären. Etwas anderes gilt für den Bürger. Bei ihm kann noch nicht davon ausgegangen werden, dass er mit der Angabe seiner E-Mail-Adresse in einem Schreiben an eine Behörde sein Einverständnis erklärt, von dieser auf elektronischem Wege eine rechtlich verbindliche Erklärung, z. B. einen Verwaltungsakt, zu erhalten. Der Bürger muss daher der Behörde gegenüber ausdrücklich erklären, dass er mit diesem Verfahren einverstanden ist. Ich hätte es begrüßt, wenn der Gesetzgeber nicht nur in der Begründung, sondern im Gesetzestext selbst ausdrücklich die Einwilligung des Bürgers in die elektronische Übermittlung von Dokumenten vorgesehen hätte.

Ebenfalls hätte ich es begrüßt, wenn in § 37 Abs. 4 VwVfG eine Regelung aufgenommen worden wäre, wonach ein Verwaltungsakt, dessen Erlass und Gültigkeit dauerhaft nachweisbar sein muss, nur dann in elektronischer Form erlassen werden darf, wenn sicher gestellt ist, dass der Inhalt des elektronischen Dokuments dauerhaft lesbar und die nach § 3a Abs. 2 VwVfG erforderliche digitale Signatur dauerhaft überprüfbar ist. Dies gilt für Verwaltungsakte wie z. B. einer Gewerbeuntersagung. Dabei sehe ich es als besonders problematisch an, dass bei digitalen Signaturen nach dem derzeitigen Stand der Technik der Sicherheitswert durch Zeitablauf geringer wird (§ 6 Abs. 1 Satz 2 Signaturgesetz). Die digitale Signatur müsste daher von Zeit zu Zeit erneuert, d. h. durch eine andere ersetzt werden. Wie und ob das in der Praxis funktioniert, muss sich erst noch zeigen. Insbesondere hätte im Gesetzestext vorgesehen werden sollen,

dass die Erneuerung der digitalen Signatur in den Verantwortungsbereich der erlassenden Behörde fällt.

Neben dem Verwaltungsverfahrensgesetz wurden mit dem Gesetz vom 21. August 2002 auch das Verwaltungsverfahren bei den Sozialleistungsträgern (Erstes und Zehntes Buch Sozialgesetzbuch) und der Finanzverwaltung (Abgabenordnung) sowie weitere Gesetze mit verwaltungsverfahrensrechtlichen Vorschriften angepasst. Der Gesetzgeber hat hier sicherlich Neuland betreten.

8.11 Veröffentlichung von Gerichtsentscheidungen

In meinem 9. TB (S. 20 Nr. 4.3) habe ich mich bereits einmal mit der Frage befasst, inwieweit Verfahrensbeteiligte bei der Veröffentlichung von Gerichtsentscheidungen hinnehmen müssen, dass damit gegebenenfalls auch personenbezogene Daten über sie bekannt gemacht werden. Anlässlich einer Eingabe aufgrund der Veröffentlichung eines Beschlusses des Bundesgerichtshofs habe ich mich erneut, diesmal auf der Grundlage eines Urteils des Bundesverwaltungsgerichts, eingehend damit auseinandergesetzt. Der Beschluss des Bundesgerichtshofs hatte aus Gründen der Verständlichkeit der Entscheidung insbesondere die Funktion eines Verfahrensbeteiligten einschließlich der Art der Beschäftigungsstelle genannt und durch die notwendige Auseinandersetzung mit einem Gesetz des betreffenden Bundeslandes für kundige Leser letztlich erkennen lassen, wer die in Frage stehende Person ist.

Ausgangspunkt meiner Bewertung war ein neueres Urteil des Bundesverwaltungsgerichts. Dieses hat in seiner Entscheidung vom 26. Februar 1997 (BVerwGE 104, 106 = NJW 1997, 2694) die Bedeutung der Veröffentlichung der maßgeblichen Entscheidungen als eine Aufgabe der Gerichte herausgestellt, die sich aus dem Rechtsstaatsgebot einschließlich der Justizgewährungspflicht, dem Demokratiegebot und auch aus dem Grundsatz der Gewaltenteilung ergibt. Dabei hat das Gericht auch auf die Notwendigkeit der Anonymisierung der Entscheidungen hingewiesen.

Hieraus ergibt sich zunächst, dass eine Entscheidung nicht ohne weiteres veröffentlicht werden darf, wenn sie im Hinblick auf ihre Verständlichkeit nicht anonymisiert werden kann. Auch wenn eine Veröffentlichung nach dem Wortlaut von § 16 Abs. 1 Nr. 1 i. V. m. § 14 Abs. 1 Satz 1 BDSG zulässig wäre, darf dies dann nicht geschehen, wenn die darin liegende Schwere des Eingriffs in das informationelle Selbstbestimmungsrecht des Betroffenen außer Verhältnis zu dem mit der Veröffentlichung der Entscheidung verfolgten öffentlichen Interesse steht. Dies kann der Fall sein, wenn es in einer Entscheidung ausnahmsweise nur um die Lösung rein individueller Probleme des Einzelfalles geht. Ebenso bedarf aber die Zulässigkeit der Veröffentlichung einer besonders sorgfältigen Prüfung, wenn sich eine Entscheidung aus Verständnisgründen nicht anonymisieren lässt, andererseits aber nachteilige Informationen über einen Betroffenen enthält, wie z. B. Strafurteile.

Unter diesen Gesichtspunkten unterfällt der vom Bundesgerichtshof entschiedene Sachverhalt den tragenden Entscheidungsgründen des Urteils des Bundesverwaltungsgerichts. Ich habe daher keine Einwendungen gegen die Veröffentlichung dieses Falls erhoben. Insgesamt gehe ich davon aus, dass die Gerichte bei den seltenen Fällen nicht anonymisierbarer Entscheidungen neben der wichtigen Aufgabe zur Veröffentlichung ebenso die schutzwürdigen Interessen der Betroffenen berücksichtigen und prüfen, ob nicht im Einzelfall hierauf zu verzichten ist.

9 Finanzwesen

9.1 Datenschutzgerechte Änderung der Abgabenordnung auf dem Weg

In meinem 18. TB (Nr. 7.2) habe ich über Gespräche mit dem BMF zur datenschutzrechtlichen Verbesserung der Abgabenordnung berichtet. Angesichts der Bedeutung, die einer datenschutzgerechten Ausgestaltung der Abgabenordnung zukommt, hat der Deutsche Bundestag in seiner Entschließung zum 18. TB ausdrücklich erklärt, dass er das BMF in seinem Bemühen, den datenschutzrechtlichen Regelungsbedarf der Abgabenordnung zu ermitteln, unterstützt und erwartet, dass die hierbei als notwendig erkannten datenschutzrechtlichen Regelungen in der nächsten Legislaturperiode getroffen werden (Empfehlungen des Innenausschusses, Bundestagsdrucksache 14/9490 vom 18. Juni 2002, Plenarprotokoll 14/248 der 248. Sitzung am 4. Juli 2002, S. 25174).

Inzwischen habe ich dem BMF ausführliche, mit den Landesbeauftragten für den Datenschutz abgestimmte Lösungsvorschläge zu den bereits im 18. TB genannten und zu weiteren Schwerpunkten, wie z. B. der zwischenstaatlichen Rechts- und Amtshilfe und zu Kontrollmitteilungen, zugeleitet. Dieser Katalog von Vorschlägen wurde in einer hierfür eingerichteten Koordinierungsrunde, an der unter Vorsitz des BMF Vertreter einiger Finanzressorts der Länder sowie von Landesbeauftragten für den Datenschutz beteiligt waren, gründlich diskutiert. Hierbei konnte ich erkennen, dass die Finanzverwaltung ernsthaft bemüht ist, den datenschutzrechtlichen Regelungsbedarf zur Ergänzung der Abgabenordnung zu prüfen und eine unter Berücksichtigung der steuerlichen Belange angemessene Lösung zu erreichen. Das BMF wird nunmehr auf der Grundlage des Besprechungsergebnisses Formulierungsvorschläge zur Ergänzung der Abgabenordnung ausarbeiten und mit den Finanzressorts der Länder abstimmen. Anschließend sollen diese in der bereits erwähnten Koordinierungsrunde erörtert werden. Ich würde es begrüßen, wenn auf dem jetzt eingeschlagenen Weg in absehbarer Zeit eine aus datenschutzrechtlicher Sicht zufrieden stellende Fassung der Abgabenordnung erreicht werden könnte.

9.2 Bekämpfung des Umsatzsteuerbetrugs schränkt Datenschutz ein

Mit dem Gesetz zur Bekämpfung von Steuerverkürzungen bei der Umsatzsteuer und zur Änderung anderer Steuergesetze (Steuerverkürzungsbekämpfungsgesetz – StVBG; BGBl. 2001 I S. 3922) soll den Finanzbehörden ermöglicht werden, dem Umsatzsteuerbetrug in Form so genannter Karussellgeschäfte besser zu begegnen. Bei diesen wirken mehrere Unternehmer zusammen, in der Absicht, die Möglichkeit des Vorsteuerabzugs missbräuchlich ausnutzen. Die bisher aufgedeckten betrügerischen Aktivitäten bewegen sich häufig in Größenordnungen mehrstelliger Millionenbeträge (s. Gesetzesbegründung in Bundestagsdrucksache 14/6883 S. 7). Besondere Aufmerksamkeit aus der Sicht des Datenschutzes erfordern die in dem StVBG geregelte Umsatzsteuer-Nachschau ohne Ankündigung und die dort festgelegte

Verpflichtung der Unternehmer, ihre Steuernummer auf der Rechnung anzugeben.

9.2.1 Umsatzsteuer-Nachschau ohne vorherige Ankündigung

Die Finanzbehörden haben durch das StVBG mit einem neuen § 27b des Umsatzsteuergesetzes (UStG) die Möglichkeit erhalten, ohne Ankündigung und außerhalb einer Außenprüfung Grundstücke und Räume von Personen, die eine gewerbliche oder berufliche Tätigkeit selbstständig ausüben, während der Geschäfts- und Arbeitszeiten zu betreten, um Sachverhalte festzustellen, die für die Besteuerung erheblich sein können (Umsatzsteuer-Nachschau). Der Vorschlag einer Nachschau ohne Ankündigung war zunächst im Referentenentwurf des BMF und auch noch in dem Regierungsentwurf für den Deutschen Bundestag allgemein als Regelung eines neuen § 88b Abgabenordnung – AO für alle Steuerarten vorgesehen.

Hiergegen wandte ich mich zunächst in den Beratungen mit dem BMF und später in einem Schreiben an die Vorsitzende des Finanzausschusses des Deutschen Bundestages, in dem ich darauf hinwies, dass eine solche Maßnahme eine unangemessene und unverhältnismäßige Belastung des rechtstreuen Steuerpflichtigen darstellt. Dies galt umso mehr, als der Vorschlag jeweils nur mit dem Ziel einer wirksamen Bekämpfung des Umsatzsteuerbetrugs begründet wurde. Ich konnte schließlich erreichen, dass die Möglichkeit einer unangekündigten Nachschau vom Gesetzgeber in § 27b UStG allein für den Bereich der Umsatzsteuer geregelt wurde.

Angesichts der außerordentlichen Höhe der Schäden durch Umsatzsteuerbetrug erscheint es grundsätzlich vertretbar, für die Finanzbehörden die Möglichkeit zu schaffen, Unternehmen ohne Ankündigung zu kontrollieren. Meiner Empfehlung, die Geltung der Vorschrift zeitlich zu befristen, damit Wirksamkeit und Verhältnismäßigkeit der Maßnahme nach angemessener Zeit gewissermaßen „automatisch“ überprüft werden müssen, wurde zwar nicht entsprochen. Der Finanzausschuss hat aber die Bundesregierung aufgefordert, zu dem StVBG „nach zwei Jahren einen Erfahrungsbericht vorzulegen, der insbesondere die datenschutzrechtlichen Tatbestände betrifft“ (Bundestagsdrucksache 14/7471 S. 7). Ich werde diesen Bericht aufmerksam prüfen.

9.2.2 Steuernummer auf der Rechnung des Unternehmers

Weiterhin schreibt das StVBG in einem neuen Absatz 1a des § 14 des UStG vor, dass der Unternehmer in seinen Rechnungen die ihm vom Finanzamt erteilte Steuernummer anzugeben hat. Diese Regelung war im Regierungsentwurf für das StVBG (Bundestagsdrucksache 14/6883) nicht enthalten und ist erst im Laufe der parlamentarischen Beratungen eingefügt worden (Bundestagsdrucksache 14/7471 S. 7). Im Rahmen der Anhörung zum Regierungsentwurf hatte ich zwar Gelegenheit, aufgrund einer entsprechenden Frage darauf hinzuweisen, dass eine solche Verpflichtung für die Unternehmen, die von Einzelpersonen gebildet werden, einer gesetzlichen Grundlage bedarf. Im Übrigen war ich an der Formulierung der Vorschrift aber leider nicht beteiligt.

Die Angabe der Steuernummer auf der Rechnung soll die Überprüfung der Lieferantenketten erleichtern und beschleunigen und so zur Bekämpfung des Umsatzsteuerbetrugs beitragen (Bundestagsdrucksache 14/7085 S. 1, s. auch Bundestagsdrucksache 14/7471 S. 7). Von der Notwendigkeit dieser Verpflichtung bin ich allerdings nicht überzeugt, da die Mitarbeiterinnen und Mitarbeiter der Finanzämter auch anhand der Anschrift des Unternehmens auf der Rechnung in der Regel in der Lage sein dürften, das zuständige Finanzamt schnell zu ermitteln.

Nach ihrem Wortlaut gilt die Vorschrift für alle Unternehmer. Mit dem BMF-Schreiben an die Obersten Finanzbehörden der Länder vom 28. Juni 2002 werden zwar z. B. Kleinunternehmer von der Verpflichtung zur Angabe der Steuernummer ausgenommen. Für mich ist jedoch nicht erkennbar, auf welche Weise etwa Rechtsanwälte oder Steuerberater – mit dem StVBG zu unterbindende – Karussellgeschäfte durchführen und so Umsatzsteuerbetrug begehen können. Es widerspricht dem Grundsatz der Verhältnismäßigkeit, wenn Unternehmer zur Angabe der Steuernummer verpflichtet werden, obwohl dies nach dem Zweck des Gesetzes nicht erforderlich ist. So könnte man auch daran denken, solche Unternehmer von dieser Verpflichtung auszunehmen, die nur Leistungen erbringen und keine Waren liefern, oder anstelle der für Kleinunternehmer maßgeblichen Grenze des § 19 UStG für den vorliegenden Zusammenhang eine höhere Grenze wählen, ab der die Verpflichtung zur Angabe der Steuernummer besteht. Auch sollte geprüft werden, die Verpflichtung zur Angabe der Steuernummer für die Fälle aufzuheben, in denen Rechnungen an Privatkunden ausgestellt werden, die nicht zum Vorsteuerabzug berechtigt sind. Ich habe das BMF hierzu und auch zur Frage der Notwendigkeit der Angabe der Steuernummer um Stellungnahme gebeten. Eine Antwort lag mir bei Redaktionsschluss noch nicht vor.

In Eingaben werden immer wieder Bedenken erhoben, Dritte könnten mit der Steuernummer bei den Finanzämtern Steuerdaten des Inhabers der Nummer erfragen. Das BMF hat mir hierzu mitgeteilt, die Beschäftigten der Finanzverwaltung seien verpflichtet, sich vor der Erteilung von Auskünften – insbesondere am Telefon – gerade im Hinblick auf die notwendige Wahrung des Steuergeheimnisses von der Berechtigung des Anfragenden zu überzeugen. Anhaltspunkt könne neben Detailkenntnissen des Anfragenden aus dem Steuervorgang auch die Steuernummer sein. Persönliche Kenntnis des Steuerpflichtigen oder ein Rückruf könnten Gewissheit verschaffen. Die Kenntnis der Steuernummer stelle bisher lediglich ein Indiz für die Identität des Anrufers dar. Alleinige Legitimationswirkung sei ihr bisher nicht zugekommen. Dies gelte in Zukunft erst recht. Ich gehe davon aus, dass die Mitarbeiterinnen und Mitarbeiter der Finanzämter dies beachten.

Neben der Umsatzsteuer-Nachschau werde ich aber auch diesen Punkt genau prüfen und gegebenenfalls gegenüber dem Finanzausschuss des Deutschen Bundestages aufgreifen. Ausgangspunkt hierfür wird sein, dass die Bundesregierung nach zwei Jahren ihren Bericht zu den Instrumenten des StVBG vorlegt (s. oben Nr. 9.2.1).

9.3 Steuernummer auf der Freistellungsbescheinigung bei Bauleistungen

Das Gesetz zur Eindämmung illegaler Betätigung im Baugewerbe (BGBl. 2001 I S. 2267, s. auch S. 3794) verpflich-

tet den Unternehmer, zur Sicherung von Steueransprüchen bei Bauleistungen von den Za hlungen für die ihm gegenüber erbrachten Bauleistungen einen Steuerabzug von 15 % vorzunehmen und diesen Betrag an das Finanzamt abzuführen (§§ 48, 48a Einkommensteuer gesetz – EStG). Der Erbringer der Bauleistung kann den Steuerabzug vermeiden, indem er dem Unternehmer eine von seinem Finanzamt ausgestellte Freistellungsbescheinigung vorlegt (§ 48b EStG). Darin ist neben dem Namen un d der Anschrift des jeweiligen Betriebes auch dessen Steuernummer anzugeben, die für die Nachfrage des Unternehmers beim Finanzamt wegen der Gültigkeit der Beschein igung (s.o. dazu) benötigt wird. Wie bei dem unter Nr . 9.2.2 behandelten Sachverhalt wurden auch hier von Petenten immer wieder Bedenken dagegen erhoben, dass Dritte, die durch V orlage der Freistellungsbescheinigung die Steuernummer erfahren, bei den Finanzämtern unbefugt die St euerdaten des Inhabers der Steuernummer erfragen können. Hierzu ist auf die unter Nr. 9.2.2 für einen insoweit gleichartigen Sachverhalt näher dargelegte Mitteilung des BMF zu verweisen, nach der die Beschäftigten der Finanzverw altung insbesondere im Hinblick auf die notwendige W ahrung des Steuergeheimnisses verpflichtet sind, sich von der Identität eines Anrufers zu überzeugen.

Der Unternehmer haftet für einen nicht oder zu niedrig abgeführten Steuerbetrag. Um sich daher von der Gültigkeit der ihm vorgelegten Freistellungsbescheinigung überzeugen zu können, wurde neben der Möglichkeit, hierzu bei dem zuständigen Finanzamt nachzu fragen, beim Bundesamt für Finanzen eine elektronische Datenbank eingerichtet (§ 48b Abs. 6 EStG). Dort hat der Unternehmer die Steuernummer desjenigen, auf den sich die Freistellungsbescheinigung bezieht, anzugeben. Sie ist erforderlich, um die in der Datenbank gespeicherte Bescheini gung aufzurufen. Eine bei der Abfrage auch anzugebende Sicherheitsnummer , die vom Finanzamt auf der Freistel lungsbescheinigung vermerkt wird, grenzt den Kreis der Abfragenden auf die Personen ein, denen die Freistellungsbe scheinigung vorgelegen hat. Nicht zuletzt gibt der Unternehmer seine eigene Steuernummer ein, um durch die vor gesehene Protokollierung seiner Anfrage im Interesse eines Haftungsausschlusses den Nachweis zu sichern, dass er sich über die Gültigkeit der Freistellungsbescheinigung vergewissert hat. Die Abfrage des Unternehmers und die ihm zugeleitete Antwort werden über eine sichere SSL-Verbindung verschlüsselt übertragen.

Insbesondere aufgrund der hier eingegangenen Eingaben habe ich mich über den Sachverhalt unterrichtet; ich sehe insoweit keine Bedenken. Lediglich wegen fehlender Löschungsfristen habe ich mich an das BMF gewandt. Es hat darauf hingewiesen, dass hi erzu Erfahrungen gesammelt werden müssten. Die Diskussion mit dem BMF dauert an.

9.4 „Riester-Rente“ erfordert datenschutzrechtliche Vorkehrungen

Die Voraussetzungen und das Verfahren für die als „Riester-Rente“ bekannt gewordene Alte rsvorsorgezulage wurden mit dem Gesetz zur Reform der gesetzlichen Rentenversicherung und zur Förderung eines kapitalgedeckten Altersvorsorgevermögens (Altersvermögensgesetz – A VmG; BGBl. 2001 I S. 1310) in einem neu in das Einkommensteuergesetz eingefügten Abschnitt „XI. Altersvorsor gezulage“ festgelegt. Notwendige Änderungen und Ergänzungen hierzu enthalten das Steueränderungsgesetz 2001 (StÄndG 2001; BGBl. 2001 I S. 3794), das V ersorgungsänderungsgesetz 2001 (BGBl. 2001 I S. 3926) und das Hüttenknappschaftliche Zusatzversicherungs-Neuregelungs-Gesetz (HZvNG; BGBl. 2002 I S. 2167).

Für den Aufbau einer zusätzlichen Altersversorgung werden Beiträge gefördert, die ein Anleger zugunsten eines auf seinen Namen lautenden, bestimmten Anforderungen entsprechenden Altersvorsorgevertrags mit einem Anbieter (z. B. Versicherungsunternehmen, Kreditinstitut) leistet. Gefördert werden aber auch Zahlungen aus dem Arbeitslohn, etwa an eine Pensionskasse, wenn di ese bestimmte Mindeststandards einhält. Soweit es für ihn günstiger ist, kann der Anleger seine Aufwendungen für di e zusätzliche Altersvorsorge stattdessen auch als Sondera usgaben beim Finanzamt geltend machen.

Die Zulagen werden durch die zentrale Stelle bei der Bundesversicherungsanstalt für Angestellte verwaltet. Sie erhält von dem Anbieter die bei dem Anleger erhobenen Daten, sie stellt vor allem die Berechtigung und die Höhe der Zulage fest und veranlasst deren Auszahlung an den Anbieter , der diese dem Anleger auf dessen Konto gutschreibt. Für die Überprüfung der Zulage und des Sonderausgabenabzugs übermitteln ihr die Träger der gesetzlichen Rentenversicherung, die Bundesanstalt für Ar beit, die Meldebehörden, die Familienkassen und die Finanzämter auf Anforderung die bei ihnen insoweit vorhandenen Daten. Die für die Besoldung oder die Amtsbezüge zust ändigen Stellen und in besonderen Fällen auch Arbeitgeber teilen der zentralen Stelle ebenfalls bestimmte Daten mit.

Insgesamt werden von den beteiligten Stellen für das Zulageverfahren in erheblichem Umfang Daten erhoben, verarbeitet und genutzt. Im Rahmen der Beratungen des Vermittlungsausschusses zum Altersvermögensgesetz zog das BMF daher zur Erörterung der erst zu diesem Zeitpunkt erarbeiteten Vorschriften für die Altersvorsor gezulage Mitarbeiter meines Hauses hinzu. Meine datenschutzrechtlichen Empfehlungen wurden in dem Entwurf berücksichtigt. Auch spätere ergänzende Regelungen insbesondere des HZvNG wurden mit mir abgestimmt.

Folgende Beispiele datenschutzrechtlich relevanter Regelungen seien genannt: Es wurde festgelegt, welche Arten von Daten der Anbieter beim Anleger zu erheben und an die zentrale Stelle zu übermitteln hat (§ 89 Abs. 2 Einkommensteuergesetz – EStG) und dass der Anbieter diese Daten nur für das Zulageverfahren verwerten darf (§ 96 Abs. 6 EStG). Damit die T räger der Rentenversicherung der zentralen Stelle dort vorhandene Sozialdaten der Anleger übermitteln können, bedurfte es u. a. einer Er gänzung des Zehnten Buchs Sozialgesetzbuch (§ 71 Abs. 1 Satz 1 Nr. 10 SGB X). Mit der Einrichtung der zentrale n Stelle als einer Finanzbehörde (§ 6 Abs. 2 Nr. 7 Abgabenordnung – AO) werden die ihr bekannt gewordenen Daten dem besonderen Schutz des Steuergeheimnisses unterstellt (§ 96 Abs. 1 EStG). Für den zur Überprüfung der Zulage und des Sonderausgabenabzugs erforderlichen Datenabgleich der zentralen Stelle wurde eine gesetzliche Grundlage geschaffen (§ 91 EStG). Eine ergänzende Rechtsverordnung re gelt vor allem Einzelheiten des vielfältigen Datenaustauschs zwischen beteiligten Stellen (Altersvorsorge-Durchführungsverordnung vom 17. Dezember 2002, BGBl. 2002 I S. 4544).

Das BMF hat sich bei diesem Vorhaben sehr darum bemüht, die datenschutzrechtlichen Erfo rdernisse zu berücksichtigen. Dies schließt nicht aus, dass im Hinblick auf den außerordentlich großen Umfang notwendiger Datenverarbeitung in der Praxis noch V erbesserungsbedarf sichtbar werden könnte. Ich werde das Vorhaben aufmerksam beobachten.

9.5 Unzulässige Offenbarung von Steuerdaten

Eine Petentin war bei einem öf fentlich-rechtlichen Kreditinstitut als technische Angest ellte beschäftigt und erhielt von diesem als Arbeitgeber Kindergeld. Aufgrund eines Erfassungsfehlers erhielt sie me hrere Jahre lang gleichzeitig auch von der Familienkasse des zuständigen Arbeitsamtes Kindergeld. Nachdem dieser Sachverhalt zwischen den beiden beteiligten Familienkassen bereits abschließend geklärt war, bat die Personalabteilung des Kreditinstitutes die Familienkasse des Arbeitsamtes im Hinblick auf eine beabsichtigte Kündigung des Arbeitsverhältnisses um Auskunft, für welchen Zeitraum Kindergeld von dort an die Petentin gezahlt worden war . Die Auskunft über diese dem Steuergeheimnis unterliegenden Angaben wurde erteilt.

Nach § 30 Abs. 4 Nr . 5 Abgabenordnung – AO ist die Offenbarung von Daten, die dem Steuergeheimnis unterliegen, gestattet, wenn hierfür ein zwingendes öffentliches Interesse besteht. Ein solches hätte bejaht werden können, wenn es um die Klärung des Sachverhaltes hinsichtlich der zu Unrecht doppelt verausgabten öf fentlichen Mittel gegangen wäre. Dies war aber gerade nicht der Fall, denn die Datenübermittlung diente ausschließ lich dazu, arbeitsrechtliche Maßnahmen gegen die Petentin zu ergreifen.

Das BMF sieht die Rechtfertigung für die Datenübermittlung in dem Interesse des Staates an dem Erhalt der Funktionsfähigkeit und der Integrität des öf fentlichen Dienstes. Ich bezweifele nicht, dass dieses Interesse ein erhebliches Gewicht hat und hierbei auch das V erhalten der Mitarbeiter innerhalb und außerhalb des öffentlichen Dienstes zu berücksichtigen ist. Angesichts der Tätigkeit der Petentin als technische Angestellte war nicht erkennbar, inwiefern ihr Verhalten die Funktionsfähigkeit des öf fentlichen Dienstes infrage gestellt hätte. Auch unter dem Aspekt der Integrität des Kreditinstitutes war im Hinblick auf die Stellung der Petentin innerhalb des Kreditinstitutes ein schwerer Nachteil im Sinne einer Schädigung des Ansehens des Kreditinstitutes nicht ersichtlich. Die Voraussetzung eines zwingenden öf fentlichen Interesses im Sinne des § 30 Abs. 4 Nr. 5 AO war somit nicht gegeben. Ich habe die unzulässige Datenübermittlung der Familienkasse an das Kreditinstitut daher als V erstoß gegen § 30 Abs. 1 und 2 Nr. 1 Buchstabe a) AO beanstandet.

9.6 Daten sind grundsätzlich beim Betroffenen zu erheben

Ein Petent wandte sich an mic h, da die für die Zahlung des Kindergeldes zuständige Fam ilienkasse des Arbeitsamtes bei dem Arbeitgeber seiner Tochter Daten erhoben hatte. Circa drei Monate vor Beendigung der Ausbildung seiner Tochter hatte der Petent der Familienkasse das voraussichtliche Ende der Ausbildung mitgeteilt. Unverzüglich nach dem erfolgreichen Bestehen der Abschlussprüfung seiner Tochter übersandte er der Familienkasse eine noch vor dem Prüfungstag ausgestellte Arbeitgeberbescheinigung. Hieraus ging noch nicht das Arbeitsentgelt der T ochter des Petenten für die Zeit ab Prüfungstag bis Ende des letzten Ausbildungsmonats hervor. Wegen dieser noch fehlenden Angabe wandte sich die Fam ilienkasse unmittelbar an den Arbeitgeber der Tochter des Petenten.

Eine Notwendigkeit für die Anfrage der Familienkasse bei dem Arbeitgeber der T ochter bestand nicht. Nach § 93 Abs. 1 Satz 3 Abgabenordnung – AO sollen andere Personen als die Beteiligten erst dann zur Auskunft angehalten werden, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziel führt ode r keinen Erfolg verspricht. Diese Voraussetzungen waren jedoch hier nicht gegeben. Der Petent ließ der Familienkasse alle erforderlichen Informationen zukommen, über die er bei Übersendung der Arbeitgeberbescheinigung verfügte. Die Familienkasse hatte keinen Anhaltspunkt dafür , dass der Petent die noch fehlende Information nicht beibringen würde. Die Familienkasse hätte sich daher zunächst an den Petenten wenden müssen. Ich habe die unzulässige Datenabfrage wegen V erstoßes gegen § 93 Abs. 1 Satz 3 AO beanstandet.

9.7 Angaben der Bundeswertpapierverwaltung in der Bescheinigung für das Finanzamt

Ein Petent hat mich gebeten, darauf hin zu wirken, dass ihm von der Bundeswertpapierverwaltung (BWpV) eine Zins- und Steuerbescheinigung ausgestellt wird, die nur die nach § 45a Abs. 2 Satz 1 Nr . 1 bis 5 Einkommensteuergesetz – EStG vorgeschriebenen Angaben enthält. In der dem Petenten ausgestellten Bescheinigung waren zusätzlich Informationen zum Wertpapier und Nennwert der Anlage sowie die Wertpapier-Kenn-Nummer angegeben. Die Bescheinigung war im Original dem Finanzamt vorzulegen und es bestand keine Möglichkeit, den Teil mit den amtlich vorgeschriebenen Angaben von den zusätzlichen Informationen abzutrennen. Zuvor hatte sich der Petent bereits vergeblich an die BWpV gewandt. Diese hatte sein Anliegen unter Hinweis auf ein im Bundessteuerblatt veröf fentlichtes Muster für maschinell erstellte Steuerbescheinigungen abgelehnt.

Nachdem ich den Sachverhalt mit dem BMF erörtert habe, wurde auch von diesem die Notwendigkeit einer Änderung beim Aufbau der Zins- und Steuerbescheinigung nach § 45a EStG anerkannt. Aufgrund eines er gänzenden BMF-Erlasses dürfen nunmehr in der Steuerbescheinigung ausschließlich die in § 45a Abs. 2 Satz 1 Nr. 1 bis 5 EStG amtlich vorgeschriebenen Angaben aufgeführt werden. Dem Petenten wurde daraufhin von der BWpV eine Steuerbescheinigung übersandt, die nur die gesetzlich vorgeschriebenen Angaben enthält. Die notwendigen Programmänderungen bei den automatisiert erstellten Steuerbescheinigungen wurden von der BWpV in die Wege geleitet.

9.8 Auskunftsersuchen von Finanzämtern an Telekommunikationsdiensteanbieter

In meinem 18. TB (Nr. 7.4) habe ich berichtet, dass Finanzämter bei Telekommunikationsdiensteanbietern Namen und Bankverbindungen von V ollstreckungsschuldnern – das sind Personen, gegen die sich ein V ollstreckungsverfahren nach § 249 Abgabenordnung (AO) richtet – erfragen. Derartige Auskunftsersuchen sind nach übereinstimmender Auffassung des BMWi, BMJ und mir nicht zulässig, wenn sie

sich nur auf § 93 AO beziehen, d. h. keinen Bezug zu einer Steuerstraftat oder Ordnungswidrigkeit erkennen lassen. Dies ergibt sich aus § 89 Abs. 6 Telekommunikationsgesetz – TKG, wonach Kundendaten nur unter den dort genannten Voraussetzungen an bestimmte andere in der Vorschrift genannte öffentliche Stellen übermittelt werden dürfen. Das BMF lehnt jedoch ein Auskunftsverweigerungsrecht der Telekommunikationsdiensteanbieter unter Hinweis auf die §§ 101 ff. AO, die nach seiner Ansicht die Anwendung des § 89 Abs. 6 TKG ausschließen, ab. In seinem Schreiben an die obersten Finanzbehörden der Länder vom 7. Januar 1997 hatte das BMF bereits seine von den genannten Bundesressorts und mir abweichende Auffassung dargelegt. Dieses Schreiben bildet eine wesentliche Ursache für eine Vielzahl unrechtmäßiger Auskunftserteilungen durch Netzbetreiber, die vermeiden wollen, von Finanzämtern wegen Auskunftsverweigerung mit Zwangsmaßnahmen belegt zu werden.

Das BMF hat mir weiterhin mitgeteilt, dass es erst dann zu einer Überprüfung seiner Rechtsauffassung bereit sei, wenn eine Entscheidung des Bundesfinanzhofs im Sinne der von BMWi, BMJ und mir vertretenen Rechtsauffassung vorläge. Ich habe daher das vorgenannte BMF-Schreiben wegen Verstoßes gegen § 89 Abs. 6 TKG beanstandet.

Der Deutsche Bundestag hat in seiner Entschließung zum 18. TB erklärt, er erwarte, dass die Bundesregierung in der dargestellten Frage zu einer einheitlichen Auffassung gelange (Empfehlungen des Innenausschusses, Bundestagsdrucksache 14/9490 vom 18. Juni 2002, Plenarprotokoll 14/248 der 248. Sitzung am 4. Juli 2002, S. 25174). Ich bin mit dem BMF übereingekommen, die Problematik im Rahmen der Gespräche über die datenschutzrechtlichen Belange in der AO (s. o. Nr. 9.1) zu erörtern.

9.9 Task Force Leuna/Minol darf personenbezogene Daten erheben

Vor dem Hintergrund von Presseberichten über die so genannte task force Leuna/Minol hat mich das BMI im Auftrag einer Gesprächsrunde unter Leitung des BMF gebeten, die Tätigkeit der Arbeitsgruppe Koordinierte Ermittlungen (AKE) und insbesondere die der Mitarbeiter der task forces datenschutzrechtlich zu bewerten. Die AKE wurde im Jahre 1996 in Weiterentwicklung von Besprechungen der verschiedenen für das Vermögen der ehemaligen DDR zuständigen Behörden wie BMF, Treuhandanstalt (THA)/Bundesanstalt für vereinigungsbedingte Sonderaufgaben (BvS), BMI und Unabhängige Kommission zur Überprüfung des Vermögens der Parteien und Massenorganisationen der DDR beim BMI im Bundeskanzleramt durch das BMF eingerichtet. Neben den bereits genannten Stellen sind dort unter Vorsitz des BMF regelmäßig auch das BKA, die Zentrale Ermittlungsstelle der Kriminalpolizei für Regierungs- und Vereinigungskriminalität beim Polizeipräsidenten in Berlin und weitere Stellen vertreten (s. Bundestagsdrucksache 13/10900 S. 347). Die AKE tritt etwa zweimal im Jahr zusammen. Ihre Aufgabe ist es, Erkenntnisse der verschiedenen Stellen zu Ansprüchen der Bundesrepublik Deutschland im Zusammenhang mit der Veruntreuung von DDR-Vermögen und Betrugsfällen zum Nachteil des Bundes bzw. der THA/BvS zusammenzuführen und durch darauf aufbauende eigene Nachforschungen die zivilrechtliche Durchsetzung von Rechtsansprüchen des Bundes zu optimieren.

Zur Umsetzung der Beschlüsse der AKE wurde die Geschäftsstelle der AKE (G-AKE), bestehend aus deren Leiter und in der Regel vier task forces, bei der im Geschäftsbereich des BMF angesiedelten BvS eingerichtet. Der Leiter der G-AKE leitet gleichzeitig die task forces, denen im Juni 2002 elf Berater (z. B. beurlaubte Steuerfahnder, Zollfahnder, Beamte des Bundesrechnungshofs mit privatrechtlichen Beraterverträgen) angehörten.

Um den Komplex Leuna/Minol daraufhin zu untersuchen, ob der Bundesrepublik Deutschland bzw. ihren Einrichtungen aufgrund eines vorwerfbaren Verhaltens ein Schaden entstanden ist und dementsprechend zivilrechtliche Schritte einzuleiten sind, wurde auf Weisung des BMF im September 2000 bei der BvS die task force Leuna/Minol geschaffen. Alle task forces haben bei einer Reihe von Behörden wie etwa dem BMWi oder bei verschiedenen Staatsanwaltschaften personenbezogene Daten erhoben und hierüber an die AKE, die task force Leuna/Minol auf Weisung des BMF auch unmittelbar an diese berichtet. Die task force Leuna/Minol hat inzwischen ihre Tätigkeit beendet.

Voraussetzung für meine datenschutzrechtliche Bewertung war zunächst, die organisatorischen Strukturen der beteiligten Stellen festzustellen und zu bewerten. Verbindliche Regelungen über das dar gestellte Organisationsgefüge waren nicht vorhanden. Auch gab es bisweilen widersprüchliche Äußerungen in den mir überlassenen Unterlagen, sodass eine Reihe von Zweifeln insbesondere hinsichtlich der Einbindung der task force Leuna/Minol in die G-AKE zu klären war. Für die AKE und deren Geschäftsstelle gab es jeweils Entwürfe für eine Geschäftsordnung, die von der AKE nur im Grundsatz gebilligt bzw. nur als weitere Arbeitsgrundlage bestimmt worden waren. Weitere Hinweise auf die Strukturen der Organisation ergaben sich aus den Sitzungsprotokollen der AKE, Weisungen in Erlassen, einzelnen Schreiben beteiligter Stellen und Erläuterungen von Beteiligten.

Insgesamt ließ sich hiernach feststellen, dass die AKE selbst als öffentliche Stelle des Bundes i. S. d. § 2 BDSG mit der Aufgabe anzusehen ist, auf der Grundlage des § 34 Abs. 1 Bundeshaushaltsordnung möglichen Schadensersatzansprüchen der öffentlichen Hand nachzugehen. Die für sie tätige G-AKE ist zwar ein Teil der BvS und damit gegenüber der AKE organisatorisch selbstständig. Sie ist dieser jedoch zur Aufgabenerfüllung im Wege der Organleihe (s. BVerfGE 63, 1, 31f.) zugeordnet. Als Teil der BvS, d. h. einer Anstalt des öffentlichen Rechts, ist sie befugt, im Rahmen der Zuständigkeit der AKE aufgrund des BDSG durch die Mitarbeiter ihrer task forces, insbesondere auch der task force Leuna/Minol, die zur Erfüllung ihrer Aufgabe erforderlichen personenbezogenen Daten zu erheben, zu verarbeiten und zu nutzen.

Im vorliegenden Fall bestanden zunächst mangels organisatorischer Klarheit Zweifel an der datenschutzrechtlichen Zulässigkeit des Handelns der Mitarbeiter der task forces. Dies sollte Anlass sein, auch im Hinblick auf die Anforderungen des Datenschutzes künftig stets für Klarheit und Übersichtlichkeit der Organisation zu sorgen.

9.10 Software für EG-Zollinformationssystem – EG-ZIS – korrigiert

In meinem 18. TB (Nr. 7.9) habe ich dargelegt, dass die EG-Amtshilfeverordnung Nr. 515/97 vom 13. März 1997 nach

Auffassung der Bundesregierung und auch nach meiner Auffassung keine ausreichende Rechtsgrundlage darstellt, um einen spontanen Informat ionsaustausch zwischen den EU-Mitgliedsstaaten zu ermöglichen. Nach der Definition in Artikel 27 Abs. 1 dieser V erordnung ist das EG-ZIS lediglich als eine Ausschreibungsdatei angelegt. Das seinerzeit von der Kommission vor gestellte Software-Programm, das es ermöglichte, komplexe Sachverhalte bildlich darzustellen und Querverbindungen zu anderen Sachverhalten aufzuzeigen, ging hierüber weit hinaus.

Inzwischen hat sich die Ko mmission den deutschen Bedenken, die auch von anderen Mitgliedsstaaten geteilt werden, angeschlossen und die Software entsprechend überarbeitet. Diese hat nunmehr nur noch den Charakter einer Ausschreibungsdatei, die den Zollbeamten bei der Erledigung seiner Aufgaben mit konkreten Informationen für den Einzelfall unterstützt. Gegen eine Einf ührung dieser überarbeiteten Software habe ich keine da tenschutzrechtlichen Bedenken. Die Inbetriebnahme des EG-ZIS ist für das Jahr 2004 vorgesehen.

Mittelfristig wird von der Kommission und den Mitgliedsstaaten weiterhin eine erweiterte Software angestrebt, die es den Mitgliedsstaaten ermöglichen soll, zusätzliche Informationen auszutauschen. Dies ist datenschutzrechtlich vertretbar, wenn im erforderlichen Umfang eine Er gänzung des Artikel 27 der genannten Verordnung erfolgt.

10 Wirtschaft

10.1 Bundeseinheitliche Wirtschaftsnummer in der Erprobung

In meinem 18. TB (Nr . 30.2) habe ich über meine Beteiligung an den V orbereitungen eines Erprobungsgesetzes für eine einheitliche Unternehmensnummer berichtet. Aus datenschutzrechtlicher Sicht war dabei entscheidend, die zu erhebenden Daten und deren Verwendungszwecke abschließend festzuschreiben. Die vorgesehene eingeschränkte Verwendung musste gewährleisten, dass die Nummer sich nicht zu einem allgemeinen Personenkennzeichen entwickeln kann, obwohl auch natürliche Personen einbezogen werden.

Am 22. Mai 2002 wurde das Gesetz zur V orbereitung einer bundeseinheitlichen Wirtschaftsnummer verkündet (BGBl. I S. 1644), das meinen Empfehlungen weitestgehend entspricht. Die Erprobung wird in den Jahren 2002 und 2003 in Bayern durchgeführt und von ei nem Beirat, dem ich angehöre, begleitet. Zu den Date nschutzaspekten, die im Rahmen der Erprobung zu beobachten und bei einem späteren Gesetzentwurf zu diskutieren sein werden, gehören insbesondere Fragen zur so genannten Abschneidegrenze und zur Erfassung von Privatpersonen, die eine Haushaltshilfe beschäftigen. Weiterhin zählen dazu die Forderung, dass es sich um eine „nicht sprechende Nummer“ (also ohne erkennbaren Personenbezug) handeln muss sowie die Fragen, ob der Stammdatensatz erweitert werden darf und inwieweit Rückmeldungen von den statistischen Ämtern zugelassen werden sollen.

Mit der derzeitigen Abschneidegrenze wird festgelegt, dass Kleinstgewerbetreibende und Freiberufler ohne Fremdbeschäftigte mit einem jeweiligen Umsatz unter 16 620 Euro pro Jahr von dem Anwendungsbereich der Wirtschaftsnummer ausgenommen sind. Dagegen bestehen jedoch T endenzen, unter Hinweis auf möglichst vollzählige Erfassung von wirtschaftlichen Bereichen, z. B. auch angestellte Freiberufler (wie Ärzte oder Rechtsanwälte) einzubeziehen.

Bezüglich der Erforderlichkeit der Erfassung privater Haushalte mit einer Haushaltshilfe konnte ich mich nicht durchsetzen. Das Argument, diese Personen hätten bereits in der Vergangenheit eine eigene Betriebsnummer erhalten, überzeugt mich ebenso wenig wie der Hinweis auf das Ziel, möglichst viele Nummernsysteme zu ersetzen. Für mich ist nicht erkennbar, welche V erwaltungsabläufe in welchem Umfang vereinfacht würden. Der infrage kommende Personenkreis beträgt ca. 2 % der Bevölkerung; käme hier außerdem die Abschneidegrenze von 16 620 Euro zur Anwendung, so wäre die Zahl der betrof fenen Personen verschwindend gering. Ich bin darüber hinaus der Auf fassung, dass es sich hier eher um einen Bereich der privaten Lebensführung handelt als um wirtschaftliche Betätigung im eigentlichen Sinne.

Die jetzt erprobte W irtschaftsnummer ist neunstellig und lässt keine Rückschlüsse auf di e wirtschaftlich Tätigen zu. Sie setzt sich zusammen aus einer „führenden“ Null und der achtstelligen Betriebsnummer der Bundesanstalt für Arbeit. Es bestehen aber auch hier Wünsche der V erwaltung, die Nummer sortierfähig und auswertbar zu machen und in andere bestehende Nummernsysteme zu integrieren. Dabei kommt es aus Datenschutzsicht entscheidend darauf an, dass sie „nicht sprechend“ bleibt.

Bezüglich des Stammdatensatzes weisen die künftigen Anwender darauf hin, dass die Syner gieeffekte mit der Menge der Daten pro W irtschaftseinheit zunähmen und daher die Grenzen der zu erfassenden Daten nicht zu eng gesetzt werden sollten. Dem ist jedoch die Zweckbestimmung der einheitlichen Wirtschaftsnummer entgegenzuhalten, d. h. die Vielfalt bestehender Nummernsysteme zu ersetzen und nicht Wirtschaftsprofile und – durch die Einbeziehung von Privatpersonen und Freiberuflern – auch Personenprofile zu ermöglichen.

Auf dem datenschutzrechtlichen Prüfstand steht auch noch der Wunsch der Statistik nach Rückmeldungen, wenn bei der Plausibilisierung eines geme ldeten Datensatzes festgestellt wird, dass z. B. die bei der Statistik gespeicherte Zuordnung eines Betriebes zu einem W irtschaftszweig mit der gemeldeten Zuordnung nicht übereinstimmt. Die Geheimhaltung der statistischen Einzelangaben ist aber seit jeher das Fundament der amtlichen Statistik (§16 Bundesstatistikgesetz). Die statistische Geheimhaltungspflicht wird als Gegenstück zur Auskunftspflicht und damit für die Erhaltung der Auskunftsbereitschaft und der Gewinnung zuverlässiger Angaben als notwendig angesehen; Ausnahmen bedürfen einer gesetzlichen Regelung und sind nur unter bestimmten Bedingungen zulässig. Ich werde die Auswertung der Erprobung kritisch begleiten und darauf achten, ob eine solche Ausnahmesituation tatsächlich gegeben ist.

Die Bundesanstalt für Arbeit hat zum 31. Oktober 2003 einen Schlussbericht über die durch die Erprobung gewonnenen Erkenntnisse mit konkreten Empfehlungen für die Einführung einer bundeseinheitlic hen Wirtschaftsnummer vorzulegen. Auf der Grundlage dieses Berichts und der in Bayern gemachten Erfahrungen werde ich mich dann bei der Gesetzgebungsarbeit für die datenschutzrechtlichen Belange einsetzen.

10.2 Finanzplatz Deutschland – „Förderung“ durch Überwachung?

Die Bundesregierung hat sich in der vergangenen Legislaturperiode das Ziel gesetzt, den Finanzplatz Deutschland zu fördern. Dabei sollte insbesondere das Vertrauen der in- und ausländischen Teilnehmer an Finanztransaktionen in Deutschland gestärkt werden. Es spielte aber auch – nicht zuletzt nach dem 11. September 2001 – die Schaffung von Regelungen zur besseren Bekämpfung krimineller Machenschaften im Finanzsektor eine nicht zu übersehende Rolle.

Hauptsächlich die Vorschriften, die eine leichtere Kontrolle von Geldflüssen und eine Überprüfung von Konten ermöglichen sollten, stießen auf vielfältigen Widerstand. Dabei wurde insbesondere die daraus resultierende deutliche Beeinträchtigung von Bürgerrechten kritisiert.

In diesem Rahmen stellte das BMF Überlegungen an, eine so genannte Konten-Evidenzzentrale beim Bundesaufsichtsamt für das Kreditwesen (inzwischen Bundesanstalt für Finanzdienstleistungsaufsicht, im folgenden Bundesanstalt genannt) einzurichten. Dadurch sollte ein umfassendes Nachweisregister für alle Giro-, Spar- und Depotkonten, also für alle in Deutschland geführten Bankkonten, geschaffen werden. Nach kurzer, aber heftiger Diskussion setzte sich jedoch unter meiner entscheidenden Mithilfe die Erkenntnis durch, dass ein solches bundesweites Register mit einer pauschalen Erfassung von allen, also auch von unbescholtenen Konteninhabern, nicht praktikabel ist, um Konten terroristischer Organisationen und Einzeltäter aufzudecken. Um der Geldwäsche, dem illegalen Schattenbankwesen und dem unerlaubten Betreiben von Bank- und Finanzdienstleistungsgeschäften auf die Spur zu kommen, bedarf es nicht eines bundesweiten Registers über alle Konteninhaber, sondern eines effektiveren Systems, wie die Bundesanstalt die erforderlichen Informationen erhalten kann, ohne eine Vielzahl von Auskunftsersuchen versenden zu müssen. Um diesen Zweck zu erreichen, müssen aber weder neue Befugnisse geschaffen noch weitere Eingriffe in das informationelle Selbstbestimmungsrecht des Einzelnen vorgenommen werden.

Nachdem die Idee, eine Konten-Evidenzzentrale einzurichten, nicht mehr weiterverfolgt wurde, ist durch das Vierte Finanzmarktförderungsgesetz vom 21. Juni 2002 (BGBl. I S. 2010) eine Rechtsgrundlage für einen automatisierten Abruf von Kontoinformationen in § 24c des Gesetzes über das Kreditwesen (KWG) geschaffen worden. Dadurch werden alle Kreditinstitute verpflichtet, ab 1. April 2003 eine besondere Datei zu führen, aus der die Bundesanstalt in einem von ihr bestimmten Verfahren die Daten automatisiert abrufen kann. Dabei handelt es sich um Daten, die nicht neu erhoben werden müssen, sondern bei der kontoführenden Bank ohnehin vorhanden sind. Diese Daten sind allerdings bislang nicht in einer Datei zusammengefasst. Im Einzelnen geht es um die Nummer eines Kontos oder eines Depots sowie den Tag der Errichtung und den Tag der Auflösung. Darüber hinaus werden der Name (bei natürlichen Personen auch der Tag der Geburt) des Inhabers und eines Verfügungsberechtigten sowie der Name und die Anschrift eines abweichend wirtschaftlich Berechtigten erfasst. Diese Daten sind nach Ablauf von drei Jahren nach der Auflösung des Kontos oder Depots zu löschen. Jedes Kreditinstitut hat zu gewährleisten, dass die Bundesanstalt jederzeit Daten aus dieser Datei automatisiert abrufen kann. Besonders zu betonen ist aus datenschutzrechtlicher Sicht, dass die Kreditinstitute durch technische und organisatorische Maßnahmen sicherstellen müssen, dass ihnen noch nicht einmal die Tatsache eines Abrufes, geschweige denn die dazu verwendeten Daten zur Kenntnis gelangen. Dieses Verfahren ermöglicht der Bundesanstalt, auf einen Blick festzustellen, mit welchen Instituten eine bestimmte Person oder ein bestimmtes Unternehmen Kontobeziehungen unterhält. Deutlich hervorzuheben ist, dass durch diesen automatisierten Abruf keine Angaben über Kontostand und Kontenbewegungen übermittelt werden. Vielmehr muss sich die Bundesanstalt aufgrund der durch diesen Abruf erhaltenen Informationen gezielt bei dem Institut, bei dem das Konto der betreffenden Person geführt wird, nach den einzelnen Umsätzen erkundigen.

Die 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Hinblick auf diese Regelung eine Entschließung gefasst, in der gefordert wird, dass im Rahmen der praktischen Umsetzung dieser Eingriff zumindest durch eine aussagekräftige Information gegenüber dem Kunden transparent gemacht wird (s. Anlage 22). Dies sollte durch eine Verpflichtung der Geldinstitute zur generellen Information der Kunden erfolgen, die die Kenntnisnahme schriftlich zu bestätigen haben.

Eine weitere beachtenswerte Regelung betrifft das so genannte Kontoscreening. Danach haben die Geldinstitute besondere organisatorische Pflichten bei der Bekämpfung und Verhinderung der Geldwäsche. Nach dem neu eingefügten § 25a Abs. 1 Nr. 4 KWG sind deshalb angemessene Sicherungssysteme zu schaffen, die die Analyse und Kontrolle von risikoreichen Konten oder Finanztransaktionen unter dem Gesichtspunkt der Geldwäsche gewährleisten können. Diese Sicherungssysteme sollen weitgehend automatisiert durch IT-Lösungen realisiert werden, um die Analyse der enormen Anzahl von Transaktionen in angemessener Zeit durchführen zu können. Durch meine Empfehlungen wurde die Formulierung dieser Regelung noch während der Arbeiten am Gesetzentwurf präzisiert. Die doch erheblich in die Privatsphäre des Betroffenen eingreifende Vorschrift ist nunmehr so gefasst, dass die Kontrolle und Analyse auf den oben beschriebenen Zweck beschränkt ist.

Die beschlossenen Regelungen sind damit im Hinblick auf die möglichen Auswirkungen einer kriminellen Nutzung des Finanzsektors aus meiner Sicht akzeptabel. Die Umsetzung der Regelungen in die Praxis werde ich aufmerksam begleiten.

10.3 Korruptionsregister – wer kommt rein?

Bereits in meinen letzten Tätigkeitsberichten (18. TB Nr. 8.12, 17. TB Nr. 8.15) habe ich über den Beschluss der Bundesregierung berichtet, Maßnahmen gegen unzuverlässige Unternehmer einzuleiten. In der letzten Legislaturperiode hatten die Koalitionsfraktionen einen Gesetzentwurf vorgelegt, der die Einrichtung und Nutzung eines Registers über unzuverlässige Unternehmen regeln sollte. Der Entwurf enthielt Regelungen, die den öffentlichen Auftraggebern ermöglichen sollten, unzuverlässige Unternehmen zu erkennen, um sie dann möglicherweise von der Vergabe öffentlicher Aufträge ausschließen zu können. In dem Gesetzentwurf blieb der konkrete Zweck der Registerabfrage

unklar, der Kreis der Abfrageberechtigten wurde nicht deutlich genug geregelt und die Konkretisierung des Begriffs „unzuverlässig“ sollte außerdem einer gesonderten Verordnung überlassen werden. Auf diese fehlende Normenklarheit hatte ich die zuständigen Ausschüsse des Deutschen Bundestages im Laufe der Gesetzesberatungen hingewiesen und im Hinblick auf den erheblichen Eingriff in die Bürgerrechte der betroffenen Unternehmer auf Abhilfe gedrungen.

Erst der vom Bundesrat angerufene Vermittlungsausschuss beschloss, sowohl den Zweck des Registers und den Kreis der zugriffsberechtigten Stellen zu konkretisieren als auch die Definition des Begriffs „unzuverlässig“ in das Gesetz aufzunehmen. Danach sollte ein Unternehmen „unzuverlässig“ sein, wenn bei ihm hinreichende Anhaltspunkte für Bestechung, Geldwäsche, Betrug, Untreue, illegale Beschäftigung, Beauftragung mit Schwarzarbeit oder andere im Gesetz genannten Straftatbestände vorlägen. Auf das Register sollten nur öffentliche Auftraggeber und die betroffenen Unternehmen in unmittelbarem Zusammenhang mit der Vergabe von öffentlichen Aufträgen Zugriff bekommen.

Dieser Beschlussempfehlung des Vermittlungsausschusses ist der Deutsche Bundestag zwar gefolgt, jedoch hat der Bundesrat dem Gesetz seine Zustimmung ohne weitere Begründung erneut verweigert.

Da sich das Problem der Vergabe von öffentlichen Aufträgen an Unternehmen, die gegen die einschlägigen gesetzlichen Bestimmungen verstoßen, nicht erledigt hat, erwarte ich in dieser Legislaturperiode eine neue Gesetzesinitiative der Bundesregierung.

Den Fortgang dieser Angelegenheit werde ich weiter begleiten.

10.4 Nachwehen des DDR-Rechts = Einschränkung von Bürgerrechten?

Die Eingabe eines Petenten hat die interessante Frage nach Art und Umfang eines Auskunftsersuchens gegen die Nachfolgeorganisation der Staatlichen Versicherung der DDR aufgeworfen.

Der Petent hatte sich zuvor an die Staatliche Versicherung der DDR in Abwicklung (SinA) gewandt und um Auskunft über eventuell dort zu seiner Person gespeicherte personenbezogene Daten gebeten. Er ging dabei davon aus, dass entsprechende Daten aus einem Versicherungsfall aus der ehemaligen DDR dort vorliegen müssten.

Bei der SinA handelt es sich um eine Anstalt des öffentlichen Rechts, die der Fachaufsicht des BMF untersteht und damit meiner datenschutzrechtlichen Kontrolle unterliegt.

Überraschenderweise ist die Bitte um Auskunft von der SinA unter Hinweis auf die Gesetzeslage in der ehemaligen DDR – die wohl eine Auskunftsverpflichtung gegenüber dem Betroffenen nicht vorsah – abgelehnt worden. Auf meine Bitte um Stellungnahme hat die SinA erwidert, dass der Petent zwar Akteneinsicht verlangt, man ihm aber mitgeteilt hätte, dass die Vorschriften des BDSG über das Auskunftsrecht nicht auf den Aktenbestand der SinA anzuwenden seien. Darüber hinaus hätte die SinA keine personenbezogenen Daten über den Petenten, vielmehr seien nur Zahlungsdaten bei der Allianz Versicherung – diese hat die gesamte Abwicklung des Versicherungsgeschäftes übernommen – verfügbar. Auf diese Daten habe die SinA keinen direkten Zugriff und könne deshalb keine Auskunft erteilen. Gleichwohl hat die SinA sowohl dem Petenten als auch mir gegenüber ausführlich aus den Versicherungsunterlagen des Petenten berichtet, sodass Zweifel an dem tatsächlichen Umfang der bei der SinA existierenden personenbezogenen Daten des Petenten bestanden.

Trotz meines Hinweises auf die Rechtslage, insbesondere auf die uneingeschränkte Geltung der Regelung zum Auskunftsrecht in § 19 BDSG, beharrte die SinA auf die alleinige Anwendung der Gesetze der ehemaligen DDR.

Daraufhin habe ich die fortgesetzte Auskunftsverweigerung der SinA gegenüber dem BMF förmlich beanstandet.

Die infolge der Beanstandung erteilte Stellungnahme des BMF war zunächst leider nicht hilfreich, da lediglich auf ein Schreiben der SinA mit deren schon bekannter Argumentation hingewiesen wurde. Eine rechtliche Würdigung des beanstandeten Verhaltens fehlte vollständig. Nach Eingang einer ergänzenden Stellungnahme des BMF ist immer noch nicht endgültig geklärt, in welchem Umfang die SinA Daten besitzt. Es ist aber davon auszugehen, dass sich aufgrund der erläuterten Vertragslage zwischen dem Bund als Rechtsnachfolger des DDR-Staates und der Allianz Versicherung tatsächlich die gesamten Versicherungsakten bei der Allianz befinden und die SinA nur aus dem mit dem Petenten geführten Schriftwechsel und aus einer Auskunft der Allianz ihre Informationen über den Versicherungsfall hat.

In dem Teil des Sachverhaltes, der sich mit der grundlegenden Frage der Fortgeltung von DDR-Recht befasst, hat das BMF die Rechtslage hinsichtlich des Geltungsbereich des DDR-Rechts in diesen Fällen klargestellt. Danach sind tatsächlich in den Fällen, in denen der Versicherungsschaden noch zu DDR-Zeiten eingetreten ist, für die rechtliche Bewertung der materiellen Anspruchsgrundlage die damals geltenden Regelungen heranzuziehen. Dies gilt selbstverständlich nicht für die Regelungen des BDSG und hier insbesondere für das Auskunftsrecht des Betroffenen.

Als Ergebnis ist hier festzuhalten, dass die SinA sehr wohl im Rahmen des § 19 BDSG eine Auskunftsverpflichtung gegenüber dem Petenten trifft. Ich werde mich weiterhin dafür einsetzen, dass der Petent die ihm zustehenden Rechte wahrnehmen kann.

10.5 SCHUFA

10.5.1 SCHUFA errichtet Warndatei im Wohnungswesen

Ein neues Projekt der SCHUFA ist der SCHUFA-Anschluss von Wohnungsunternehmen. Hierdurch soll die Bonität des Wohnungsinteressenten durch den Vermieter überprüft werden können. Die SCHUFA selbst wirbt mit dem Slogan „Mit uns finden Sie solvente Mieter“. Der Service für die gewerbliche Wohnungswirtschaft umfasst laut SCHUFA die folgenden Leistungen:

- Auskunftserteilung bei Vertragsabschluss,
- Kurzabfrage vor Beitreibungsmaßnahmen,
- Nachmelden mit laufenden Bonitätsinformationen über ihre Kunden,
- Adressermittlung bei unbekannt verzogenen Schuldnern,
- individuelle Bestandsauswertungen.

Bereits bei Abschluss des Miet vertrages sollen Vermieter der SCHUFA die Mieterdaten mit der Konsequenz melden, dass in Zukunft alle Mieter, deren Vermieter Vertragspartner der SCHUFA sind, in einer Datei gespeichert sind.

Der Vermieter soll ferner nicht vertragsgemäßes V erhalten des Mieters an die SCHUFA melden. Ein datenschutzrechtlich fragwürdiges V orhaben, da diese Einmeldungen auf subjektiven Feststellungen des Vermieters beruhen und den Rechtsstandpunkt des Mieters nicht unbedingt berücksichtigen. Zwar sollen – laut SCHUFA – Fälle, in denen der Mieter die Höhe der geltend ge machten Nebenkosten bestreitet oder in denen der Mieter eine Mietminderung wegen eines Mangels der Mietsache geltend macht, nicht zu einer Einmeldung führen, doch bedarf es für eine Einmeldung als Negativmerkmal keines Rechtstitels. Eine Überprüfung des Umstandes, ob eine Vermieterforderung unbestritten ist oder nicht, stellt sich somit als schwierig dar.

Von der SCHUFA geplant war darüber hinaus, dass anfragende Vermieter eine Zusammenstellung aller eingemeldeten monatlichen Raten und laufenden V erpflichtungen des jeweiligen Mietinteressenten erhalten sollten. Die Zusammenstellung sollte auf den Einmeldungen aller anderen SCHUFA-Vertragspartner zu der betreffenden Person basieren. Der Vermieter bekäme somit auch solche Auskünfte über den Mieter bzw. Mietinteressenten, die mit dem Mietverhältnis im engeren Sinne ni chts zu tun hätten, vielmehr aus anderen geschäftlichen Betätigungen des Betrof fenen stammen. Aufgrund des W iderstandes der Datenschutzaufsichtsbehörden hat sich die SCHUF A bereit erklärt, das Merkmal „Summe der monatlichen Belastung“ „bis auf weiteres zurückzustellen und zumindest derzeit nicht umsetzen zu wollen“, leider nur eine Aussage, die zukünftiges Verhalten völlig offen lässt.

Bei der SCHUF A anfragende Vermieter erhalten nicht nur Auskünfte über nichtvertragsgemäßes Verhalten der Betroffenen bezogen auf andere/frühere Mietverhältnisse. Vielmehr bekommen sie im Rahmen des so genannten B-V erfahrens der SCHUFA Auskünfte über jegliches nichtvertragsgemäßes Verhalten der Mietinteressenten.

Ein datenschutzrechtlich bede nkliches Verfahren. Ein Betroffener muss so damit rechnen, als Mieter abgelehnt zu werden, weil er z. B. seine Handyrechnung nicht rechtzeitig bezahlt hat. Bei den heute ohnehin schwierigen V erhältnissen auf dem Wohnungsmarkt und dem hohen W ert des Gutes „Wohnung“ ein inakzeptables Ergebnis.

Die Berechtigung einer derartigen Mieterwarndatei halte ich bereits deswegen für zweifelhaft, weil das Kreditrisiko bei Vermietern anders zu bewerten ist als das anderer Kreditgeber. Vermieter haben ein Pfandrecht gegenüber den Mietern, und es steht ihnen regelmäßi g eine Kaution zur V erfügung. Lässt man jedoch eine W arndatei der SCHUF A für das Wohnungswesen zu, so ist es meines Erachtens ausreichend, wenn das Verfahren im Rahmen einer „geschlossenen Benutzergruppe“ betrieben wird. Das heißt, Angaben über Betroffene, die von Vermietern gemeldet werden, werden auch nur an andere Vermieter und nicht auch an alle anderen Vertragspartner der SCHUFA übermittelt. Umgekehrt bekommen anfragende Vermieter auch nur Informationen über vertragswidriges Verhalten des jeweils Betrof fenen aus Mietverhältnissen und nicht auch aus anderen V erbindlichkeiten.

10.5.2 Wann liegt eine automatisierte Einzelentscheidung im Sinne des § 6a BDSG vor?

Im Rahmen von Gesprächen zwischen den Datenschutzaufsichtsbehörden, der SCHUFA und dem Zentralen Kreditausschuss zum Thema Scoring-V erfahren der SCHUFA ist folgende Problematik zu T age getreten, die den Aufsichtsbehörden bis dato nicht bekannt war:

Bei der Entscheidung über eine Kreditgewährung ist es übliche Praxis der Kreditinstitute, für die Prüfung der Kreditwürdigkeit einer Person deren Score-W ert heranzuziehen, den wiederum das jeweilige Kreditinstitut bei der SCHUF A abfragt. Die SCHUFA ermittelt diesen Wert aus den ihr vorliegenden Daten mittels eines automatisierten Verfahrens. Nach Aussagen der Vertreter des Zentralen Kreditausschusses war es bei einigen Banken üblich, den Score-Wert nicht mehr separat – und damit für den Bearbeiter des jeweiligen Kreditantrags erkennbar – auszuweisen. Vielmehr wurde der von der SCHUFA übermittelte Score-Wert direkt automatisiert in andere Parameter des Kreditinstitutes eingearbeitet. Der Kreditsachbearbeiter wurde – so der Zentrale Kreditausschuss – nur noch mit dem Ergebnis der Computeranalyse „Kreditgewährung ja/nein“ konfrontiert, ohne die einzelnen, zu dem Ergebnis führenden Berechnungen nachvollziehen zu können.

Diese Praxis stellt m. E. eine unzulässige automatisierte Einzelentscheidung nach dem neuen § 6a BDSG dar . Danach „dürfen Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, nicht ausschließlich auf eine automatisierte V erarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen“. Sowohl die SCHUFA als auch der Zentrale Kreditausschuss stellten sich auf den Standpunkt, dass die V oraussetzungen des § 6a BDSG nicht vorlägen und beriefen sich auf die Begründung des Regierungsentwurfs zu § 6a BDSG, in der die in der T at irritierende Aussage getroffen worden war, dass das Scoring-Verfahren nur dann unter die Regelung des § 6a BDSG falle, wenn sowohl das Scoring-V erfahren als auch die anschließende Entscheidung in einer Hand lägen. SCHUFA und Zentraler Kreditausschuss ar gumentierten nun damit, dass der Score-Wert von der SCHUF A und die letztendliche Kreditentscheidung von einem Sachbearbeiter des jeweiligen Kreditinstitutes getroffen würden und somit die Entscheidung gerade nicht in einer Hand läge. Bei dieser Ar gumentation wurde allerdings außer Acht gelassen, dass das Verfahren des Kreditinstitutes so konstruiert war , dass der Score-W ert in seiner Aussage nicht mehr überprüfbar war , da er automatisch mit anderen W erten verarbeitet wurde. Eine Entscheidungsmöglichkeit über die Anerkennung des Score-W ertes als positiv oder negativ war nicht gegeben; m. E. ein gravierender Fall einer automatisierten Einzelentscheidung.

Ich habe daraufhin den für das BDSG federführend zuständigen Innenausschuss des Deutschen Bundestages auf die irritierende Begründung zu § 6a BDSG aufmerksam gemacht. Der Deutsche Bundestag hat daraufhin in seinen Beratungen zu der Novellierung des BDSG die folgende Klarstellung zu § 6a BDSG vorgenommen:

„Entgegen der Begründung des Regierungsentwurfs kommt es bei § 6a für die Beurteilung, ob eine Entscheidung ausschließlich auf eine automatisierte V erarbeitung personenbezogener Daten gestützt wi rd, nicht darauf an, ob das

Scoring-Verfahren und die abschließende Entscheidung in einer Hand liegen. Der Schutzgedanke des § 6a geht vielmehr davon aus, dass [.....] eine Bewertung von Persönlichkeitsmerkmalen, wie z. B. der Kreditwürdigkeit, in jedem Fall eine Beurteilung durch einen Menschen erfordert, die das Ergebnis einer standardisierten Computeranalyse nicht zur einzigen Entscheidungsgrundlage macht, sondern Raum lässt für eine Überprüfung und Relativierung dieses Ergebnisses, insbesondere auf Grund eigener zusätzlicher Erkenntnisse oder besonderer Umstände des Einzelfalles" (vgl. Beschlussempfehlung und Bericht des Innenausschusses zu dem Gesetzentwurf der Bundesregierung – Bundestagsdrucksache 14/4329, 14/4458 – Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze, Bundestagsdrucksache 14/5793, Begründung zu XVI (§ 34 Abs. 4 BDSG), S. 65 – so beschlossen durch den Deutschen Bundestag in seiner Sitzung am 6. April 2001, Plenarprotokoll 14/165, Tagesordnungspunkt 19).

Damit dürfte der Argumentation der SCHUFA und des Zentralen Kreditausschusses die Grundlage entzogen sein.

10.5.3 SCHUFA als Evidenzzentrale für das Bundeskriminalamt

Zwischen dem Bundeskriminalamt und der KSV-Kreditschutz Vereinigung GmbH, einem Unternehmen der SCHUFA-Organisation, wurde im Dezember 1999 ein Vertrag geschlossen, nach dem das Bundeskriminalamt Daten der Dokumentensachfahndung an die KSV übermittelt. Gemäß dem Vertrag besteht der der KSV übermittelte Dokumenten-Sachfahndungsbestand aus Datensätzen, die Angaben über die Dokumentennummer, die Dokumentenart und den ausstellenden Staat des in der Sachfahndung ausgeschriebenen Dokumentes enthalten. Sinn und Zweck der Vereinbarung ist es, hohe Schäden für die Wirtschaft zu verhindern bzw. zu minimieren, die durch die Nutzung gestohlener oder verloren gegangener Ausweisdokumente entstehen. Als dieses neue Betätigungsfeld der SCHUFA den Datenschutzaufsichtsbehörden bekannt wurde, stand man dieser vertraglichen Vereinbarung zunächst skeptisch gegenüber. Befürchtungen wurden laut, dass Daten über verloren gegangene oder gestohlene Ausweise in den übrigen Datenbestand der SCHUFA einfließen könnten. Der BfD wurde hier als zuständige Datenschutzaufsichtsbehörde für das Bundeskriminalamt um Prüfung gebeten, ob eine solche Vereinbarung rechtlich zulässig sei.

Nach § 10 Abs. 3 i. V. m. Abs. 2 BKA-Gesetz ist es dem Bundeskriminalamt in bestimmten Fällen erlaubt, personenbezogene Daten auch an, wie hier, nicht öffentliche Stellen zu übermitteln. Auch darüber hinaus sehe ich keinen Verstoß gegen geltendes Recht. Gleichwohl gibt es eine datenschutzrechtliche Schwachstelle: Nach dem Pass- und dem Personalausweisgesetz dürfen die Identifikationspapiere nicht so verwendet werden, dass mit ihrer Hilfe ein Abruf personenbezogener Daten aus Dateien oder eine Verknüpfung von Dateien möglich ist. Bei vertragsgerechter Handhabung können die der SCHUFA vom Bundeskriminalamt übermittelten Daten nicht auf diese rechtlich unzulässige Weise genutzt werden, da die übermittelten Daten grundsätzlich von der SCHUFA nicht personalisierbar sind. Es werden lediglich die Nummern der Dokumente übermittelt, die seitens der SCHUFA nicht anderen Daten zugeordnet werden können. Dies könnte sich allerdings dann ändern, wenn ein Kreditinstitut im Rahmen der Überprüfung eines Neukunden nicht nur dessen Ausweisnummer an die SCHUFA übermittelte zwecks Abgleich mit der Dokumenten-Sachfahndungsliste des Bundeskriminalamtes, sondern diese Abfrage in einem Arbeitsgang mit der Abfrage über die Kreditwürdigkeit des Neukunden verbände. In diesem Falle würde das Kreditinstitut an die SCHUFA nicht separat die Ausweisnummer, sondern auch die übrigen Stammdaten des Neukunden übermitteln. Die Ausweisnummer wäre dann personalisierbar und es läge ein Verstoß gegen das Pass- und das Personalausweisgesetz vor. Eine solche Vorgehensweise der Kreditinstitute wäre zwar nicht vertragsgemäß, aber in der Praxis aus Überlegungen der Arbeitserleichterung auch nicht auszuschließen.

Ich habe die Aufsichtsbehörden auf diese Gefahr hingewiesen, die die Praxis der Kreditinstitute in diesen Fällen beobachten.

10.5.4 Eintragung bestrittener Forderungen von Telekommunikationsunternehmen in das SCHUFA-Register

Aufgrund mehrerer Bürgereingaben habe ich festgestellt, dass es im Berichtszeitraum immer wieder vorkam, dass Telekommunikationsunternehmen eine Eintragung bei der SCHUFA wegen Nichtzahlung einer Rechnung durch ihre Kunden veranlasst hatten, obwohl die zugrunde liegende Forderung von Kundenseite bestritten wurde.

Zwar sind die Telekommunikationsunternehmen gegenüber der SCHUFA vertraglich gebunden, dieser auch Daten aufgrund nichtvertragsgemäßen Verhaltens (z. B. ausstehender Forderungsbetrag nach Kündigung, Kartenmissbrauch) ihrer Kunden zu übermitteln. Diese Meldungen dürfen nach dem BDSG aber nur erfolgen, soweit dies nach Abwägung aller betroffenen Interessen zulässig ist.

Da es sich bei dem hier erörterten Sachverhalt – die geltend gemachte Forderung wird von Kundenseite bestritten – nicht um den Fall der generellen Zahlungsunfähigkeit bzw. Zahlungsunwilligkeit handelt, liegt eine Meldung des Kunden an die SCHUFA weder im berechtigten Interesse des Telekommunikationsunternehmens noch in einem anzuerkennenden Interesse der SCHUFA. Bei der hier in jedem Einzelfall erforderlichen Interessenabwägung ist das schutzwürdige Interesse des Kunden an einer Nichteintragung in einem solchen Fall höher zu bewerten als das Interesse der Wirtschaft an einem Eintrag. Daher habe ich die betroffenen Telekommunikationsunternehmen aufgefordert, entsprechend zu verfahren.

10.5.5 Speicherung der SCHUFA-Auskunft beim Telekommunikationsunternehmen

Wegen der hohen wirtschaftlichen Vorleistungen der Telekommunikationsunternehmen – Subventionierung des Handys sowie sofortige Freischaltung eines Anschlusses für den Kunden – ist es im Bereich des Mobilfunks marktüblich, die Bonität eines Kunden vor Abschluss eines Vertrages über Telekommunikationsdienstleistungen zu überprüfen. Es besteht zwar die Möglichkeit, das wirtschaftliche Risiko der Unternehmen z. B. durch die Hinterlegung einer Sicherheitsleistung des Kunden aufzufangen. Hiervon wird in der Praxis aber kein Gebrauch gemacht. Entsprechende Auskünfte werden mit schriftlicher Einwilligung des Betroffe-

nen bei der SCHUFA oder anderen Wirtschaftsauskunfteien eingeholt. Im Zusammenhang mit dieser Einwilligungserklärung 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 über ihn gespeicherten Daten hinzuweisen.

Fraglich ist, wie lange die von der SCHUFA bzw. anderen Wirtschaftsauskunfteien erteilten Auskünfte in den Systemen der Telekommunikationsunternehmen auch nach Zustandekommen des Vertrages gespeichert bleiben dürfen.

Unter Berücksichtigung des allgemeinen Grundsatzes, dass die Datenerhebung und -speicherung nur in dem erforderlichen Umfang erfolgen darf, ist die dauerhafte Speicherung der Auskunft datenschutzrechtlich unzulässig. Hinzu kommt, dass die Auskunft auch bereits nach kurzer Zeit überholt und wertlos ist, weil sie sich naturgemäß nur auf den Zeitpunkt der Anfrage bezieht. Ich habe daher im Berichtszeitraum Telekommunikationsunternehmen gebeten, die Auskünfte der SCHUFA bzw. anderer Auskunfteien nach einer angemessenen Speicherfrist von längstens einem Monat zu löschen.

10.6 Die Kundenkarte – Rabattgewährung oder Datenfang?

Laut einer Emnid-Umfrage soll die so genannte Kundenkarte für viele Deutsche nach der Krankenversicherungs- und der ec-Karte die wichtigste Karte in der Brieftasche geworden sein. Kundenkarten, auch Rabattkarten genannt, werden mittlerweile von verschiedenen Anbietern herausgegeben. So stehen z. B. hinter der Payback-Karte, dem größten Kundenbindungssystem in Deutschland, mehrere große Konzerne. In den meisten Fällen gewähren die Kundenkarten den Konsumenten Rabatte von 1 bis 5 %; zusätzlich bekommen Karteninhaber z. B. Coupons für noch höhere Rabatte bei Sonderaktionen, Prämien, Eintrittskarten für Sportveranstaltungen oder Konzerte und vieles mehr. Die Verbraucher sollen so an das Unternehmen oder die hinter der Kundenkarte stehenden Konzerne gebunden werden und ihre Käufe auf die entsprechenden Geschäfte konzentrieren. Doch geht das Interesse der Kundenkartenanbieter in der Regel weiter. Als Gegenleistung für die Rabattgewährung wollen die Anbieter auch etwas vom Kunden erfahren. Angaben zu Interessen, Konsum- und Kaufgewohnheiten, soziale und familiäre Verhältnisse werden z. T. auf den Anmeldeformularen abgefragt oder aber subtil über das tatsächliche Kaufverhalten in Erfahrung gebracht. Die Daten ermöglichen dem Anbieter, eine Vorstellung von den Wünschen und Verhaltensweisen der eigenen Kunden zu bekommen. Dies kann sich auf die Produktgestaltung, die Präsentation und vor allem auf die Art der Werbung auswirken. Je präziser die Angaben sind, desto höher ist das Risiko, dass bei der Werbung manipulativ vorgegangen werden kann. Eine große Gefahr besteht auch darin, dass die z. T. sensiblen Konsumdaten auch für Zwecke der Profilbildung genutzt oder auch missbraucht werden, z. B. durch Verkauf an andere Firmen.

Trotz der datenschutzrechtlichen Gefahren sind Kundenbindungsprogramme nicht von vornherein zu verurteilen. Jeder Verbraucher ist Herr seiner Daten, er muss sich keine Kundenkarte nehmen, wenn er davon nicht überzeugt ist. Aus Datenschutzsicht ist allerdings zu fordern, dass die Position des Verbrauchers durch Transparenz und Information gestärkt wird. Jeder muss wissen, wozu welche Daten abgefragt werden, welche Daten über ihn gespeichert werden und zu welchem Zweck und ob die Daten weitergegeben werden. Jeder Inhaber einer Kundenkarte sollte wissen, welche Unternehmen hinter der Karte stehen und inwieweit sein Kaufverhalten zu einem Kundenprofil zusammengeführt wird. Erst eine genaue Information gibt ihm die Möglichkeit abzuwägen und frei zu entscheiden, ob er für die ihm gewährten Vorteile auch die einhergehenden Gefahren in Kauf nehmen will.

In diesem Zusammenhang geht das so genannte „Permission Marketing“ einen offenen, kunden- und damit auch datenschutzfreundlichen Weg der Kundenbindung und des Marketing. Statt subtil die vermeintlichen Wünsche der Verbraucher auszuforschen, setzt die Strategie des „Permission Marketing“ auf die Stärkung der eigenen Gestaltungsmöglichkeiten der Verbraucher. Hierbei werden nur Informationen, sprich Werbung, versandt, die vom Empfänger ausdrücklich erwünscht sind und die er auch jederzeit wieder abbestellen kann. Sein Kundenprofil legt der Konsument selbst fest und er kann es stets verändern, wenn er an anderen Artikeln oder gar nicht mehr an einer Bewerbung interessiert ist. Interaktive Kommunikationstechnologien wie E-Mail, SMS, Online-Chats etc. machen dies möglich.

Ein etwas anderer Weg der Kundenbindung, der sich sowohl für Verbraucher als auch für Unternehmen lohnen könnte.

10.7 Schuldnerdaten im Internet

Mit dem Gesetz zur Änderung der Insolvenzordnung und anderer Gesetze (BGBl. 2001 I S. 2710) wurde durch Ergänzung des § 9 der Insolvenzordnung (InsO) die Möglichkeit geschaffen, öffentliche Bekanntmachungen in Insolvenzverfahren auch im Internet vorzunehmen. Hierdurch sollen Kosten eingespart werden. In der Begründung hierzu wird erläutert, in Verbraucherinsolvenzverfahren mit regelmäßig geringen Massen hätten die Veröffentlichungskosten – insbesondere bei Bekanntmachungen in Tageszeitungen – dazu beigetragen, dass diese Verfahren nicht eröffnet werden konnten und dem Schuldner der Weg zur Restschuldbefreiung dadurch versperrt blieb (Bundestagsdrucksache 14/5680 S. 24).

Regelungen zum Schutz der Schuldner bei Veröffentlichung ihrer Daten im Internet sah der Gesetzentwurf nicht vor. Vor dem Hintergrund der daraufhin gefassten gemeinsamen Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. April 2001 zur Veröffentlichung von Insolvenzinformationen im Internet (s. Anlage 15) habe ich mich mit meinen Bedenken an den Rechtsausschuss des Deutschen Bundestages gewandt: Dritte, etwa Auskunfteien oder Wirtschaftsinformationsdienste könnten die veröffentlichten Daten unbegrenzt kopieren, speichern, auswerten und auch nach Abschluss des Insolvenzverfahrens beliebig lange im Internet zur Verfügung stellen. Dies führe zu einem Eingriff in das Persönlichkeitsrecht des Schuldners, der über die Beeinträchtigung hinausgehe, die dieser nach der jetzigen Gesetzeslage im Hinblick auf die begrenzten Auswertungsmöglichkeiten der Veröffentlichungen in Zeitungen oder Amtsblättern hinnehmen müsse. Insbesondere stehe dies auch im Widerspruch zu dem mit der Restschuldbefreiung

angestrebten Zweck, dem Schuldner zu ermöglichen, nach Abschluss des Insolvenzverfahrens wieder unbelastet am Geschäftsverkehr teilzunehmen.

Bei der vom Gesetzgeber verabschiedeten Regelung wurden – soweit möglich – Sicherungen zum Schutz des Persönlichkeitsrechts der in das Internet eingestellten Schuldner vorgesehen. Aufgrund einer ergänzend in die Insolvenzordnung eingefügten Ermächtigung hat das BMJ in der Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet (BGBl. 2002 I S. 677) unter anderem festgelegt, dass die Veröffentlichung nur die personenbezogenen Daten enthalten darf, die nach der Insolvenzordnung bekannt zu machen sind. Weiterhin ist nach dieser Verordnung sicherzustellen, dass die Daten während der Veröffentlichung unversehrt, vollständig und aktuell bleiben und spätestens nach Ablauf von zwei Wochen seit dem ersten Tag der Veröffentlichung nur noch abgerufen werden können, wenn die Abfrage den Sitz des Insolvenzgerichts und bestimmte weitere Daten des jeweiligen Falles nennt. Auch ist nach dem Stand der Technik dafür Sorge zu tragen, dass diese Daten nicht durch Dritte elektronisch kopiert werden können. Nicht zuletzt schreibt die Verordnung vor, dass die Veröffentlichung von Daten aus einem Insolvenzverfahren spätestens einen Monat nach der Aufhebung oder der Rechtskraft der Einstellung des Insolvenzverfahrens gelöscht wird.

Weiter nahm der Bundestag einen Entschließungsantrag an, in dem er die Bundesregierung bittet zu prüfen, wie verhindert werden kann, dass Daten, die nach § 9 InsO im Internet veröffentlicht wurden, nach Ablauf der gesetzlichen Löschungsfrist durch Dritte über das Internet verbreitet werden. In die Prüfung soll die Frage einbezogen werden, ob insoweit eine eigenständige Bußgeldvorschrift geschaffen werden soll. Die Unterrichtung durch die Bundesregierung, an der ich beteiligt worden bin, ist am 12. Dezember 2002 erfolgt (Bundestagsdrucksache 15/181).

Wenn auch nicht von der gesetzlichen Möglichkeit abgesehen wurde, Bekanntmachungen in Insolvenzverfahren im Internet zu veröffentlichen, so begrüße ich doch sehr, dass das federführende BMJ und der Deutsche Bundestag großes Verständnis für die damit verbundenen Eingriffe in das Persönlichkeitsrecht der jeweils betroffenen Schuldner gezeigt und sich nachdrücklich bemüht haben, diese auf das Erforderliche zu begrenzen.

Zu meinem Bedauern wurde allerdings mein Vorschlag, gesetzlich festzulegen, dass Dritte Daten aus amtlichen Bekanntmachungen im Rahmen von Insolvenz- und gleichartigen Verfahren in Papierform nicht über die Fristen der Verordnung zu § 9 InsO oder andere gleichartige Fristen hinaus im Internet verbreiten dürfen, im Bericht der Bundesregierung nicht aufgenommen. Die durch diesen Vorschlag berührten wirtschaftlichen Interessen der entsprechenden Verlage, Auskunfteien und Wirtschaftsinformationsdienste sollten jedenfalls nicht Anlass dafür sein, Überlegungen auch in dieser Richtung von vornherein auszuschließen. Nach Auskunft von Landesbeauftragten für den Datenschutz wenden sich in letzter Zeit bereits jede Woche etwa ein bis zwei Petenten wegen der Veröffentlichung ihrer Daten aus Insolvenz- oder Zwangsversteigerungsverfahren im Internet an diese Stellen. Auch wenn es hierbei nicht jeweils um die Veröffentlichung dieser Daten über bestimmte Fristen hinaus geht, zeigt dies doch auf, wie drängend und sensibel das vorliegende Problem gesehen werden sollte. Gerade auch vor dem Hintergrund der erwähnten Eingaben sehe ich es als bedenklich an, den Zeitpunkt für weitere Regelungen zum Schutz der Betroffenen, insbesondere für Bußgeldvorschriften, von vornherein erst an die vorgesehene zweite Stufe der Novellierung des Bundesdatenschutzgesetzes anzubinden, da nach meiner Einschätzung nicht abzuschätzen ist, in welchem Zeitrahmen die zweite Stufe abgewickelt werden kann.

10.8 Warndateien im Wohnungswesen

Es gibt immer stärkere Bestrebungen der Wohnungswirtschaft, sich durch die Errichtung von regionalen Warndateien vor Mietausfällen durch säumige Mieter zu schützen. Neben der SCHUFA, die sich um den Anschluss der gewerblichen Wohnungswirtschaft an den Kreis ihrer Vertragspartner bemüht, schließen sich auch mehr und mehr Wohnungsunternehmen und einzelne Vermieter zu Gläubigerschutzgemeinschaften zusammen und errichten Warndateien.

Hier werden zum Teil sensibelste Daten erhoben, gespeichert und übermittelt, deren Rechtmäßigkeit jedoch zweifelhaft ist. Bereits das Interesse an einer Wohnung kann dazu führen, dass Betroffene in eine Datei aufgenommen werden. Wohnungssuchende, die längere Zeit auf Wohnungssuche sind und in dieser Zeit an mehreren Wohnungen Interesse gezeigt haben, fallen Vermietern direkt als unseriös ins Auge. Detaillierte Fragen nach den Vermögensverhältnissen wie bestehende Ratenzahlungen, Höhe von Unterhaltszahlungen etc., über Fragen nach der Staatsangehörigkeit bis hin zur Frage nach Personalausweis- oder Passnummer sind üblich. Vermieter melden in diese Warndateien zum Teil verspätete oder unregelmäßige Mietzahlungen (die im Einzelfall z. B. durch Mietminderung wegen Mangels etc. begründet sein können und nicht unbedingt auf eine generelle Zahlungsunfähigkeit oder -willigkeit hinweisen), vertragswidriges Verhalten oder Verstöße gegen die Hausordnung.

Das Interesse der Wohnungswirtschaft, „schwarze Schafe“ unter den Mietinteressenten zu erkennen und dadurch das betriebswirtschaftliche Risiko bei der Vermietung zu verringern, ist nachvollziehbar und verständlich. Doch müssen auf der anderen Seite auch die Belange der Wohnungssuchenden beachtet werden. Die Wohnung zählt zum Mittelpunkt des privaten Lebensbereiches. Wenn es möglich ist, dass durch ungeprüfte Eingaben von Mieterdaten jedermann zum „Negativmieter“ gestempelt werden kann, dann lässt sich nicht ausschließen, dass Personen auch unverschuldet und ohne berechtigten Anlass in diesen Ruf geraten. Auch die Einwilligung der Betroffenen in dieses Verfahren steht der datenschutzrechtlichen Bedenklichkeit nicht entgegen. Gerade bei der Mietsituation in Ballungsräumen bleibt Wohnungssuchenden in der Regel keine freie Wahl, ob sie in diese Art der Datenerhebung und -nutzung einwilligen oder nicht. Die Rechtmäßigkeit der Einwilligungserklärung nach dem BDSG dürfte in den meisten Fällen zumindest bedenklich sein.

Die Aufsichtsbehörden befassen sich mit dieser Problematik. Wünschenswert wäre hier die Festlegung auf einen datenschutzrechtlichen Forderungskatalog, den Warndateien im Wohnungswesen zu beachten hätten.

10.9 Keine Hilfe gegen unerwünschte Werbeflut?

Die Werbung ist ein wirtschaftlich bedeutender Teil der Marktwirtschaft. Viele Menschen wollen aber gar keine Werbung und manche nur bestimmte Werbung. Während man sich gegenüber Briefwerbung und Wurfsendungen und dem damit verbundenen überquellenden Briefkasten inzwischen ganz gut wehren kann, ist die Situation bei unverlangter elektronischer Werbung, die in den letzten Jahren einen enormen Umfang angenommen hat, bis heute sehr unerfreulich, wie man den nachfolgenden beiden Beiträgen entnehmen kann (vgl. darüber hinaus Nr. 11.4). Hier gibt es aber vielleicht ein Lichtlein am Ende des Tunnels, und zwar Artikel 13 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates der Europäischen Union, dem bis zum 31. Oktober 2003 das nationale Recht der Mitgliedsstaaten entsprechen muss.

Danach ergreifen die Mitgliedsstaaten geeignete Maßnahmen, um (gebührenfrei für die Teilnehmer) sicherzustellen, dass unerbetene Nachrichten zum Zweck der Direktwerbung grundsätzlich nicht gestattet sind.

Auf jeden Fall verboten ist die Versendung elektronischer Nachrichten ohne Angabe des Absenders bzw. Auftraggebers oder gültiger Adresse, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann.

Es bleibt abzuwarten, ob durch diese europäische Richtlinie die elektronische Werbeflut tatsächlich eingedämmt wird. Einer Verlagerung der Werbung ins weitere Ausland kann möglicherweise durch entsprechende Filter in einer Reihe von Fällen begegnet werden.

10.9.1 Jetzt habe ich aber die Faxen dick!!!

Unerwünschte Werbung ist bei Faxgeräten ein besonders großes Problem. Hier fallen beim Empfänger nicht nur erhebliche zusätzliche Kosten (Strom, Papier, Toner) an. Zudem wird die bestimmungsgemäße Funktion der Faxanlage stark beeinträchtigt, weil das Faxgerät in dieser Zeit besetzt ist und andere wichtige Schreiben weder empfangen noch gesendet werden können. Besonders ärgerlich ist ein durch Werbefaxe ausgelöster nächtlicher Papierstau, weil ihn der Empfänger oft nicht bemerkt (das gilt natürlich auch, wenn Papier und Toner durch Werbefaxe aufgebraucht werden). Bei Faxgeräten im Privatbereich ist darüber hinaus besonders störend, dass die Geräte immer noch recht laut sind und durch nächtliche Werbefaxe die Nachtruhe erheblich beeinträchtigt werden kann.

Nach höchstrichterlicher Rechtsprechung ist unverlangte Faxwerbung unzulässig und verstößt gegen § 1 des Gesetzes gegen den Unlauteren Wettbewerb, wenn zwischen Absender und Empfänger keine Geschäftsbeziehung besteht und auch sonst der Absender nicht annehmen darf, die Zusendung durch Telefax erfolge mit dem mutmaßlichen Einverständnis des Empfängers. Abmahnungen oder Klagen erscheinen allerdings wenig vielversprechend; abgesehen von dem Aufwand und den Kosten ist häufig der Absender der Faxwerbung nicht erkennbar. Um Faxpapier, Toner und Nerven zu sparen, gibt es folgende andere Möglichkeiten:

- Auch für die Faxwerbung gibt es eine so genannte Robinson-Liste, die im Auftrag des BITKOM (Bundesverband Informationswirtschaft, Kommunikation und neue Medien e. V.) geführt wird.
- Ein Formular zur Eintragung in die Liste ist unter der Fax-Nr.: 01805/000761 abrufbar. Die Liste gilt allerdings nur für Mitglieder im Bundesverband, die sich zur Beachtung verpflichtet haben.
- Bei Bestellung von Waren kann man schriftlich widersprechen, dass die Daten für Zwecke der Werbung und Marktforschung benutzt werden.
- ISDN-Anlagen können Faxe ohne erkennbare Anrufnummer abweisen.
- Bei schwerwiegenden Belästigungen oder bei Bedrohungen kann man bei seinem Telekommunikationsunternehmen eine so genannte Fangschaltung beantragen.
- Wenn man auf eine Bekanntgabe (z. B. aus beruflichen Gründen) der Faxnummer nicht angewiesen ist, kann man auf die Veröffentlichung im Telefonverzeichnis verzichten.
- Wenn gar nichts hilft und man die Faxen dick hat, bleibt nur noch eins: Beantragung einer neuen Faxnummer.

10.9.2 Unerwünschte E-Mails oder Das kleinere Übel

E-Mails, die Inhaber einer E-Mail-Adresse ungefragt erhalten, werden euphemistisch unerwünscht genannt. Diese Bezeichnung lässt leider nicht den tagtäglichen Kampf und die Wut der Betroffenen erkennen, die diese wohlgemeinten Werbebotschaften hervorrufen. Der englischen Bezeichnung „spam“ kann das aufgrund seiner ursprünglichen Verwendung in einer Satiresendung schon eher gelingen. Denn diese E-Mails haben sich inzwischen zu einer wahren Plage ausgewachsen. Hinzu kommt das Problem der so genannten Dialer, die – ebenso unerwünscht installiert – den Internetnutzer nicht nur Zeit und Nerven, sondern auch Geld kosten (s. u. Nr. 11.4).

Den ratsuchenden Bürgern kann ich kaum Erfreuliches oder Hilfreiches mitteilen:

Dass nach überwiegend einheitlicher deutscher Rechtsprechung das Versenden unerwünschter E-Mails nicht erlaubt ist, was aber leider vielfach nicht beachtet wird. Dass die Versender von spams in vielen Fällen nicht ermittelt werden können, weil die Absenderadresse und die Identifikationsangaben beim Provider gefälscht sind – da hilft dann auch der in § 13a Unterlassungsklagengesetz verankerte Auskunftsanspruch des Betroffenen nicht weiter. Dass ein großer Teil dieser E-Mails aus außereuropäischen Staaten kommt und somit die deutschen oder europäischen Datenschutzgesetze nicht gelten. Dass die spammer inzwischen nicht nur die im Internet gesammelten und in Verzeichnissen verfügbaren E-Mail-Adressen verwenden, sondern automatisch und systematisch Adressen generieren, sodass es über kurz oder lang jeden trifft. Dass ein Widerspruch beim Versender meistens nicht nur wirkungslos ist, sondern diesem lediglich bestätigt, dass es sich um eine aktive E-Mail-Adresse handelt.

Was nützt da noch ein Eintrag in die Robinson-Liste oder ein vorsichtiges und zurückhaltendes Umgehen mit der eigenen E-Mail-Adresse, muss sich angesichts dieser Situation jeder Betroffene fragen. Und was tun die Provider? Die

tun ihr Möglichstes, d. h. was im Rahmen der Gesetze erlaubt ist. Sie weisen E-Mails von so genannten Open Relay Servern ab – das sind Server, die ein Versenden von E-Mails unter einer beliebigen, frei wähl- und fälschbaren Absenderadresse zulassen. Sie filtern E-Mails vor, die von bekannten spam-Adressen stammen. Sie bieten zusätzlich Filter für ihre Kunden an, die diese dann selbst einsetzen müssen. Sie sperren entsprechend ihre n Nutzungsbedingungen die Adressen von eigenen Kunden, wenn diese ihnen als spammer gemeldet werden. Eine inhaltliche Filterung der E-Mails durch den Provider kommt jedoch wegen des Fernmeldegeheimnisses nicht in Frage, auch wenn einige Nutzer dies vorschlagen.

Sicherlich gäbe es eine Möglichkeit, die unerwünschte Werbeflut im Netz weitgehend einzudämmen. Die sähe dann folgendermaßen aus, weltweit und für alle: Anmeldung beim Provider nur mit Vorlage des Personalausweises, Protokollierung und Inhaltskontrolle des gesamten E-Mail-Verkehrs, bedingungsloser Auskunftsanspruch für jeden jederzeit. Unabhängig vom Aufwand und den Kosten wird doch jeder angesichts eines solchen Szenarios die unerwünschten E-Mails als das kleinere Übel hinnehmen! Und sie weiterhin ignorieren und die Löschen-Taste betätigen.

11 Telekommunikations- und Teledienste

11.1 Europäische Entwicklungen des Datenschutzrechts in den neuen Medien

Die Ausgestaltung des Datenschutzes in den neuen Medien wird heutzutage nicht mehr nur durch den deutschen Gesetzgeber bestimmt. Die Internationalität der Unternehmen, der Geschäftsmodelle und der zum Einsatz kommenden technologischen Lösungen macht es vielmehr immer wichtiger, auf europäischer Ebene auf die damit verbundenen Herausforderungen für den Datenschutz zu reagieren. Dies hat die Europäische Union erkannt und mit der Datenschutzrichtlinie für die elektronische Kommunikation bereichsspezifische Datenschutzregelungen vor gegeben, die von den Mitgliedsstaaten in nationales Recht umgesetzt werden müssen. Neben diesen gesetzgeberischen Aktivitäten hat die Europäische Union aber auch Beratungsgremien zum Schutz der personenbezogenen Daten in den neuen Medien geschaffen, wie beispi elsweise die International Working Group for Data Protection in T elecommunications und die Internet Task Force der Artikel 29-Gruppe.

11.1.1 In-Kraft-Treten der EU-Datenschutzrichtlinie für elektronische Kommunikation

Mit der EU-Richtlinie 2002/58/EG über „die V erarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation“ vom 12. Juli 2002 hat die EU auf die rasante Entwicklung bei den modernen Kommunikationsmedien reagiert und den Datenschutz in diesem Bereich weiter gestärkt. Damit wurde die alte T elekommunikations-Datenschutzrichtlinie 97/66/EG aufgehoben. Die Mitgliedsstaaten haben die Richtlinie umzusetzen und dies der Kommission entsprechend mitzuteilen. Die Umsetzung, für die eine Frist bis zum 31. Oktober 2003 gesetzt wurde, soll im Rahmen einer allgemeinen Novellierung des Telekommunikationsgesetzes erfolgen.

Die Regelungen zum Datenschutz in diesem Bereich mussten an die Entwicklungen der Märkte und T echnologien für elektronische Kommunikationsdienste angepasst werden. Der Schutz der Nutzerdaten so llte unabhängig von der benutzten Technologie sichergestellt werden. Der Geltungsbereich der neuen Richtlinie wurde deshalb weiter gefasst als bisher und bezieht sich jetz t auf alle Bereiche der elektronischen Kommunikation. Entsprechend dem technischen „Zusammenwachsen“ von Telekommunikations- und Telediensten wurde eine Richtlin ie geschaffen, die den Datenschutz für beide Bereiche regelt. Dies ist aus meiner Sicht besonders positiv zu bewerten, weil es in der Praxis immer wieder schwer fällt, diese Bereiche zu trennen.

Neu aufgenommen wurde eine Regelung zu Standortdaten im Mobilfunk, die nur unter bestimmten V oraussetzungen verarbeitet und an Dritte übermittelt werden dürfen. Damit sollte eine Schutzvorschrift zugunsten der Nutzer so genannter standortbasierter Dienste (Location Based Services, s. Nr. 11.6) geschaffen werden. Der Anwendungsbereich der bisherigen V orschrift zum Schutz vor unerwünschten Anrufen wurde erweitert auf die Zusendung unerwünschter E-Mails. Danach ist die Zusendung von W erbung nur nach vorheriger Einwilligung zulä ssig; anonyme Direktwerbung ist auf jeden Fall verboten. Im Hinblick auf T eilnehmerverzeichnisse wurde eine Informationspflicht über den Zweck dieser Verzeichnisse und die technisch erweiterten Nutzungsmöglichkeiten aufgenommen.

11.1.2 Ergebnisse der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation

Die International Working Group for Data Protection in T elecommunications hat seit ih rer Gründung 1983 eine V ielzahl von Empfehlungen zur V erbesserung des Datenschutzes in der T elekommunikation herausgegeben. T eilnehmer sind Datenschutzbehörden, aber auch Regierungsstellen, Vertreter internationaler Or ganisationen und W issenschaftler aus aller W elt. Auch Mitarbeiterinnen meines Hauses nehmen an den zweimal jährli ch stattfindenden Sitzungen teil.

Im Berichtszeitraum wurden gemeinsame Standpunkte erarbeitet und Arbeitspapiere zu Fragen des Datenschutzes bei der Nutzung des Internets und der T elekommunikation beschlossen. Die technische Entwicklung in diesem Bereich macht es erforderlich, dass grundlegende Fragen auch in einer engen internationalen Zusammenarbeit diskutiert und beantwortet werden.

Einige wichtige Er gebnisse sollen hier beispielhaft aufgeführt werden. So wurde im Februar 2001 ein gemeinsamer Standpunkt zum Thema „Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten“ verabschiedet. Wegen der verbesserten Genauigkeit von Aufenthaltsinformationen und dem vermehrten Angebot standortbasierter Dienste wurden grundlegende Prinzipien empfohlen, die von den anbietenden Unternehmen beachtet werden sollen. Anbieter von Mehrwertdiensten sollen nur Zugang zu Aufenthaltsdaten erhalten, wenn der Nutzer seine informierte Einwilligung gegeben hat. Die Erstellung von Bewegungsprofilen durch Anbieter von T elekommunikations- und Mehrwertdiensten soll grundsätzlich verboten sein. Etwas anderes gilt nur, wenn dies für die Erbringung des Dienstes notwendig ist und der Nutzer eingewilligt hat. Die Aufenthaltsinformationen sollen möglichst nicht mit personenbe-

zogenen Angaben an Anbieter von Mehrwertdiensten weitergegeben werden. Soweit technisch realisierbar, sollen pseudonymisierte Informationen genutzt werden.

Im August 2001 wurde ein Arbeitspapier zu „Datenschutz und internetgestützter Stimmabgabe bei Wahlen zu Parlamenten und anderen staatlichen Einrichtungen" erarbeitet. In vielen Ländern wird die Möglichkeit der Wahl in elektronischer Form diskutiert. Die Einhaltung des Wahlgeheimnisses und die Frage der Transparenz und Überprüfbarkeit des Wahlverfahrens sind von entscheidender Bedeutung für die Akzeptanz von online-voting. Bei papiergestützten Wahlen ist dies leichter erreichbar. Die Arbeitsgruppe hat deshalb empfohlen, die kompliziert en technischen Fragen bezüglich der Verlässlichkeit und Sicherheit der Verfahren vor einem Einsatz zu beantworten und eine gründliche Risikoanalyse sowie Testverfahren durchzuführen. Die Authentifizierungsverfahren sollten nicht weniger sicher sein als bei papiergestützten Abstimmungen. Die gesamte Hard- und Software einschließlich des Quellcodes muss dokumentiert und einer Prüfung zugänglich gemacht werden. Zusätzlich müssen vertrauenswürdige Zertifizierungsverfahren für Hard- und Software eingesetzt werden (vgl. hierzu auch Nr. 7.8.2).

Im Frühjahr 2002 wurde ein Arbeitspapier zur Überwachung der Telekommunikation vorgelegt. Da in vielen Ländern die Befugnisse staatlicher Stellen zur Überwachung ausgeweitet wurden, erschien es wichtig, nochmals deutlich zu machen, dass bei Eingriffen in das Fernmeldegeheimnis Notwendigkeit und Verhältnismäßigkeit zu beachten sind. In dieser Hinsicht wurden die vom Europäischen Parlament aufgestellten Vorschläge ausdrücklich unterstützt. So wird gefordert, dass die Staaten ein gemeinsames Schutzniveau gegenüber nachrichtendienstlichen Tätigkeiten anstreben und einen Verhaltenskodex ausarbeiten sollen, der sicherstellt, dass die Tätigkeit der Nachrichtendienste in Übereinstimmung mit den Grundrechten und dem Schutz der Privatsphäre ausgeübt wird. Die Politik soll die Sensibilisierung der Nutzer moderner Kommunikationssysteme für die Notwendigkeit und Möglichkeit des Schutzes vertraulicher Informationen erhöhen. Benutzerfreundliche Kryptosoftware soll gefördert, entwickelt und hergestellt werden.

11.1.3 ITF, übernehmen Sie!

Die Internet Task Force (ITF) ist eine Art „Sondereinsatz-Gruppe" der Artikel 29-Gruppe (s. o. Nr. 3.6), wenn es darum geht, besondere Aufgaben im Zusammenhang mit Datenschutzfragen im Internet zu lösen oder Problemen in diesem Bereich auf den Grund zu gehen. So wurde Ende 2000 ihr bisher umfangreichstes und vielbeachtetes Papier „Privatsphäre im Internet – Ein integrierter EU-Ansatz zum Online-Datenschutz" veröffentlicht. Trotz des Umfangs ist dieses Arbeitspapier nicht nur für Laien auf den Gebieten der Technik und des Datenschutzes ein hilfreiches Grundlagen- und Nachschlagewerk zu vielen Fragen in unterschiedlichen Bereichen des Internet.

Anfang 2002 erhielt die ITF den Auftrag, den Online-Authentifizierungsdienst „Passport" von Microsoft näher zu untersuchen. Passport dient dazu, dem Nutzer durch ein so genanntes Single-Sign-On ein wiederholtes Anmelden mit immer denselben Angaben (z. B. Lieferadresse, Bankdaten) bei von Microsoft angebotenen Diensten und zahlreichen angeschlossenen Diensten zu ersparen. Zu diesem Zweck muss der Nutzer sich beim Passport Service registrieren lassen und erhält eine eindeutige Identifikationsnummer. Ein solcher Service mag ja unter bestimmten Umständen durchaus nützlich sein, Unbehagen ruft es aber schon hervor, wenn der Nutzer keine Wahl hat, sobald er Microsoft-Dienste in Anspruch nehmen will. Vor allem weil mithilfe der Identifikationsnummer detaillierte Profile des einzelnen Nutzers erstellt werden können.

Da massive Kritik von Seiten der Nutzer und der Datenschützer nach Einführung des Dienstes nicht lange auf sich warten ließ, hatte sich Microsoft auf Anfrage der Artikel 29-Gruppe bereit erklärt, zur Klärung der vielen offenen Fragen aktiv beizutragen. Mit der erhofften Offenheit hat Microsoft der ITF Rede und Antwort gestanden und Änderungen in den datenschutzrelevanten Bereichen versprochen. Dies betrifft insbesondere die Unterrichtung der Nutzer vor der Erhebung der Daten, die Einwilligungserklärung und die Verwendung der Identifikationsnummer.

Hier zeigt sich, dass auch ein marktbeherrschender US-Hersteller wie Microsoft nach entsprechender Intervention durchaus bereit ist, europäische Datenschutzregelungen zu berücksichtigen. Letztlich dürfte Microsoft seinen Passport Service in entscheidenden Punkten nachbessern.

Ein endgültiges Ergebnis lag bei Redaktionsschluss noch nicht vor.

11.2 Datenschutz im Internet

11.2.1 Neues Datenschutzrecht für die elektronischen Medien

Schon relativ kurz nach der Novellierung des Teledienstedatenschutzgesetzes (TDDSG) im Dezember 2001 wird die nächste Gesetzesänderung vorbereitet. Initiiert durch die Entschließung des Deutschen Bundestags vom 4. Juli 2002 (Bundestagsdrucksache 14/8649) wird damit das Ziel verfolgt, „die Eigenverantwortung der Medienwirtschaft zu stärken und ihr mehr Freiraum für Selbstregulierung zu geben, zugleich aber sicherzustellen, dass der Staat und seine Aufsichtsinstanzen eine Auffangverantwortung behalten und diese auch wahrnehmen können", kurz: eine regulierte Selbstregulierung oder Co-Regulierung zu installieren.

Das vorgeschlagene Modell sieht vor, die bestehenden Datenschutzaufsichtsstrukturen beizubehalten, aber durch eine neue Säule der freiwilligen Selbstregulierung zu ergänzen. Damit wird jedoch kein zusätzliches Kontrollinstrument geschaffen, sondern im gleichen Maße, wie der Medienwirtschaft mehr Verantwortung übertragen wird, sollen die Datenschutzaufsichtsbehörden entlastet werden. Die Selbstregulierungseinrichtungen bedürfen einer förmlichen Anerkennung durch mich. Das Verfahren und die inhaltlichen Details der Akkreditierung sollen im Gesetz offengelassen werden und von mir noch festzulegen sein.

Zusätzlich soll die Zusammenführung der Bereiche Teledienste, Mediendienste und Rundfunk in ein Gesetz das Datenschutzrecht für die elektronischen Medien vereinfachen, wobei im Wesentlichen bestehendes Recht übernommen werden soll. Besonders begrüßenswert ist die Klärung der alten Streitfrage „Telekommunikations- oder Teledienst" durch die explizite Zuordnung der Zugangsvermittlung, der

E-Mail-Dienste und der Internettelefonie zu den Telekommunikationsdiensten.

Die vom zuständigen Ministerium für Wirtschaft und Arbeit in einem ersten Entwurf formulierten Strukturüberlegungen werden zurzeit in den Ländern diskutiert. In einem späteren Schritt sollen die Datenschutzaufsichtsbehörden und Vertreter der betroffenen Unternehmen, des Rundfunks und der Presse in einer Expertenrunde zu Wort kommen. Dass schon jetzt Vorbehalte bezüglich der Selbstregulierungseinrichtungen laut werden, die mit der nicht gewährleisteten Unabhängigkeit solcher Stellen begründet werden, mag nicht verwundern, ist damit doch eine Umverteilung der Aufgaben verbunden. Andere Stimmen lassen vernehmen, dass die Wirtschaft auch ohne Co-Regulierung durch den Staat auskommen könne und somit eine alleinige Selbstkontrolle die richtige Lösung sei.

Wird das geplante Modell der regulierten Selbstregulierung realisiert, so ist dies im Bereich der Datenschutzaufsicht ein Schritt in eine neue Richtung.

11.2.2 Nichts Neues im Datenschutz bei Telediensten

Immer mehr Internetprovider setzen die Vorschriften des Teledienstedatenschutzgesetzes um. Die Bemühungen der Datenschutzaufsichtsbehörden – Kontrollen und Beratung, unter anderem in Form von Orientierungshilfen – scheinen also Früchte zu tragen. Vielleicht hat auch das gute Beispiel einiger Provider andere folgen lassen. Doch leider gibt es auch immer mehr neue Anbieter, für die der Datenschutz und das TDDSG unbekannte Größen sind, sodass im Ergebnis weiterhin keine flächendeckende Verbesserung des Datenschutzes bei Telediensten festzustellen ist. Das vermögen auch die hin und wieder auflammenden Abmahnwellen nicht zu leisten, die das Fehlen der so genannten Privacy Policy oder des Impressums auf Internetseiten mit einem Bußgeld belegen wollen, aber aufgrund der Art der Durchführung wohl weniger dem Datenschutz als der Geldbörse der Abmahnenden dienlich sein sollen.

Lediglich die Problemschwerpunkte, die die Diskussion mit den Nutzern und der Datenschützer untereinander beherrschen und gelöst werden müssen, ändern sich sporadisch: Waren es in der Vergangenheit cookies und die damit verbundene Möglichkeit der Profilbildung, später dann die Verwendung von online erhobenen personenbezogenen Daten in der offline-Welt für die Zusendung von Werbebriefen, so ist es heute die Überflutung mit unerwünschten E-Mails (s. o. Nr. 10.9.2). Dies ist in erster Linie ein Verbraucherschutzproblem, was aber durch die ungewollte Verwendung, Sammlung und Weitergabe der E-Mail-Adresse zum Datenschutzproblem werden kann. Zukünftig werden uns wohl eher Datenschutzprobleme im Zusammenhang mit Zahlungsverfahren im Internet (s. u. Nr. 11.2.3) beschäftigen, da die Tendenz zu erkennen ist, Dienste oder Informationen kostenpflichtig anzubieten. Dies sind zumindest Überlegungen einiger Anbieter, da der Versuch, die Angebote nur über Werbung zu finanzieren, wenig erfolgreich war.

11.2.3 Datenschutzgerechte Zahlungsverfahren im Internet

In meinem letzten Tätigkeitsbericht habe ich darüber informiert, dass sich die Datenschutzbeauftragten künftig eingehend mit der datenschutzrechtlichen Bewertung von Zahlungssystemen im Internet beschäftigen werden (18. TB Nr. 8.4). Im Februar 2001 fand dann eine Präsentationsveranstaltung beim Brandenburgischen Landesdatenschutzbeauftragten statt, zu der sieben Anbieter von Zahlungssystemen im Internet eingeladen wurden.

Eine sehr differenzierte datenschutzrechtliche Bewertung der bei der Veranstaltung vorgestellten Verfahren konnte nach dieser kurzen Präsentation allerdings nicht vorgenommen werden. Es wurden zwar anhand bestimmter Kriterien Vorteile und Schwachstellen aus datenschutzrechtlicher Sicht diskutiert. Ein Vergleich der einzelnen Verfahren untereinander war aber nur schwer möglich, da den vorgestellten Lösungen ganz unterschiedliche Ansätze von der reinen Software-Lösung bis zum integrierten Zahlungsverfahren zugrunde lagen. Die Verfahren wurden zunächst daraufhin untersucht, inwieweit sie sich an den vorgegebenen Zielen von Datenvermeidung und Datensparsamkeit ausrichteten. Darüber hinaus wurden Aspekte der Datensicherheit in die Betrachtung einbezogen sowie Stellung dazu genommen, ob die Zahlungsvorgänge für den Kunden transparent und nachvollziehbar sind.

Im Ergebnis konnte festgehalten werden, dass alle sieben Anbieter bei Datenvermeidung und Datensparsamkeit auf einer Skala durchgängig von zufriedenstellend bis absolut positiv zu bewerten waren. Die Kriterien der Datensicherheit erfüllten alle Anbieter gut bis sehr gut. Diese Bewertung hat allerdings eine eingeschränkte Aussagekraft, da sie auf nicht näher überprüfbaren Angaben der Anbieter beruht. Auch bei der Transparenz und Handhabbarkeit der Zahlungssysteme für den Kunden gab es keine nennenswerten negativen Einschränkungen. Wegen der Einzelheiten der Untersuchungsergebnisse möchte ich auf die Internetseite des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg www.lda.brandenburg.de verweisen.

Zusammenfassend kann ich festhalten, dass alle sieben Anbieter ein hohes Interesse an Fragen des Datenschutzes und der Datensicherheit haben, da diese Merkmale auch von Anbieterseite als entscheidend für die Akzeptanz empfunden werden. Datenschutz und Datensicherheit werden weniger als Behinderung vielmehr als Marktvorteil begriffen. Bei allen vorgestellten Verfahren sind unterschiedliche Möglichkeiten der anonymen oder pseudonymen Nutzung vorgesehen, die ein entsprechendes Maß an Sicherheit beim Zahlungsverkehr im Internet gewährleisten. Es wird weiter zu beobachten sein, wie sich diese elektronischen Zahlungssysteme zukünftig am Markt etablieren werden.

11.3 Hoheitliche Eingriffe in die Telekommunikation

Regelmäßig berichte ich über die Situation der Telefonüberwachung in Deutschland und muss dabei immer wieder – so auch in diesem Jahr – einen stetigen Anstieg der Überwachungszahlen melden (s. Nr. 8.3). Neben der kritischen Begleitung von Rechtssetzungsmaßnahmen zur Schaffung neuer Rechtsgrundlagen für die Überwachung von Telekommunikation (s. Nrn. 8.2.1, 8.2.4) setze ich mich auch für eine datenschutzgerechte Umsetzung von Überwachungsmaßnahmen ein. Meine Beteiligung an den Arbeiten zur Telekommunikations-Überwachungsverordnung mag hierfür

ein Beispiel sein. Schließlich gilt mein besonderes Augenmerk, den Bestrebungen im europäischen und im deutschen Raum entgegenzuwirken, die eine verdachtsunabhängige Vorratsdatenspeicherung von Verbindungsdaten bei den Telekommunikationsunternehmen einführen wollen.

11.3.1 Technische Aspekte bei der Überwachung von E-Mail

Überwachungsmaßnahmen des E-Mail-Verkehrs werden von den Strafverfolgungsbehörden schon seit längerer Zeit durchgeführt. Bisher sind die Anforderungen an die Übermittlung der überwachten E-Mails allerdings nicht geregelt, da kein Standard für die Übertragung besteht und insbesondere keine Verschlüsselung vorgesehen ist. Dies hat zur Folge, dass die überwachten E-Mails vom Anbieter zur Strafverfolgungsbehörde offen über das Internet übertragen werden.

Ich halte die unverschlüsselte Übertragung sensibler E-Mails für bedenklich (s. auch 17. TB Nr. 8.4 und 18.4). Die Tatsache, dass eine E-Mail-Adresse überwacht wird, ist bereits eine sehr brisante Information, die eine gesicherte Übertragung der E-Mail erforderlich macht – selbst wenn die ursprüngliche E-Mail unverschlüsselt ist. Deshalb hat die Regulierungsbehörde für Telekommunikation und Post im Sommer 2002 die betroffenen Anbieter, Hersteller und Behörden eingeladen, um eine Regelung für die sichere Übertragung der überwachten E-Mails zu finden. Diese Initiative wird auch von mir unterstützt. Inzwischen haben hierzu mehrere Gespräche stattgefunden.

Ich rechne damit, dass die „Technische Richtlinie zur Beschreibung der Anforderungen an die Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation“ Anfang 2003 geändert und die beschlossene Technik im Frühjahr 2003 umgesetzt wird. Damit sollte dann eine ungeschützte Übertragung der Vergangenheit angehören. Eine schneller umsetzbare Lösung wäre hier zwar wünschenswert gewesen, war aber aus technischen und organisatorischen Gründen nicht möglich.

11.3.2 Die neue Telekommunikations-Überwachungsverordnung

Mit § 88 Telekommunikationsgesetz (TKG) gibt es seit Juli 1996 eine Ermächtigungsgrundlage zum Erlass einer Verordnung für die technische Umsetzung von Überwachungsmaßnahmen im Bereich der Telekommunikation. Bereits im Mai 1998 wurde ein erster Entwurf für eine „Verordnung über die technische und organisatorische Umsetzung von Überwachungsmaßnahmen in der Telekommunikation (Telekommunikations-Überwachungsverordnung – TKÜV)” vorgelegt. Dieser wurde in der Öffentlichkeit sehr kontrovers diskutiert und aufgrund der dabei geäußerten Kritik vom federführenden BMWi kurzfristig zurückgezogen (s. 17. TB Nr. 10.1.5.1 und 18. TB Nr 10.1.3). Im darauffolgenden Jahr wurden dann vom Ministerium die „Eckpunkte für den Regelungsrahmen der Rechtsverordnung nach § 88 TKG” vorgelegt.

Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung vom 10. Mai 2001 (s. Anlage 16) darauf aufmerksam gemacht, dass die technikneutrale Formulierung der ersten Entwürfe datenschutzrechtlich problematisch sei. Es bestand zum damaligen Zeitpunkt die Gefahr, dass nicht nur die Sprachtelefonie und der Telefaxverkehr, sondern auch alle anderen elektronischen Kommunikationsplattformen und damit insbesondere das Internet erfasst würden.

Die TKÜV ist dann am 29. Januar 2002 in Kraft getreten und ersetzt die bislang geltende Fernmeldeverkehr-Überwachungs-Verordnung aus dem Jahr 1995. Es wurde ein in langen Diskussionen gefundener tragfähiger Kompromiss zwischen den berechtigten Belangen der Strafverfolgungs- und Sicherheitsbehörden auf der einen und den nachzuvollziehenden Interessen der verpflichteten Telekommunikationsunternehmen auf der anderen Seite gefunden. So sind etwa Internetprovider – bis auf die Fälle angeordneter Überwachungen von E-Mails – durch die TKÜV von der gesetzlichen Verpflichtung freigestellt worden, technische Überwachungseinrichtungen vorzuhalten. Gleiches gilt auch für die Betreiber von Corporate Networks.

Die TKÜV wurde bereits zum 24. August 2002 geändert und dabei um Vorschriften für die technische und organisatorische Umsetzung von Maßnahmen der strategischen Beschränkung ergänzt. Grund hierfür war die Novellierung des Artikel-10-Gesetzes (G10), das nunmehr in den §§ 5 und 8 Maßnahmen als strategische Beschränkungen vorsieht, bei denen die Überwachung eines Teils der Telekommunikation aus oder zu bestimmten Regionen im Ausland angeordnet werden kann (s. auch Nr. 19.2). Derartige strategische Beschränkungen unterscheiden sich grundlegend von den übrigen Überwachungsmaßnahmen. Dies wirkt sich bei ihrer technischen Umsetzung in der Weise aus, dass sie Betreiber anderer Telekommunikationsanlagen betrifft. Die Vorschriften dazu sind in Teil 3 der TKÜV zusammengefasst. Die bisherigen Regelungen für die Umsetzung von Überwachungsmaßnahmen nach den §§ 100a, 100b Strafprozessordnung, dem § 3 G10 sowie den §§ 39 bis 43 Außenwirtschaftsgesetz werden hiervon nicht berührt und sind inhaltlich unverändert geblieben.

11.3.3 Überlegungen zur Vorratsspeicherung

Es ist sicherlich nicht immer leicht, die richtige Balance zwischen dem Schutz personenbezogener Daten und den Sicherheitsinteressen des Staates zu finden. Im Berichtszeitraum wurden von verschiedenen Seiten jedoch Überlegungen angestellt, die das Gleichgewicht zulasten des einzelnen Bürgers zu verändern drohten und deshalb bei Datenschützern die Alarmglocken schrillen ließen.

Anlass war in erster Linie eine Gesetzesinitiative des Bundesrates, die wesentliche datenschutzrechtliche Grundsätze außer Acht ließ und aus Datenschutzsicht einen massiven Angriff auf das Recht auf informationelle Selbstbestimmung darstellte. Nachdem die Befugnisse der Strafverfolgungsbehörden schon zuvor erheblich erweitert worden waren (vgl. hierzu Nr. 2), sah der Gesetzentwurf (Bundesratsdrucksache 275/02) eine Ermächtigungsgrundlage für die Bundesregierung vor, durch Verordnung Regelungen für eine Vorratsspeicherung im Bereich der Telekommunikation und der Internetnutzung zu treffen. Durch Aufnahme von Mindestspeicherfristen für Kommunikationsdaten in das Telekommunikationsgesetz und das Teledienstedatenschutzgesetz sollte gewährleistet werden, dass Strafverfolgungs- und Sicherheitsbehörden nicht mehr wie bisher durch gesetzliche

Löschungsfristen daran gehindert werden, auf für sie relevante Daten zurückzugreifen.

Bei allem Verständnis für das öffentliche Interesse an einer effektiven Strafverfolgung muss unter Abwägung mit den Grundrechten der Betroffenen solchen Überlegungen nachdrücklich entgegen getreten werden. Die vorgeschlagene Vorratsspeicherung würde nämlich eine umfassende flächendeckende Sammlung und Vorhaltung von Kommunikationsdaten bedeuten, ohne dass ein bestimmter Anlass zur Speicherung besteht. Das heißt, es würden sensible – auch dem Fernmeldegeheimnis unterliegende – Daten von Bürgern gesammelt, obwohl gegen sie kein konkreter Verdacht vorliegt. Dies wäre ein gravierender Eingriff in das Persönlichkeitsrecht und weder mit dem Grundsatz der Datenvermeidung und -sparsamkeit noch mit dem Verhältnismäßigkeitsgrundsatz in Einklang zu bringen. Zudem wäre auch fraglich, ob eine solche Regelung dem Gebot der konkreten Bestimmung des Zwecks der Datenverarbeitung entspricht.

Die Bundesregierung hat in ihrer Stellungnahme (Bundestagsdrucksache 14/9801) den Gesetzentwurf zwar insgesamt abgelehnt, hinsichtlich der Einführung von Mindestspeicherfristen jedoch unter Hinweis auf die Notwendigkeit der oben erwähnten Rechtsgüter - und Interessenabwägung nur bemerkt, dass der Vorschlag des Bundesrates eine solche Abwägung nicht erkennen lasse. Somit wurde die Forderung nach einer Vorratsspeicherung nicht ausdrücklich und eindeutig abgelehnt. Ich werde die Diskussion zu diesem Thema daher weiterhin sorgsam verfolgen, zumal auf europäischer Ebene ein Vorstoß in die gleiche Richtung unternommen worden ist. Ein Vorschlag der dänischen EU-Ratspräsidentschaft im Jahr 2002 sieht vor, in den Bereichen Telekommunikation und Internet Mindestspeicherfristen von einem Jahr oder länger für die bei der Nutzung dieser Medien anfallenden Verbindungsdaten einzuführen. Hiergegen haben die Europäischen Datenschutzbeauftragten anlässlich der Internationalen Datenschutzkonferenz vom 9. bis 11. September 2002 in Cardiff tief greifende Bedenken geäußert. In dem dort verabschiedeten „Statement of the European Data Protection Commissioners on mandatory systematic retention of telecommunication traffic data“ (s. Anlage 4) werden erhebliche Zweifel an der Rechtmäßigkeit des Vorschlags geltend gemacht. Diesen Beschluss der Europäischen Datenschutzkonferenz habe ich zum Anlass genommen, die Bundesregierung unter Bezugnahme auf ihre ablehnende Haltung gegenüber der Bundesratsinitiative um weitere Unterstützung bei den Beratungen des Ministerrats in Brüssel zu bitten. Das Thema war bei Redaktionsschluss noch nicht Gegenstand von Gesprächen auf Ministerebene. Auf Arbeitsebene haben jedoch bereits Beratungen, u. a. zu einem Entwurf der Multidisziplinären Gruppe „Organisierte Kriminalität“ begonnen. Darin wird gefordert, schon in nächster Zukunft bindende Regeln für die Angleichung der Vorschriften der Mitgliedsstaaten über die Pflicht zur Speicherung von Telekommunikationsdaten für Zwecke der Strafverfolgung festzulegen.

Auch die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 24./25. Oktober 2002 in Trier hat sich intensiv mit den Überlegungen zur Vorratsdatenspeicherung sowohl auf nationaler als auch auf europäischer Ebene beschäftigt und eine Entschließung „Systematische verdachtslose Datenspeicherung in der Telekommunikation und im Internet“ (s. Anlage 24) angenommen, in der die Bundesregierung aufgefordert wird, für mehr Transparenz der Beratungen auf europäischer Regierungsebene einzutreten und insbesondere einer Regelung zur flächendeckenden Vorratsdatenspeicherung nicht zuzustimmen.

11.3.4 Neue Informationen zum Auskunftsverfahren nach § 90 Telekommunikationsgesetz

Bereits in meinem letzten Tätigkeitsbericht habe ich ausführlich über das automatisierte Auskunftsverfahren gemäß § 90 TKG berichtet (s. 18. TB Nr. 10.3). Von besonderem datenschutzrechtlichen Interesse war die Klage von Mobilfunkanbietern gegen die Verpflichtung, den Namen, die Anschrift sowie die Rufnummer ihrer Kunden auch in den Fällen der so genannten Prepaid-Cards zu erheben und in das Auskunftssystem nach § 90 TKG einzustellen. Das Gerichtsverfahren ist gegenwärtig in letzter Instanz beim Bundesverwaltungsgericht anhängig. Mit einer Entscheidung wird noch im Jahr 2003 gerechnet. Nach einigen Anfangsschwierigkeiten ist das automatisierte Auskunftsverfahren mittlerweile etabliert. Trotz der hohen Abfragezahlen von etwa 40 000 Auskunftsbegehren pro Woche zeigten Kontrollen, dass es keine datenschutzrechtlich zu bemängelnden Auffälligkeiten gibt.

11.3.4.1 Novellierung von § 90 Telekommunikationsgesetz

Nachdem das Verwaltungsgericht Köln mit Urteil vom 22. September 2000 (AZ.: 1 1 K 7710/98) festgestellt hat, dass die Anbieter von Mobilfunkdiensten nicht verpflichtet sind, bei Verträgen über so genannte Prepaid-Cards Bestandsdaten ihrer Kunden zu erheben (s. dazu 18. TB Nr. 10.3.1), ist von der Bundesregierung gegen das Urteil Berufung eingelegt worden. Gleichzeitig hat das Bundesministerium für Wirtschaft und Technologie begonnen, den § 90 TKG – der die Auskunftsersuchen durch Sicherheitsbehörden auch im automatisierten Verfahren regelt – zu überarbeiten. Hintergrund dafür war, die Befugnis der Strafverfolgungs- und Sicherheitsbehörden, Informationen über Namen, Adresse sowie Rufnummer von Anschlussinhabern erhalten zu können, auch für den Bereich der Prepaid-Cards sicherzustellen.

Nach Ansicht der Bundesregierung sollten die Telekommunikationsunternehmen durch eine eindeutige Rechtsgrundlage verpflichtet werden, künftig die Daten aller ihrer Kunden – also auch derjenigen mit einem Prepaid-Vertrag – im automatisierten Abrufverfahren zur Verfügung zu stellen. Die Datenschutzbeauftragten des Bundes und der Länder haben die Entwürfe zur Erweiterung des § 90 TKG in einer gemeinsamen Entschließung vom 24. Mai 2002 kritisiert (s. Anlage 23). Nach den Vorschlägen der Bundesregierung wären die Unternehmen dazu gezwungen, Daten zu speichern, die für die Erbringung ihrer Dienste nicht erforderlich sind. Es käme also zu einer datenschutzrechtlich bedenklichen Vorratsdatenspeicherung. Auch die im Entwurf neu aufgenommene Verpflichtung, den Personalausweis zu prüfen, würde zusätzliche Informationen liefern, die für den Vertragsabschluss nicht benötigt werden. Ein weiterer Kritikpunkt betraf die vorgesehene Möglichkeit, mit unvollständigen oder ähnlichen Suchbegriffen bei der Abfrage der Kundendaten zu arbeiten.

Das Oberverwaltungsgericht Münster hat zwischenzeitlich über die Berufung entschieden und die Ansicht des Verwaltungsgerichts Köln nicht bestätigt. Eine schnelle Neuregelung des automatisierten Auskunftsverfahren ist deshalb zunächst zurückgestellt worden. Die Regelung wird im Rahmen der Novellierung des TKG überarbeitet werden. Das Verfahren befindet sich zurzeit in der Revisionsinstanz beim Bundesverwaltungsgericht.

11.3.4.2 Keine unzulässigen Abfragen

Gemäß § 90 Abs. 4 TKG protokolliert die Regulierungsbehörde für Telekommunikation und Post für Zwecke der Datenschutzkontrolle jede Datenabfrage. Dabei werden alle Daten des Abrufs und der Antworten der Telekommunikationsnetzbetreiber festgehalten. Wie ich in meinem letzten Tätigkeitsbericht dargestellt habe, war mir eine effektive Datenschutzkontrolle aufgrund der technischen Gegebenheiten zunächst nicht möglich (vgl. 18. TB Nr. 10.3.3). Mittlerweile konnten diese Schwierigkeiten nach einer Änderung in der Datenbank überwunden werden. So werden ein so genannter Hashwert, der aus der abgefragten Telefonnummer gebildet wird, und der Straßenname unverschlüsselt gespeichert. Wenn nun geprüft wird, ob in einem bestimmten Zeitraum eine Anfrage zu einer Person stattgefunden hat, können die infrage kommenden Protokolleinträge innerhalb weniger Minuten entschlüsselt werden. In einem zweiten Schritt kann geprüft werden, ob tatsächlich eine Abfrage zu dieser Person vorgenommen worden ist.

Meinen Kontrollen lagen zum Teil Eingaben zugrunde, in denen sich Bürger mit einem Verdacht an mich gewandt hatten, anhand ihrer Telefonnummer sei ihre Adresse ermittelt worden. Darüber hinaus gab es Fälle, bei denen Polizeidienststellen aufgrund interner Ermittlungen einen möglichen Missbrauch des Verfahrens befürchteten. Es konnte festgestellt werden, dass in keinem der geprüften Fälle eine Anfrage nach § 90 TKG gestellt wurde. Dabei konnte ich mich auch davon überzeugen, dass eine effektive Kontrolle des Verfahrens nun möglich ist.

Zum Mengengerüst der Abfragen nach § 90 TKG habe ich festgestellt, dass im Jahr 2000 wöchentlich 15 000 bis 20 000 Abfragen erfolgten. Diese Zahlen erhöhten sich im vergangenen Jahr auf ca. 25 000 bis 30 000 Anfragen pro Woche. Seit Ende des Jahres 2001 kann ein weiterer Anstieg der Abfragezahlen auf etwa 40 000 Fälle pro Woche beobachtet werden. Ich werde diese Entwicklung verfolgen und zusammen mit der Regulierungsbehörde für Telekommunikation und Post kritisch begleiten.

11.4 Missbrauch von 0190-Nummern

Würde man eine Rangliste von Bürgereingaben zu bestimmten Themen erstellen, wären die Beschwerden über den Missbrauch von so genannten Mehrwertdiensterufnummern sowie die damit verbundenen Belästigungen und Betrügereien mit an vorderster Stelle zu finden. Die Bandbreite der Missbrauchsfälle ist groß. Zu erwähnen ist zum einen die zunehmende Nutzung von Telekommunikationsanschlüssen für Werbezwecke mittels unverlangter Zusendung von Telefax-, SMS-Nachrichten oder E-Mails (s. hierzu auch Nr. 10.9), oft verbunden mit der Aufforderung, eine 0190-Nummer anzurufen. Dies führt nicht nur zu einer enormen Belästigung der Anschlussinhaber, sondern verursacht bei Faxsendungen auch zum Teil hohe Kosten für Toner und Papier. Die Methoden beim Missbrauch von Mehrwertdiensterufnummern sind aber auch noch dreister: So werden beispielsweise Besitzer von Handys unter Vortäuschung eines Bekanntschaftsverhältnisses oder eines Gewinns per SMS aufgefordert, eine kostspielige 0190-Rufnummer zurückzurufen. Schließlich werden in erheblichem Umfang auch Internetnutzer mittels Dialer-Programmen betrogen, die zur Herstellung einer Internetverbindung und zur Abrechnung von im Internet angebotenen Dienstleistungen dienen. Diese Dialer sind meistens so programmiert, dass der Aufbau einer kostenpflichtigen Internetseite über eine 0190-Rufnummer oder eine Auslandsrufnummer erfolgt, was der Nutzer nicht immer erkennen kann. Es treten auch Fälle auf, in denen Dialer-Software vom Nutzer sogar unbemerkt auf den PC herunter geladen worden ist. Die böse Überraschung kommt dann bei der nächsten Telefonrechnung.

Alle Fälle des Missbrauchs von Mehrwertdiensterufnummern haben eines gemeinsam: Es handelt sich weniger um ein Datenschutz- als vielmehr um ein Verbraucherschutzproblem. Den Bürgern, die sich an mich gewandt hatten, konnte ich daher im Rahmen meiner Zuständigkeit als Datenschutzaufsichtsbehörde in der Regel nur wenig weiterhelfen. Teilweise wurden zwar auch Verstöße gegen datenschutzrechtliche Bestimmungen vorgetragen. So wurde in den Fällen unverlangter elektronischer Werbung beispielsweise die Vermutung geäußert, der Telekommunikationsnetzbetreiber habe die Rufnummer ohne die erforderliche Einwilligung an Dritte zu Werbezwecken weitergegeben. Anhaltspunkte für eine derartige Datenschutzverletzung haben sich aber in keinem einzigen Fall ergeben. Die Rufnummern waren entweder in Telefonverzeichnissen veröffentlicht und damit für jedermann zugänglich oder sie wurden zum Teil durch die nicht unterdrückte Rufnummernübermittlung bekannt. Bei meinen Recherchen bin ich auf eine weitere mögliche Erklärung gestoßen, wie die Anbieter von Werbung an die Rufnummern gelangen. Häufig werden Rufnummern nämlich beliebig nach dem Zufallsprinzip generiert, ohne dass der Anschlussinhaber bekannt ist. Beim Versenden elektronischer Werbung wird dann in Kauf genommen, dass nicht jede generierte Rufnummer vergeben ist.

Einen gewissen datenschutzrechtlichen Bezug hatte der Missbrauch von Mehrwertdiensterufnummern bzw. dessen Bekämpfung aber in anderem Zusammenhang:

Die Frage, wie man sich gegen unerwünschte elektronische Werbung wehren kann, lässt sich rechtlich leicht beantworten. Nach der Rechtsprechung zum Gesetz gegen den unlauteren Wettbewerb ist es unzulässig, Werbung über Telekommunikationsanschlüsse zu versenden, wenn zwischen Absender und Empfänger keine Geschäftsbeziehung besteht. Der Betroffene kann den Absender daher auf Unterlassung verklagen und ggf. Schadensersatz in Anspruch nehmen. Dies gestaltete sich allerdings nicht immer einfach, denn es traten Schwierigkeiten bei dem Versuch auf, den Inhaber der 0190-Rufnummer zu ermitteln. Diese Rufnummern werden von der Regulierungsbehörde für Telekommunikation und Post (RegTP) in 1000er Blöcken Netzbetreibern zugeteilt, die sie in der Regel aber nicht selbst nutzen, sondern Serviceprovidern oder anderen Diensteanbietern zur Vermarktung überlassen. Die RegTP kann daher zwar

feststellen, welchem Netzbetreiber die Mehrwertdiensterufnummer zugeteilt worden ist. Sie kennt jedoch nicht den Endnutzer. Bei der Suche nach dem Absender unverlangter elektronischer Werbung musste sich der Betroffene daher an den Netzbetreiber und erforderlichenfalls an weitere Serviceprovider wenden. Diese sahen sich aber aufgrund einer datenschutzrechtlichen Bestimmung an einer Auskunft gehindert. Im Hinblick auf das so genannte Verbot der Inverssuche ist nämlich die Auskunftserteilung über Namen und andere Daten von Kunden, von denen nur die Rufnummer bekannt ist, unzulässig. Der Gesetzgeber hat aus diesem Grund zum Schutz der Betrof fenen im Unterlassungsklagengesetz (UKlaG) zusätzlich zu dem Auskunftsanspruch für Verbraucherschutzverbände nach § 13 UKlaG auch für jeden Einzelnen einen Anspruch gegenüber T elekommunikationsdiensteanbietern auf Auskunft über Namen und ladungsfähige Anschrift der am T elekommunikationsverkehr beteiligten Personen geschaf fen, soweit Unterlassungsansprüche wegen unverlangter Werbung, der Lieferung unbestellter Sachen und der Erbr ingung unbestellter Leistungen geltend gemacht werden sollen (§ 13a UKlaG). T rotz anfänglicher datenschutzrechtlicher Bedenken gegen einen solchen weitgehenden Auskunftsanspruch habe ich mich im Gesetzgebungsverfahren unter Berücksichtigung des hohen Verbraucherschutzinteresses letztlich nicht gegen diese Regelung gestellt.

Auch die weiteren Bemühungen der Bundesregierung zur Stärkung der Verbraucherrechte habe ich unterstützt. Ende 2002 war ich an der Vorbereitung des Entwurfs eines Gesetzes zur Bekämpfung des Missbrauchs von Mehrwertdiensterufnummern beteiligt, der u. a. die Einrichtung einer Datenbank bei der RegTP für alle Mehrwertdiensterufnummern vorsieht. Die Datenbank, aus der auch ersichtlich sein soll, an wen die einzelne Rufnummer weitergegeben worden ist, soll allgemein zugänglich sein und im Internet veröffentlicht werden. Um die Feststellung der Mehrwertdiensterufnummer für die Betrof fenen zu erleichtern, soll diese künftig vom Diensteanbieter stets ungekürzt gespeichert werden. Gegen eine solche Lockerung des Grundsatzes, dass die Zielrufnummern als Verbindungsdaten in der Regel um die letzten drei Ziffern zu kürzen sind, sofern der Kunde nichts anderes beantragt, habe ich nach gründlicher Interessenabwägung keine Einwände erhoben. Mit dem In-Kraft-Treten des Gesetzes ist voraussichtlich Mitte des Jahres 2003 zu rechnen.

11.5 Abgrenzung der Ordnungswidrigkeitstatbestände zwischen Telekommunikations-Datenschutzverordnung (TDSV) und BDSG

Ein Kunde, der entgegen seinem W unsch von einem Telekommunikationsdiensteanbieter in ein öf fentliches Kundenverzeichnis eingetragen worden war (vgl. zu dieser Problematik auch Nr. 11.13), hatte bei einer Polizeidienststelle Anzeige erstattet, weil er in dem Verstoß gegen § 13 Abs. 2 TDSV den T atbestand einer Ordnungswidrigkeit erfüllt sah.

Da bußgeldbewehrte Datenschutzverletzungen sowohl im BDSG als auch speziell für den Bereich der Telekommunikation im T elekommunikationsgesetz (TKG) bzw . in der TDSV aufgeführt sind, stellte sich die Frage nach der Abgrenzung zwischen diesen Vorschriften bzw. nach deren Anwendbarkeit. Während der auf der Grundlage von § 96 Nr. 9 TKG Ende 2000 neu in die TDSV aufgenommene Bußgeldkatalog (vgl. § 17 TDSV) für den Fall einer unzulässigen Veröffentlichung in Kundenverzeichnissen keine Sanktionen androht, ließe sich dieser Sachverhalt dagegen unter § 43 Abs. 2 Nr . 1 BDSG (unbefugte Erhebung oder V erarbeitung personenbezogener Daten, die nicht allgemein zugänglich sind) subsumieren.

Gegenüber der Regulierungsbehörde für T elekommunikation und Post (RegTP), die nach § 96 Abs. 2 TKG zuständige Verwaltungsbehörde für die Verfolgung von Ordnungswidrigkeiten im T elekommunikationsbereich ist, habe ich die Auffassung vertreten, dass die Ordnungswidrigkeitstatbestände im TKG und in der TDSV abschließend geregelt sind. Soweit die Absicht bestanden hätte, einen V erstoß gegen § 13 Abs. 2 TDSV mit einem Bußgeld zu bedrohen, hätte der Verordnungsgeber diesen Sachverhalt in den Katalog nach § 17 TDSV aufnehmen müssen. Da dies nicht geschehen sei, bestehe keine Möglichkeit, auf die allgemeinen Bußgeldvorschriften des BDSG zurückzugreifen. Die RegTP war ebenfalls der Meinung, dass die spezielleren Vorschriften der TDSV die Anwendbarkeit der allgemeinen Ordnungswidrigkeitstatbestände des BDSG für den Bereich des telekommunikationsspezifischen Datenschutzes ausschließen, und hat das eingeleitete Ordnungswidrigkeitsverfahren eingestellt.

Diese gemeinsame Auffassung wird im Übrigen auch durch die amtliche Begründung des V erordnungsgebers zu § 17 TDSV gestützt, in der das Erfordernis der Aufnahme eigener Bußgeldtatbestände damit begründet wird, dass die BDSG-Regelungen im T elekommunikationsbereich nicht gelten. Eine Anwendung der Vorschriften des BDSG auf Telekommunikationsdiensteanbieter kommt m. E. nur in Betracht, wenn es sich außerhalb des Anwendungsbereichs nach § 1 TDSV um Fragen handelt, die nicht telekommunikationsspezifische Regelungen betreffen, wie z. B. die Datenübermittlung an die SCHUF A oder andere W irtschaftsauskunfteien.

11.6 Datenschutzrechtliche Anforderungen an Location Based Services

Im Mobilfunkbereich werden neue Dienstleistungen angeboten, die dem Nutzer in Abhängigkeit von seinem Standort zur Verfügung gestellt werde n. Diese kann man kurz als standortbezogene Dienste bezeichnen, oder mit der üblichen englischen Bezeichnung Location Based Services (LBS). Die Anwendungsmöglichkeiten sind vielfältig: Hinweise auf in der Nähe gelegene Restaurants oder Kinos, Verkehrsinformationen, Einkaufshilfen, Suchfunktionen für Freunde. Diese Dienste können in unterschiedlichen Formen angeboten werden. Beim „Pull Dienst“ ruft der Nutzer den Dienst während der bestehenden Verbindung aktiv auf (z. B. W etterdienst, Staumeldung, Nachrichten). Bei „Push Diensten“ abonniert der Nutzer einen oder mehrere Dienste, die ihm dann an bestimmten Punkten durch das Unternehmen zur Verfügung gestellt werden. „T racking Dienste“ speichern jeden Wechsel der Mobilfunkz elle und der Kunde erhält dann eine entsprechende Mitteilung über den Aufenthaltsort des Teilnehmers (z. B. Flottensteuerung bei Transportunternehmen). Für das so genannte Routing ist keine genaue Lokalisierung notwendig. Bei Anruf einer überregionalen Ruf-

nummer wird der Anrufer an den für den Ort zuständigen Ansprechpartner weitergeleitet (z. B. Telefonseelsorge).

Für die Nutzung solcher Dienste stehen verschiedene, unterschiedlich genaue Lokalisierungstechniken zur Verfügung, auf die hier nicht detailliert eingegangen werden soll. Bei der Ermittlung der Funkzelle, in der der Kunde sich befindet, wird z. B. nur eine Genauigkeit zwischen 50 m und 10 km erreicht. Eine genauere Lokalisierung ist nur durch Kombination mit anderen Techniken und Verfahren möglich. Die genaueste Methode ist das Global Positioning System, bei dem die Ortung durch ein Satellitensystem erfolgt (auf ca. 10 m genau).

Die neuen Dienstleistungen bringen aus Sicht des Datenschutzes Risiken mit sich. Es besteht die Gefahr des gläsernen Mobilfunknutzers. So können Bewegungsprofile erstellt werden. Auch ist es technisch möglich, den persönlichen Lebensstil des Nutzers zu speichern und dessen Kaufverhalten abzufragen (Nutzerprofile). Außerdem würde ein entsprechender Datenpool von besonderem Interesse für die Strafverfolgungs- und Sicherheitsbehörden sein. Im deutschen Recht gibt es noch keine spezielle Rechtsgrundlage für die Erhebung der Lokalisierungsdaten. Deshalb ist die Einwilligung des Betroffenen notwendige Voraussetzung für die Übermittlung und Nutzung von Standortdaten. Damit verbunden ist eine vorherige und ausreichende Unterrichtung des Nutzers über die grundlegenden Verarbeitungstatbestände der Daten. Nur eine informierte Einwilligung des Nutzers legitimiert die Verarbeitung seiner Standortdaten. Dies kann beim Abschluss eines schriftlichen Vertrages unproblematisch gewährleistet werden.

Im Mobilfunk wird man aber im Regelfall die Form der elektronischen Einwilligung mittels Handy wählen, deren Voraussetzungen in § 89 Abs. 10 Telekommunikationsgesetz, § 4 Telekommunkations-Datenschutzverordnung geregelt sind. Allerdings ist danach eine Rücknahme dieser Einwilligung innerhalb einer Woche zulässig, sodass auch der Dienst theoretisch erst nach einer Woche angeboten werden könnte. Ein Angebot von LBS in dieser Form ist weder für Kunden noch Anbieter interessant.

Auch von meiner Seite wurde dieses Problem gesehen und mit der Regulierungsbehörde für Telekommunikation und Post und dem BMWi diskutiert. Es besteht Einvernehmen, dass die gesetzlich vorgesehene Rücknahmemöglichkeit nicht zu einem Aus für diese Dienste führen soll. Aus diesem Grund soll bis zu einer entsprechenden Regelung im deutschen Recht in diesem Punkt auf aufsichtsbehördliche Maßnahmen verzichtet werden. Voraussetzung ist dabei natürlich, dass die angebotenen Verfahren ansonsten datenschutzgerecht ausgestaltet sind.

Die europäische Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG vom 12. Juli 2002, s. Nr. 11.1.1) enthält in Artikel 9 eine entsprechende Regelung. Danach sind eine Einwilligung und eine vorherige Mitteilung erforderlich, für welche Zwecke und wie lange Daten verarbeitet werden und ob eine Weitergabe an Dritte erfolgt. Auch eine Rücknahme der Einwilligung für die Zukunft und eine zeitweise Untersagung der Übertragung der Daten muss auf einfache Weise und jederzeit möglich sein.

Diese Vorgaben sollten möglichst umfassend in Deutschland umgesetzt werden. Dabei muss genau geprüft werden, welche Voraussetzungen man an die Einwilligung stellt. Geregelt werden sollte auch die Frage, ob jedes Mal bei Nutzung eines Dienstes eine Einwilligung erforderlich ist, oder ob für einen bestimmten Dienst oder eine Dienstegruppe eine einmalige Einwilligung ausreicht. Diese Lösung wäre denkbar. Datenschutzrechtlich unzulässig wäre es allerdings, wenn der Nutzer mit einer einzigen Erklärung seine Einwilligung für alle denkbaren Dienste abgeben könnte. Wegen der teilweise sehr unterschiedlichen Ausgestaltung wäre es für den Kunden nicht möglich, im Voraus alle möglichen Alternativen zu bedenken und bei seiner Entscheidung zu berücksichtigen.

11.7 Datenschutzaspekte bei der Handyreparatur

Auf die mit der Reparatur eines Handys verbundenen Datenschutzprobleme habe ich bereits im 18. TB (Nr. 10.6.2) aufmerksam gemacht. Die dort wiedergegebenen Empfehlungen hinsichtlich der im Gerät gespeicherten Daten gelten unverändert fort. Hatte ich damals noch auf die Zuständigkeit der Aufsichtsbehörden für den nicht öffentlichen Bereich verwiesen, ergab sich im Berichtszeitraum die Notwendigkeit, die Problematik im Rahmen meiner Datenschutzaufsicht mit den Mobilfunkanbietern zu erörtern, die häufig selbst Reparaturaufträge ihrer Kunden entgegennehmen und ausführen. Dabei habe ich festgestellt, dass zwar überwiegend das so genannte Austauschverfahren angewandt wird. Die Kunden können jedoch auch eine Individualreparatur beauftragen, bei der sie ihr eigenes Handy zurückerhalten. Um diese Wahlmöglichkeit ausüben zu können, müssen die Kunden hierüber informiert werden. Ich habe die Mobilfunkanbieter daher aufgefordert, die Auftragsvordrucke entsprechend zu gestalten und ihre Kunden auch darüber aufzuklären, dass sie im Falle des Austauschverfahrens das abgegebene Handy, auf dem möglicherweise schützenswerte persönliche Daten gespeichert sind, nicht mehr zurückerhalten. Was die von mir vor Erteilung des Reparaturauftrags empfohlene Löschung der im Handy gespeicherten Daten angeht, kann natürlich über eine Eigenverantwortung der Kunden nicht hinweg gesehen werden. Gleichwohl erwarte ich von den Telekommunikationsdiensteanbietern, dass sie ihre Kunden auch umfassend informieren, wo ihre Kommunikationsdaten gespeichert sind und wie sie diese selbst löschen können. Unabhängig davon halte ich es für geboten, beim Austauschverfahren sicherzustellen, dass die gespeicherten Daten auch ohne ausdrücklichen Auftrag des Kunden vom Mobilfunkanbieter oder einem beauftragten Serviceunternehmen auf jeden Fall gelöscht werden. Nach meiner Einschätzung wird dies bereits so praktiziert. Damit ist gewährleistet, dass im Wege des Handyaustausches keine personenbezogenen Daten an Dritte gelangen.

11.8 Mithörschutz bei öffentlichen Telefonstellen

Noch gibt es die vertrauten gelben Telefonzellen, auch wenn die Bedeutung öffentlicher Fernsprecheinrichtungen angesichts der ständig steigenden Anzahl von Mobilfunkanschlüssen immer mehr abnimmt. Die Deutsche Telekom AG ist nach den Vorschriften des Telekommunikationsgesetzes und der Telekommunikations-Universaldienstleistungsverordnung verpflichtet, solche öffentlichen Telefonstellen entsprechend dem allgemeinen Bedarf flächendeckend bereitzustellen. Vorgaben

in Bezug auf die Ausstattung enthalten die Vorschriften nicht. In jüngster Zeit konnte man beobachten, dass geschlossene Telefonzellen zunehmend durch andere Einrichtungen wie Telefonhauben oder Telestationen ersetzt werden. Einige Bürger haben sich bei mir darüber beschwert, ein Teil der neuen öffentlichen Telefonstellen – vor allem die Telefonsäulen – würden keinen Schutz vor Wetter und insbesondere vor unerwünschten Mithörern bieten.

Aus den zum Schutz des Fernmeldegeheimnisses erlassenen Vorschriften lässt sich zwar keine Verpflichtung für einen Telekommunikationsdiensteanbieter herleiten, nur geschlossene Telefonzellen, die das Mithören von Telefongesprächen erschweren oder gar verhindern, bereitzustellen. Gleichwohl habe ich Verständnis für das Anliegen von Bürgern, die trotz des erreichten hohen Grades der Versorgung mit Festnetz- und Mobilfunkanschlüssen auf öffentliche Telefonstellen angewiesen sind und nicht möchten, dass ihre Gespräche von Dritten mitgehört werden. Aus diesem Grund habe ich die bei mir eingegangenen Beschwerden zum Anlass genommen, die Deutsche Telekom AG zu bitten, bei der Bereitstellung öffentlicher Telefonstellen ein Mindestmaß an Schutzvorrichtungen vorzusehen, die das Mithören wenigstens erschweren. Das Unternehmen hat mir zugesichert, das Konzept zur Aufstellung von öffentlichen Telefonstellen berücksichtige neben Kosten- und Genehmigungsgründen auch datenschutzrechtliche Aspekte. In der Planung sei vorgesehen, die kritisierten Telestationen regelmäßig mit einem Glasdach und einem Seitenteil zu versehen. Bereits errichtete Telestationen, bei denen diese Ausstattung fehlt, würden nachgerüstet. Bei Mehrfachstandorten sei ein Mindestabstand von etwa einem Meter vorgesehen. Unter Datenschutzgesichtspunkten werde insbesondere auch die Möglichkeit angeboten, die Anzeige der gewählten Rufnummer im Display zu unterdrücken, damit vorbeigehende Passanten die Rufnummer nicht erkennen können.

11.9 Inkassoverfahren durch Dritte

Viele Telekommunikationsdiensteanbieter führen bei Zahlungsverzug ihrer Kunden das außergerichtliche Mahnverfahren nicht selbst durch. Sie schalten hierzu und für die anschließende gerichtliche Beitreibung häufig Inkassounternehmen ein. Die Rechtsgrundlage für die dazu notwendige Übermittlung von Bestands- und Verbindungsdaten an Dritte findet sich in § 7 Abs. 1 Satz 2 und 3 Telekommunikations-Datenschutzverordnung (TDSV). Voraussetzung ist, dass der Dritte vertraglich zur Einhaltung des Fernmeldegeheimnisses sowie der einschlägigen datenschutzrechtlichen Bestimmungen der TDSV verpflichtet worden ist.

Die Möglichkeit, den Forderungseinzug einem Inkassobüro zu übertragen, hat im Jahr 2001 auch für Verbindungsnetzbetreiber, über die im sogenannten offenen Call-by-Call-Verfahren Telefongespräche geführt werden, an Bedeutung zugenommen. Der Anschlussnetzbetreiber, bei dem der Kunde seinen Telefonanschluss hat, ist zwar nach § 15 Telekommunikations-Kundenschutzverordnung nach wie vor verpflichtet, seinen Kunden eine Gesamtrechnung mit den Entgelten aller in Anspruch genommenen Diensteanbieter zu erstellen und geleistete Zahlungen anteilig an die anderen Unternehmen weiterzuleiten. Die Deutsche Telekom AG als größter Anschlussnetzbetreiber hat jedoch seit dem 1. Juli 2001 unter Aufgabe ihrer bisherigen Praxis das gesamte Reklamations- und Mahnwesen an die Call-by-Call-Anbieter abgegeben. Diese müssen jetzt nicht nur selbst das Mahnverfahren durchführen, sondern sind auch Ansprechpartner für Kundenbeschwerden, Rechnungsreklamationen und Rückfragen zu einzelnen Rechnungspositionen. Diese neue Situation hat die Call-by-Call- Anbieter bewogen, aus wirtschaftlichen Gründen ein externes Unternehmen mit dem Mahnverfahren und dem Forderungseinzug zu beauftragen. Die oftmals sehr geringen Rechnungsbeträge, die bei Call-by-Call-Gesprächen anfallen, können von den einzelnen Anbietern nämlich kaum kostendeckend beigetrieben werden. Auf dem Telekommunikationsmarkt wurden zu diesem Zweck Inkassounternehmen gegründet, die gleich mit mehreren Call-by-Call-Anbietern zusammenarbeiten und durch die Bündelung der Rechnungsbeträge zu einem effizienten Inkassoverfahren beitragen. Ihnen wurde nicht nur das Mahnverfahren, sondern darüber hinaus auch das gesamte Beschwerdemanagement übertragen.

Eines dieser Unternehmen hat sich im Bewusstsein der erforderlichen Sensibilität bei der Verarbeitung personenbezogener Daten gerade im Bereich des außergerichtlichen und gerichtlichen Mahnverfahrens an mich gewandt und um präventive datenschutzrechtliche Beratung gebeten. Zu diesem Zweck wurde mir das Betriebskonzept und ein hierzu eingeholtes Rechtsgutachten eines Experten für Telekommunikationsrecht vorgelegt. In einem Gespräch mit Vertretern des Unternehmens und dem sachverständigen Gutachter wurden die datenschutzrechtlichen Fragestellungen einvernehmlich erörtert.

Gegenstand der Erörterungen war auch die im Vorfeld zu klärende Frage, wer hier für die Kontrolle des Datenschutzes überhaupt zuständig ist. Da das Unternehmen selbst nicht Telekommunikationsdiensteanbieter im Sinne des Telekommunikationsgesetzes (TKG) und der TDSV ist, war zu prüfen, ob nach § 91 Abs. 4 TKG von meiner Zuständigkeit auszugehen ist oder die Datenschutzkontrolle gemäß § 38 BDSG in die Kompetenz der Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich fällt. Ich habe hierzu das Bundesministerium für Wirtschaft und Technologie sowie die Regulierungsbehörde für Telekommunikation und Post um Stellungnahme gebeten. Auch in der Arbeitsgruppe „Telekommunikation, Tele- und Mediendienste“ des Düsseldorfer Kreises als oberstes Koordinierungsgremium der obersten Aufsichtbehörden für den Datenschutz im nicht öffentlichen Bereich wurde das Problem beraten. Nach eingehender Prüfung aller Beteiligten wurde meine Kontrollzuständigkeit für das Factoring von Telekommunikationsdienstleistungen als Annex zu meinen Befugnissen nach § 91 Abs. 4 TKG anerkannt und die Anwendbarkeit dieser Vorschrift bejaht. Ausschlaggebend war die Überlegung, dass das Unternehmen zwar selbst keine Telekommunikationsdienste anbietet, jedoch eine über ein bloßes Inkasso hinausgehende telekommunikationsspezifische Tätigkeit ausübt und an der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirkt. Es verarbeitet und nutzt im Zuge des Inkasso- und Mahnverfahrens sowie im Rahmen des Beschwerdemanagements die zu diesem Zweck erhobenen personenbezogenen Daten. Im Übrigen war zu berücksichtigen, dass die Vorschrift des § 91 Abs. 4 TKG ihrem Sinn und Zweck nach eine Zersplitterung der datenschutzrechtlichen Kontrollzuständigkeit im Bereich der Telekommunikation gerade vermeiden will.

11.10 Datenschutzrechtlich relevante Serviceleistungen

Die heutzutage von den T elekommunikationsunternehmen angebotenen Serviceleistungen führen in der Regel zu einer besonderen Nutzung von V erbindungsdaten und berühren damit unmittelbar die datenschutzrechtlichen Interessen der von diesen Leistungen Betrof fenen. Dabei kann unterstellt werden, dass sie für die Nutzer einen Mehrwert darstellen, denn sonst würden sie von den Kunden der Unternehmen nicht nachgefragt werden. Gleichwohl ist dies nur die eine Seite der Medaille. Dies gilt beispielsweise für die Systeme, mit denen sich der Aufenthaltsort Dritter gegen deren W illen ausspähen lässt. In derartigen Fällen werde ich von betroffenen Bürgern, aber auch – etwa im Vorfeld der Einführung einer neuen Servicelei stung – von den Unternehmen selbst angesprochen und um Rat gefragt.

11.10.1 Die „Klingelmännchen und -mäuschen“ von heute

Im letzten Tätigkeitsbericht habe ich mich bereits zu dem neuen Dienst CallGuard geäußert, der Callcenter vor Scherz- oder Störanrufern schützen soll. Leider ist die Zahl der so genannten „Junk Calls“ nach wie vor erschreckend hoch, wobei solche Anrufe Nerven der Mitarbeiter kosten, Anrufe von echten Kunden blockieren und das betrof fene Unternehmen auch finanziell schädigen. Früher hat man als „Klingelmännchen oder -mäuschen“ aus Spaß an Haustüren geklingelt, heute scheint vor allem unter Jugendlichen das „Anklingeln“ von kostenlosen oder kostenreduzierten Service-Rufnummern (0800- und 0180-Nummern) als Zeitvertreib verbreitet zu sein, da es den Anrufer nichts oder nur wenig kostet.

Die Telekommunikationsunternehmen, die sich dieser Problematik seit einiger Zeit angenommen haben, haben inzwischen die so genannten Blac klist-Funktionen weiterentwickelt. Bei CallGuard erfolgt die Aufnahme in eine Sperrliste bereits dann, wenn das Gespräch eine bestimmte Dauer von beispielsweise we nigen Sekunden unterschreitet (Anrufer, die einfach auflegen nachdem die Verbindung zustande gekommen ist). Dies hat den Nachteil, dass auch Anrufer auf die Sperrliste kommen können, die versehentlich eine solche Servicerufnummer gewählt haben. Bei einem weiteren inzwischen angebotenen Programm erfolgt die Aufnahme in die Sperrliste auf V eranlassung des entsprechenden Callcenter-Mitarbeiters, z. B. durch Drücken einer bestimmten Tastenkombination während des Gespräches. Versucht nun ein solcher Anrufer die Service-Rufnummer erneut zu erreichen, werden die Daten gegeneinander abgeglichen. Stimmen die Rufnummern überein, wird der Anruf abgewiesen und der Anrufer erhält einen entsprechenden Hinweis.

Nach meiner Auf fassung handelt es sich bei der Speicherung der Daten in der Sperrliste und dem Datenabgleich um die Verarbeitung personenbezogener Daten im Auftrag des entsprechenden Kunden im Sinne des § 11 BDSG. Datenherr und für die Einhaltung der maßgeblichen Rechtsvorschriften Verantwortlicher wäre somit der Kunde (z. B. das Callcenter eines Unternehmens) und nicht der T elekommunikationsdiensteanbieter. Damit richtet sich die Datenverarbeitung nach allgemeinem Datenschutzrecht. Einschlägig ist insoweit § 28 BDSG. Insofern bleibe ich bei meiner bereits im 18. TB geäußerten Auffassung, wonach die Speicherung der Rufnummer von Scherz- oder Störanrufern in den Sperrlisten nur für eine begrenzte Frist erfolgen darf. Anderenfalls wären die Interessen der Betroffenen nicht angemessen berücksichtigt. In Abstimmung mit der Regulierungsbehörde für Telekommunikation und Post und aufgrund schon vorliegender Erfahrungen halte ich eine Dauer von maximal einer Woche für angemessen und verhältnismäßig. Bereits diese Sperrfrist führt zu einer deutlichen Reduzierung von Scherzanrufen. Wichtig sind in diesem Zusammenhang auch eindeutige Regelungen über das V erfahrensmanagement. So sollte der Zugrif f auf solche Dateien nur für wenige besonders berechtigte Personen wie Systemadministratoren freigeschaltet sein.

Da es sich um ein spezielles Problem in der T elekommunikation handelt, wäre eine entsprechende bereichsspezifische Datenschutzregelung für die Datenverarbeitung wünschenswert. Ich würde es begrüßen, wenn im Zuge der bevorstehenden Novellierung des Telekommunikationsgesetzes eine entsprechende Rechtsgrundlage geschaffen wird.

11.10.2 Voreinstellung der Rufnummernübermittlung

In meinem vorletzten Tätigkeitsbericht habe ich mich bereits ausführlich zum Thema der Rufnummernübermittlung geäußert (17. TB Nr. 10.2.8). Damals ging es mir in erster Linie um eine Information über die damit zusammenhängenden datenschutzrechtlichen Anforderungen und Pflichten zur Information der Kunden durch die T elekommunikationsunternehmen.

Inzwischen werden die Kunden in der Regel ausreichend informiert. Es gibt in Einzelfällen aber immer noch Defizite. So habe ich z. B. auf einem Formular für die Beantragung eines ISDN-Anschlusses kein e Informationen über die bestehenden Wahlmöglichkeiten des Kunden zur Anzeige seiner Rufnummer bei Anruf (CLIP – calling line identification presentation) oder zur Unterdrückung der Rufnummernanzeige (CLIR – calling line identification restriction) vorgefunden. Es gab lediglich einen Hinweis in der Gerätebeschreibung, was nicht ausreichend ist. Die erforderlichen Informationen werden inzwischen auf dem entsprechenden Antragsformular selbst gegeben.

Ferner habe ich festgestellt, dass bei Mobilfunkgeräten, insbesondere bei Prepaid-Produkten, die Standardeinstellungen (default setting) der Handys eine permanente Rufnummernübermittlung vorsehen, was nach meiner Auf fassung – bei enger Auslegung – nicht im Ei nklang mit den Vorschriften der Telekommunikations-Datenschutzverordnung (TDSV) steht. Da die überwiegende Mehrheit der Mobilfunkkunden keinen Eintrag ins öf fentliche Kommunikationsverzeichnis beantragt, müsste der Kunde nach § 11 Abs. 3 TDSV die Übermittlung seiner Rufnummer ausdrücklich wünschen, also eine Willenserklärung abgeben. Allerdings halte ich es auch für ausreichend, wenn der Mobilfunkanbieter bei V ertragsabschluss seine Kunden deutlich auf die vorhandene Standardeinstellung hinweist und über die Möglichkeit zur Änderung dieser Voreinstellung informiert.

11.10.3 Rückruf bei Nichtmelden

Der Einzug der Digitaltechnik im Bereich der T elekommunikationsanlagen brachte nicht nur eine Fülle an nützlichen

Funktionen, sondern auch fast unbemerkt eine veränderte Gefährdungslage für das Fernmeldegeheimnis. Die denkbaren Angriffe bestehen auch in der missbräuchlichen Nutzung vorhandener Funktionalitäten. Die Verhinderung des Missbrauchs dieser durchaus gewünschten und nützlichen Funktionalitäten bedarf einer Reihe von Maßnahmen, die gewährleisten, dass den datenschutzrechtlichen Vorschriften Rechnung getragen wird. Ein Beispiel hierfür ist der so genannte „Rückruf bei Nichtmelden", den verschiedene Netzbetreiber ihren Kunden anbieten. Dieses Leistungsmerkmal löst eine automatische Mitteilung an den Anrufer, der einen Angerufenen nicht erreicht hat, aus, sobald der Angerufene wieder telefoniert bzw. den Hörer betätigt hat. Manche Telefonkunden möchten aber nicht, dass Dritte erfahren, ob sie in der Zwischenzeit telefoniert haben, oder sie befürchten, dass Dritte auf diese Art und Weise erfahren, ob sie zu Hause sind oder ob ungebetene Besucher freies Feld haben. Aufgrund einer Reihe von Beschwerden, die wegen solcher Befürchtungen an mich gerichtet worden sind, habe ich mich im Berichtszeitraum mit der datenschutzrechtlichen Bewertung dieser Funktion bei einem großen Telekommunikationsunternehmen beschäftigt.

Nach eingehender Prüfung der Informationen über die Ausgestaltung des Leistungsmerkmals und über die technischen Details konnte ein Verstoß gegen datenschutzrechtliche Bestimmungen im Bereich der Telekommunikation nicht festgestellt werden. Meine Rechtsauffassung wird auch von der Regulierungsbehörde für Telekommunikation und Post geteilt, mit der ich mich dies bezüglich in Verbindung gesetzt habe. Nach meiner Einschätzung kann das Leistungsmerkmal nicht als geeignetes Instrument zur Überwachung der Telekommunikation angesehen werden, weil der Verbindungsversuch lediglich für drei Stunden gespeichert und danach gelöscht wird. Zudem wird der Rückruf durch jede Aktivität beim angerufenen Anschluss, zum Beispiel bereits durch Abheben und Auflegen des Telefonhörers, ausgelöst, sodass der Anrufer nicht erfährt, ob der Angerufene ein Telefongespräch geführt hat. Wegen der relativ kurzen Speicherdauer kann diese Funktion noch als Speicherung von Verbindungsdaten zum Aufbau einer weiteren Verbindung angesehen werden. Dies ist nach § 6 Abs. 2 TDSV ausdrücklich zugelassen.

Für alle, die sich persönlich besonders stark von dem Leistungsmerkmal in ihrer Privatsphäre gestört fühlen, folgender Tipp: Beim Anschluss eines Anrufbeantworters, der sich nach dem ersten Klingeln einschaltet, kann der Anrufer den Rückruf nicht aktivieren.

11.10.4 Wo ist er denn?

Moderne Kommunikationsmittel können zur Verbesserung der Sicherheit eingesetzt werden. So wird beispielsweise eine zusätzliche Hardware für das Handy angeboten, die mittels SMS einen Alarm aussendet, wenn das Handy einen vorgegebenen Bereich verlässt. Mithilfe dieser Technik können Eltern beispielsweise informiert werden, wenn ihr Kind zu weit vom Weg in den Kindergarten abkommt. Das Handy kann dann auch angerufen werden, um unauffällig zu hören, ob sich das Kind in einer gefährlichen Situation befindet. Was bei einem Kindergartenkind eine gewisse Sicherheit vermittelt, wird von einem Jugendlichen sicherlich als Bevormundung und Überwachung verstanden. Hier müssen die Erziehungsberechtigten verantwortungsvoll prüfen, ob und wann ein solches Gerät angemessen ist. Gleichfalls kann es aber auch, etwa im Handschuhfach eines Autos versteckt, zur Überwachung von Personen missbraucht werden. Demnächst wird eine Überwachungskamera auf den Markt kommen, mit der man sich das aktuelle Bild per Multimedia Messaging Service auf das Handy schicken lassen kann. Ein Bespitzeln Dritter ist mit diesen Produkten ohne weiteren Aufwand möglich. Wie bei vielen Dingen des täglichen Lebens gilt auch hier, dass sie sinnvoll, aber auch zum Schaden für Andere eingesetzt werden können. Gerade im Bereich der neuen Technologien ist daher ein verantwortungsvoller Umgang mit den Produkten gefordert.

Das gleiche gilt für bestimmte Dienste in den Mobilfunknetzen. So bietet etwa ein Mobilfunknetzbetreiber einen Dienst an, mit dem ein verlegtes Handy gefunden werden kann. Dabei wird der ungefähre Standort im Internet auf einer Karte sichtbar gemacht. Dieser Dienst kann sinnvollerweise u. a. dazu genutzt werden, den Standort eines Außendienstmitarbeiters zu erfahren, ohne ihn durch ständige Anrufe zu stören. Obwohl der Dienst passwortgeschützt ist, bestand bei seiner Nutzung ein hohes Missbrauchspotenzial. Auf meine Anregung hin hat der Netzbetreiber eingeführt, dass bei jeder Ortung eine entsprechende Kurzmitteilung an das Handy gesendet wird. Wenn nun der Handybesitzer gegen seinen Willen geortet und ihm dies automatisch mitgeteilt wird, kann er darauf reagieren. Der neugierige Mitmensch hat dann das Nachsehen. Dieses Beispiel zeigt, wie durch eine kleine Änderung die Möglichkeit, einen Dienst zu missbrauchen, deutlich reduziert werden kann, ohne seine Nutzung einzuschränken.

11.11 Einzelverbindungsnachweis

Der Einzelverbindungsnachweis (EVN) wird einzig zu dem Zweck erstellt, um den Anschlussinhaber in die Lage zu versetzen, die Höhe seiner Telefonrechnung detailliert nachvollziehen zu können, da dort jede entgeltpflichtige Verbindung im Einzelnen aufgelistet ist. Andere Nutzungsmöglichkeiten des EVN sind dagegen ausgeschlossen. So darf beispielsweise ein Unternehmen, auch soweit es die Kosten für die bei ihm eingehenden Telefonate übernimmt, keinen EVN mit der Angabe der vollständigen Rufnummern erhalten, um damit das Anrufverhalten seiner Kunden auswerten und konkrete Werbemaßnahmen vornehmen zu können.

11.11.1 Entgeltfreie Verbindungen – nicht auf der Rechnung

Nach § 7 Abs. 3 Telekommunikations-Datenschutzverordnung hat der Diensteanbieter unmittelbar nach Beendigung der Verbindung aus den erhobenen Verbindungsdaten die für die Berechnung des Entgelts erforderlichen Daten zu ermitteln und nicht erforderliche Daten unverzüglich zu löschen. Bei entgeltfreien Verbindungen besteht daher keine Notwendigkeit, solche Verbindungsdaten nach Versendung der Rechnung abzuspeichern. Dies gilt beispielsweise für Verbindungen zu 0800-Rufnummern, die für den Anrufer kostenfrei sind. Das hat für die Kunden, die einen EVN beantragt haben, zur Folge, dass dort nur die entgeltpflichtigen Verbindungen aufgeführt werden dürfen. Damit wird das Fernmeldegeheimnis, dem auch die im EVN aufgeführten Verbindungsdaten unterliegen, nur so weit eingeschränkt, wie es zugunsten der Transparenz der Rechnung erforder-

lich ist. Die Daten müssen allerdings so aussagekräftig sein, dass Höhe und Richtigkeit der für die einzelnen Verbindungen geltend gemachten Entgelte nachprüfbar sind. Da die oben erwähnten Verbindungen als solche gar nicht entgeltrelevant sind, dürfen diese auch nicht in der Rechnung ausgewiesen werden.

11.11.2 Sollen auch Angerufene einen Einzelverbindungsnachweis erhalten?

Nicht nur der Anrufer, sondern auch der Angerufene kann in bestimmten Fällen einen EVN zur Prüfung der Abrechnung erhalten. Dies gilt etwa für die oben erwähnten 0800er Rufnummern, bei denen nur dem Angerufenen Kosten entstehen. Dabei wäre die Angabe der vollständigen Rufnummer auf dem EVN allerdings nicht datenschutzgerecht. Unabhängig von der Nutzung der Rufnummernunterdrückung könnte der Inhaber der 0800er Rufnummer dann nämlich den Anrufer identifizieren. Deshalb darf nur die um drei Stellen verkürzte Rufnummer auf dem EVN erscheinen. Diese Auffassung, die ich schon früher vertreten habe, ist nunmehr durch die Regelung in der Telekommunikations-Datenschutzverordnung aus dem Jahr 2000 eindeutig bestätigt worden.

Bei bestimmten anderen Rufnummern sind die Verbindungsdaten sowohl für den Anrufer als auch für den Angerufenen abrechnungsrelevant, so etwa bei 0180er und 0190er Rufnummern. Aber auch hier dürfen die Angerufenen im Rahmen des EVN nur die gekürzten Rufnummern erhalten. Bei den 0190er Rufnummern gilt zwar die Besonderheit, dass der Angerufene nicht für die von ihm erbrachte Dienstleistung zu zahlen hat, sondern vielmehr selbst ein entsprechendes Entgelt erhält. Neben dem Abrechnungsverhältnis mit dem Endkunden besteht aber noch zusätzlich ein Vertragsverhältnis mit dem Telekommunikationsunternehmen, das den Dienst technisch durchführt. Um diese Besonderheit angemessen berücksichtigen zu können, habe ich mich mit der Regulierungsbehörde für Telekommunikation und Post darauf verständigt, dass bei den 0190er Rufnummern auch dem angerufenen Diensteanbieter ein EVN ausgestellt werden darf.

EVN, die teilweise auch kurzfristig elektronisch abgerufen werden können, haben für die Diensteanbieter noch eine weitere wirtschaftliche Bedeutung. So kann mithilfe der Auswertung der Rufnummern etwa die Wirksamkeit von regionalen Werbemaßnahmen beurteilt werden. Da die letzten drei Ziffern gekürzt sind und damit der einzelne Nutzer nicht erkennbar ist, bestehen von Seiten des Datenschutzes keine Bedenken gegen eine solche Auswertung.

11.12 Öffentliche Kundenverzeichnisse

Öffentliche Kundenverzeichnisse, also Telefonbücher und CD-ROM, sowie Abfragen über das Internet und die telefonische Auskunft werden gerne genutzt, und viele Telefonteilnehmer wollen so auch erreichbar sein – aber nicht alle. Oftmals hat der Teilnehmer gute Gründe, seine Rufnummer oder Adresse nicht publik werden zu lassen. Gleichwohl passiert es immer wieder, dass gegen den Willen des Anschlussinhabers seine Daten veröffentlicht werden. Ein Beispiel, das auch in der Presse nachzulesen war, betraf ein Frauenhaus in Tübingen. Damit war nicht nur der Aufenthaltsort der dort betreuten Frauen offenkundig geworden. Es entstand auch beträchtlicher materieller Schaden, da das Frauenhaus sich gezwungen sah, umzuziehen.

Bei den Betroffenen, die sich wegen eines Falscheintrags ihrer Daten an mich gewandt haben, handelt es sich im Wesentlichen um Kunden der Deutschen Telekom AG (DTAG). Auf meine Nachfrage hat die DT AG im Regelfall angegeben, dass ein „individueller Arbeitsfehler“ Ursache für den unerwünschten Eintrag gewesen sei. Auffällig war, dass der Kunde häufig keinen neuen Anschluss beantragt, sondern den vorhandenen nur geändert haben wollte, so z. B. die Umwandlung eines analogen in einen ISDN-Anschluss. Während früher in diesen Fällen alle Vertragsangaben neu erhoben werden musste n, werden mittlerweile die bisherigen Daten übernommen und nur bei Bedarf aktualisiert. Damit konnte die DT AG eine wesentliche Fehlerquelle ausschließen. Gleichwohl bedarf es auch weiterhin der intensiven Schulung der mit der Auftragsannahme betrauten Mitarbeiter, um individuellen Fehlern vorzubeugen.

Verbesserungsbedarf sehe ich auch bei der Bearbeitung von Kundenbeschwerden. So hatten sich in der Vergangenheit vermehrt Kunden vergeblich an die DTAG gewandt, um den Falscheintrag ihrer Daten korrigieren zu lassen. Erst nachdem sie sich wegen der mangelhaften Bearbeitung ihres Anliegens an mich gewandt hatten, wurde ihrem Wunsch entsprochen.

Schließlich stellte sich heraus, dass eine fehlerhafte Software in vielen Fällen das korrekte Entfernen von Einträgen unmöglich gemacht hatte. Es dauerte einige Monate, bis dieser Fehler beseitigt wurde.

Fehler bei der Bearbeitung von Kundendaten betreffen im Übrigen nicht nur den Telefonbucheintrag. Mir ist auch ein Fall bekannt geworden, bei dem ein Kunde keine Rechnung mehr erhielt. Da der Rechnungsbetrag, der unverändert vom Konto abgebucht wurde, nicht auf fällig war, bemerkte der Kunden dies erst gar nicht. Schließlich stellte sich heraus, dass die Rechnungsanschrift falsch eingegeben war und ein anderer Kunde die Rechnungen mit Einzelverbindungsnachweis erhalten hatte.

11.13 Inflation der Verbindungsdaten

Als in den Vermittlungsstellen der Fernmeldeämter noch die Relais klapperten, gab es praktisch keine Verbindungsdaten, sondern nur eine mechanische Zählung der Gesprächseinheiten. Heute sieht die Telekommunikationswelt jedoch anders aus. Die Daten einer Kommunikationsverbindung werden häufig nicht nur einmal, sondern mehrfach und dann noch an verschiedenen Stellen gespeichert. So beispielsweise beim so genannten Call-by-Call Verfahren, wenn die Daten für die Abrechnung auch bei dem alternativen Netzbetreiber entstehen. Meist erstellt dieser keine eigene Rechnung, sondern übermittelt die Verbindungsdaten an die Deutsche Telekom AG (DTAG), damit diese dem Kunden eine Gesamtrechnung ausstellen kann. Bei entsprechendem Wunsch des Kunden finden sich diese Daten dann auch auf dem Einzelverbindungsnachweis. Für die Bearbeitung von Kundenbeschwerden über die von Call-by-Call-Anbietern erhobenen Entgelte übermittelt die DTAG die Verbindungsdaten, zusammen mit weiteren Informationen, etwa dem Namen und der Anschrift des Kunden, wieder zurück an den alternativen Netzbetreiber. Sollte dieser nicht selbst die

Beschwerden bearbeiten, werden die Daten schließlich an ein Abrechnungsunternehmen weitergegeben.

Verbindungsdaten werden von den Telekommunikationsunternehmen aber auch erfasst, damit diese untereinander die Kosten für die Weiterleitung der Gespräche, die so genannten Interconnectiongebühren, abrechnen und prüfen können. Weiterhin dürfen Verbindungsdaten zur Verhinderung einer unberechtigten Nutzung von Telekommunikationsdiensten oder auch – sofern der Kunde zugestimmt hat – zur bedarfsgerechten Gestaltung von Telekommunikationsdiensten verarbeitet und genutzt werden. Soviel zur Theorie, bei der es schon mühsam ist, die Übersicht über die verschiedenen Stellen zu behalten, die die Daten eines Telefonats speichern.

Die Praxis der Verarbeitung von Verbindungsdaten bereitet zusätzliche Probleme für den Datenschutz. Dies gilt beispielsweise für die Sicherungskopien (Backup), die von den Telekommunikationsunternehmen gefertigt werden. Diese enthalten z. T. Verbindungsdaten, die nicht abrechnungsrelevant sind und daher nicht über die gesetzliche Frist hinaus gespeichert werden dürfen. Da diese Daten für die Telekommunikationsunternehmen aber Geld wert sind, stoße ich mit meiner Forderung auf Datenlöschung auf wenig Verständnis.

Problematisch sind auch die mehrjährigen handels- und steuerrechtlichen Aufbewahrungspflichten für Rechnungen. Diese rechtfertigen nach Auffassung eines Call-by-Call Anbieters auch die entsprechend lange Speicherung der vollständigen Einzelverbindungsdaten. Folgerichtig waren in diesem Fall alle Verbindungsdaten seit Gründung des noch recht jungen Unternehmens verfügbar. Die vollständige Zielrufnummer und genaue Uhrzeit ist meines Erachtens jedoch für handels- und steuerrechtliche Zwecke nicht erforderlich.

In einem anderen Unternehmen wird die Zielrufnummer der Verbindungen vollständig in eine Datenbank übernommen, auch wenn dies nicht dem Kundenwunsch entspricht. Dort bleibt der Datensatz noch etwa drei Monate zur Bearbeitung möglicher Kundenbeschwerden erhalten. Der Netzbetreiber argumentiert, dass er diese Daten gesperrt habe, da nach Rechnungserstellung kein Zugriff auf die vollständigen Rufnummern erfolge und sie damit von ihm nicht genutzt würden. Lediglich die entsprechend dem Kundenwunsch zusätzlich gespeicherte Zielrufnummer werde noch verwendet. Diese Auffassung verkennt, dass das Löschungsgebot nicht durch das Sperren von Daten erfüllt werden kann.

Nach meinen Erfahrungen wird noch viel Arbeit erforderlich sein, um die Unternehmen von einem sparsamen Umgang mit Verbindungsdaten zu überzeugen, auch wenn das Speichern in manchen Fällen einfacher ist.

11.14 Nutzung von Bestandsdaten zu Werbezwecken in der Telekommunikation

Die einen finden es nur lästig, andere begrüßen die zusätzlichen Informationen. Heute ist es üblich, dass fast bei jeder von den Telekommunikationsunternehmen übersandten Rechnung Werbematerial beigefügt ist. Oftmals ist es schwierig zu unterscheiden, ob solche Materialien nützliche Informationen für die eigene Vertragsgestaltung oder nur allgemeine Werbung enthalten. Gerade dieser Unterschied ist aber für die datenschutzrechtliche Bewertung dieses Sachverhalts wichtig, wobei ich wegen der Schwierigkeit der Abgrenzung in manchen Fällen einen eher großzügigen Maßstab bei der Prüfung anlege.

Nach § 89 Abs. 2 Nr. 1 Buchst. a Telekommunikationsgesetz (TKG) bzw. § 5 Abs. 1 Telekommunikations-Datenschutzverordnung (TDSV) ist die Verarbeitung und Nutzung von Bestandsdaten von Kunden für die inhaltliche Ausgestaltung oder Änderung des Vertragsverhältnisses auch ohne Einwilligung des Betroffenen möglich. Dies gilt jedoch nicht für die Nutzung solcher Daten für Zwecke der Werbung, Kundenberatung oder Marktforschung gemäß § 89 Abs. 7 TKG bzw. § 5 Abs. 2 TDSV. In diesen Fällen ist die ausdrückliche Einwilligung des Betroffenen erforderlich. Dies geschieht in der Regel bei Abschluss von Telekommunikationsverträgen, in dem man auf dem Antragsformular die entsprechende Textpassage (ich stimme zu, dass ...) ankreuzt.

Vor diesem Hintergrund kann man etwa Hinweise auf neue oder günstigere Tarife, auf neue Handys oder Telefonendgeräte noch zur inhaltlichen Ausgestaltung von Telekommunikationsverträgen rechnen. Als reine Werbung, die der ausdrücklichen Zustimmung bedarf, sind dagegen allgemeine Kundeninformationen über das Unternehmen ohne Bezug zum bestehenden Vertragsverhältnis anzusehen. Unzulässig in diesem Zusammenhang ist auf jeden Fall eine Werbung für Drittfirmen, wenn die Einwilligung nicht erteilt wurde.

11.15 Erfahrungsbericht: Telekommunikationsanlagen bei Bundesministerien II

In meinem letzten Tätigkeitsbericht (Nr. 10.16) habe ich von einer Umfrage bei den Bundesministerien berichtet, in der ich nach der Verarbeitung der Verbindungsdaten in den Telekommunikationsanlagen gefragt hatte. Bei vier Ministerien habe ich im Berichtszeitraum einen Beratungs- und Kontrollbesuch durchgeführt und konnte mich von der praktischen Umsetzung der Anforderungen überzeugen. Dabei war nicht alles problemlos.

In einem Fall waren z. B. noch Verbindungsdaten aus etwa zweieinhalb Jahren unzulässigerweise gespeichert, darunter sogar die vollständigen Gesprächsdaten des Ministers und der Personalräte. Entsprechend der Dienstvereinbarung hätten von diesem Personenkreis die Rufnummern der dienstlichen Gespräche gar nicht erst erhoben werden dürfen. Bei den privaten Gesprächen aller Mitarbeiter hätten zudem die letzten zwei Stellen der Zielrufnummer gelöscht werden müssen. Schließlich wurde entgegen den Regelungen der Dienstanschlussvorschriften (DAV) bzw. der eigenen Dienstvereinbarung auch die Uhrzeit der Verbindung erfasst.

Wenn dabei keine sensiblen Daten einsehbar sind, habe ich nichts gegen eine bei Bedarf freigeschaltete Fernwartung einer Telekommunikationsanlage einzuwenden. Erhebliche Bedenken hatte ich insoweit allerdings bei einem Datenbankserver, auf dem die Verbindungsdaten gespeichert wurden. Hierbei war es einer privaten Firma über einen Fernwartungszugang möglich, auf die Daten zuzugreifen, ohne dass eine wirkungsvolle Kontrolle stattfand.

Auch wenn dies außer gewöhnliche Beispiele sind, konnte generell festgestellt werden, dass zwischen der Theorie in

den Dienstvereinbarungen und der Praxis erhebliche Unterschiede bestehen. Die Dienstvereinbarungen werden meist an neue technische und organisatorische Verhältnisse nicht angepasst oder ihre Umsetzung stößt auf technische Probleme, die nicht angemessen gelöst werden. In einigen Fällen fehlt es auch an der Sensibilität für den Datenschutz, etwa wenn Ausdrucke von Dienstgesprächen dann vernichtet werden, wenn der Schrank voll ist. Eine Anweisung zur Aufbewahrungsdauer gab es in diesem Fall nicht.

Entsprechend den Regelungen der DAV erfolgt ein Ausdruck der Liste der Privatgespräche nur dann, wenn der Mitarbeiter dies im Einzelfall wünscht, etwa wenn der zu zahlende Betrag ungewöhnlich hoch ist. In vielen Ministerien wird jedoch immer ein Einzelverbindungsnachweis erstellt. Es ist nun einerseits bequem und heute durchaus üblich, einen Einzelverbindungsnachweis zu erhalten. Andererseits werden damit aber sensible Daten entgegen einer bestehenden Regelung verarbeitet. Gleichwohl hat sich kein einziger Mitarbeiter bei mir bislang über diesen Abrechnungsmodus beschwert. Ich habe daher von der Forderung abgesehen, hier unmittelbar das Verfahren zu ändern, zumal seit längerem eine Überarbeitung der DAV geplant ist. Es kann abgewartet werden, wie die Regelungen der neuen DAV in diesem Bereich ausfallen.

Auch neue technische Entwicklungen sind von Seiten des Datenschutzes zu berücksichtigen. So war beispielsweise in einem Ministerium ein CTI-System (Computer Telephony Integration) eingeführt worden. Über den PC des jeweiligen Mitarbeiters können die letzten Telefonverbindungen und Anrufversuche eingesehen werden und sein Telefon ferngesteuert werden. Dieses System kann in vielen Fällen die Arbeit erleichtern. So muss man Telefonnummern nicht nochmals heraussuchen, ein Mausklick genügt für die erneute Anwahl. Andererseits muss den Mitarbeitern aber mitgeteilt werden, dass hier eine weitere Speicherung aller Verbindungsdaten stattfindet und dass sie diese Daten löschen können. Nur ein Mitarbeiter, der darüber informiert ist, kann etwa den Eintrag zu einem vertraulichen Privatgespräch entfernen.

Nach diesen Erfahrungen möchte ich meine Empfehlung an die behördlichen Datenschutzbeauftragten nochmals wiederholen, die Verarbeitung der Verbindungsdaten der Telekommunikationsanlagen zu kontrollieren. Hier sollte nicht nur betrachtet werden, welche Daten ausgedruckt werden, sondern auch, welche Daten wie lange in der Datenbank tatsächlich gespeichert sind. Weiterhin sollte geprüft werden, ob technische Neuerungen eine Anpassung der Dienstvereinbarung erforderlich machen.

11.16 ... und in der Pause wird gesurft. Dienstliche und private Internetnutzung am Arbeitsplatz

Das Internet hat auch vor deutschen Amtsstuben nicht Halt gemacht. Denn dieser vielfältigen Informationsquelle, die die Arbeit erwiesenermaßen erleichtert und beschleunigt, will sich die Moderne Verwaltung eines Modernen Staats erklärtermaßen nicht verweigern. So werden immer mehr Arbeitsplätze mit einem direkten Zugang zum Internet ausgestattet. Und schon fast zwangsläufig stellt sich dann die Frage, ob und, wenn ja, unter welchen Bedingungen neben der dienstlichen auch die private Nutzung zugelassen werden soll.

Da die Antwort nicht unbedingt auf der Hand liegt, haben sich mehrere Behörden mit der Bitte um Beratung und Unterstützung an mich gewandt. Hierbei zeigte sich, dass die Bereitschaft gewachsen ist, die private Nutzung in einem begrenzten Maße zu erlauben – vermutlich als Folge der Einsicht, dass die Natur des Internet eine strikt dienstliche Nutzung kaum zulässt und dass ein Verbot das programmatisch von oberster Stelle verkündete „Internet für alle“ Lügen strafen würde.

In einem Leitfaden habe ich daher ein Modell entwickelt, das die private Nutzung von Internetdiensten in geringem Umfang und unter bestimmten Bedingungen erlaubt. Um in diesem Fall zu einer datenschutzgerechten Lösung zu kommen, gilt es nicht nur unterschiedliche gesetzliche Regelungen im Bereich der dienstlichen und der privaten Nutzung sinnvoll und praktikabel zu verzahnen, sondern auch die berechtigten Interessen des Dienstherrn an einer angemessenen Kontrolle und die der Beschäftigten an einer unbeobachteten Nutzung in Einklang zu bringen.

Der Leitfaden enthält neben allgemeinen datenschutzrechtlichen Grundsätzen für die dienstliche und für die private Nutzung auch solche, die bei der Protokollierung der Verbindungs- und Nutzungsdaten, besser bekannt als „Surf-Daten“, umgesetzt werden sollten und die – dem Motiv „Datensparsamkeit“ folgend – unabhängig von der Art der Nutzung gelten. In einer Muster-Dienstvereinbarung, die diese Grundsätze abbildet und den inhaltlichen Rahmen für die Nutzung der Internetdienste absteckt, sind datenschutzrechtlich vertretbare Kontrollmaßnahmen durch den Dienstherrn und Regelungen bei missbräuchlicher oder unerlaubter Nutzung festgelegt. Die Kontrollmaßnahmen beziehen sich gleichermaßen auf die dienstliche und – durch Einwilligung des einzelnen Beschäftigten – auch auf die private Nutzung, da eine technische Trennung zwischen diesen Bereichen in dem dargestellten Modell nicht vorgesehen ist. Der Leitfaden ist auf meiner Internetseite unter www.bfd.bund.de/information/Leitfaden.pdf abrufbar.

Ob der Dienstherr auch mit weniger Kontrolle auskommen kann, liegt in seiner Entscheidung. Das gilt auch für die Frage, ob er die private Nutzung des Internetzugangs überhaupt erlaubt oder eher ein anderes Modell – z. B. ein behördliches Internetcafé für privates Surfen – realisieren will.

12 Postunternehmen

12.1 Was lange währt, wird endlich gut: Die neue Datenschutzverordnung für Postdienste

Wie bereits in meinem 18. TB (Nr. 29.1) berichtet, hatte das BMWi im Jahr 2000 mit den Arbeiten an der neuen Postdienste-Datenschutzverordnung (PDSV) begonnen. Die Arbeiten wurden inzwischen beendet, sodass die PDSV endlich am 3. Juli 2002 in Kraft treten konnte. Diese Verordnung enthält die speziellen Regelungen des Datenschutzes bei Postdienstunternehmen. Geregelt werden die Erhebung und der Umgang mit den personenbezogenen Daten und damit fundamentale Rechte und Pflichten der am Postverkehr Beteiligten.

Erfreulicherweise hat das BMWi mit meiner Hilfe überwiegend datenschutzrechtlich gelungene Lösungen der von mir angesprochenen Probleme gefunden.

Insbesondere ist nunmehr die W eitergabe von neuen Anschriften aus dem Nachsendeverfahren an andere W ettbewerber klar geregelt. Die Daten dürfen nur zum Zweck der Postzustellung übermittelt werden, wenn der Betrof fene nicht widersprochen hat.

Die Regelungen der neuen PDSV sind den Erfordernissen des technischen Fortschritts angepasst. Die Einführung modernster Informationstechnik, wie z. B. elektronischer Quittierung von Auslieferung von Postsendungen (Handscanner) oder elektronischer Sendungsverfolgung im Internet (Tracking & Tracing) wird von ausgewogenen datenschutzrechtlichen Regelungen begleitet.

Leider wurden bei der Umsetzung nicht alle meine Forderungen berücksichtigt.

So findet sich beim Nachsendeverfahren keine konkrete Regelung zur Lösung des Informationsproblems im Bereich Pressepost, die aus Kostengr ünden nicht nachgesandt wird. Sollte der Nachsendeauftraggeber der W eitergabe seiner neuen Anschrift an Dritte wi dersprochen haben, erhält weder der Abonnent seine Zeitschrift noch der Verlag die neue Anschrift seines Kunden. Da darauf bei der Erteilung eines Nachsendeauftrages nicht besonders hingewiesen wird, der Kunde aber im Regelfall trotz V orauszahlung seine Zeitschrift nicht mehr erhält, ist Är ger vorprogrammiert. Die Deutsche Post AG versucht diesen Är ger zu vermeiden, indem Nachsendeauftraggeber, die der W eitergabe ihrer Anschrift an Dritte widersprochen haben, wenige T age nach Stellung des Nachsendeauftrage s automatisch eine Postkarte (s. Abbildungen 3 und 4) von der Deutschen Post AG erhalten, um auf die Konsequenzen hinzuweisen. Diese erneute Abfrage stößt aber auch auf Kritik, wie eine V ielzahl von Eingaben an mich belegt. Insbesondere die T atsache, dass man trotz der Streichung der Einwilligung auf dem Nachsendeauftrag nochmals aktiv tätig werden muss, um eine Weitergabe der neuen Anschrift an V erlage zu verhindern, stößt bei den Betrof fenen auf Unverständnis. Eine kundenfreundlichere Lösung wäre, die betreffenden Verlage würden eine Vereinbarung mit ihren Kunden treffen, die sie berechtigte, sich von der Deutschen Post AG die jeweils aktuelle Anschrift geben zu lassen.

Die von mir geforderte Regelung zum Umgang mit Postsendungen für Verstorbene wurde zwar diskutiert, aber letztlich nicht in die Verordnung aufgenommen. Somit ist weiterhin unklar, wie das jeweilige Postunternehmen mit solchen Postsendungen zu verfahren hat. Ob z. B. solche Sendungen nur an als Erbe ausgewiesene Personen zugestellt werden dürfen oder Hinterbliebene einen Nachsendeauftrag erteilen müssen oder die Sendungen an den Absender zurückgegeben werden müssen, bleibt nach wie vor ungeklärt. Solche Sendungen werden weiterhin durch die verschiedenen Postunternehmen nicht einheitlich behandelt. Die jetzige Vorgehensweise der Deutschen Post AG, bei der die Zusteller auf Anfrage des Absenders Informationen über das mutmaßliche Ableben von Postempfängern ohne genaue Prüfung an die Absender weiter geben, ist damit weiterhin zumindest rechtlich zweifelhaft.

Obwohl nicht alle meine Forderungen erfüllt wurden, stellt die neue PDSV insgesamt eine datenschutzrechtlich gelungene Regelung dar, die die unterschiedlichen Interessen der Postdienstleister einerseits und der Kunden andererseits angemessen berücksichtigt.

12.2 Nachsendung bei Umzug – wer erhält eigentlich meine neue Adresse?

Seit der Liberalisierung des Postmarktes und durch die Novellierung des Postgesetzes (PostG) im Jahr 1998 haben sich auch Änderungen in den Beziehungen zwischen den verschiedenen Postunternehmen er geben. So haben jetzt im lizensierten Postbereich Unternehmen gegenüber einem marktbeherrschenden Anbieter von Postdienstleistungen Anspruch auf Zugang zu den dort vorhandenen Informationen über Adressänderungen (§ 29 Abs. 2 PostG). Hierdurch soll die Konkurrenzfähigkeit der kleineren Unternehmen gestärkt werden. Dies hat erhebliche Auswirkungen auf das Nachsendeverfahren der Deutschen Post AG.

Mit dem Nachsendeverfahren bietet die Deutsche Post AG einen Service an, der es dem Bür ger ermöglicht, sich bei einem Umzug oder bei einer vorüber gehenden Abwesenheit vom W ohnort die an seine alte Anschrift adressierte Post nachsenden zu lassen. Bisher wurden die Adressdaten nur innerhalb des Unternehmens Deutsche Post AG im Nachsendeauftragszentrum in München verarbeitet. Nunmehr können auch Konkurrenzunternehmen diese Daten erhalten. Die Gefahr eines Missbrauchs von Daten aus Nachsendeaufträgen ist besonders hoch, da ein großes wirtschaftliches Interesse der werbetreibenden Industrie an möglichst umfassenden Adressdaten von neu zugezogenen Bürgern besteht. In § 7 der neuen Postdienste-Datenschutzverordnung wurden klare Regelungen über die Weitergabe von Adressdaten geschaf fen. Die Deutsche Post AG muss demnach Anschriftenänderungen an W ettbewerber weitergeben, sofern der Bür ger dem nicht explizit widersprochen hat. Dies hatte notwendigerweise Änderungen im Nachsendever fahren der Deutschen Post AG zur Folge. Sie musste zum einen in dem weitestgehend automatisierten V erfahren Schnittstellen schaf fen, die diese Datenweitergabe ermöglichen. Zum anderen war der bisher zur Erteilung eines Nachsendeauftrags verwendete Vordruck den neuen rechtl ichen Gegebenheiten anzupassen. So ist der Auftraggebe r über die erstmalig mögliche Adressweitergabe an Wettbewerber zu informieren, und ihm ist eine entsprechende Widerspruchsmöglichkeit einzuräumen. Die Deutsche Post AG hat daraufhin in enger Abstimmung mit mir ein neues Formular entwickelt, das diesem Umstand Rechnung trägt. Unter der URL http://www.deutschepost.de/nachsendeservice kann der Nachsendeauftrag auch online gestellt werden.

Im Übrigen hatte ich die Neugestaltung des Formulars bereits aus Gründen der unzureichenden Formulierung der Einwilligungserklärung zur Adressweiter gabe an Dritte – also nicht Wettbewerber – in meinem 17. TB (Nr. 29.2.1) gefordert. Die unzureichende Formulierung der Einwilligungsklausel, die zum einen den Auftraggeber über die V erarbeitung seiner Daten im Unklaren ließ und zum anderen nicht besonders hervorgehoben war, hatte zu einer V ielzahl von Eingaben geführt. Allerdings hatten die Fehler sehr häufig bei den Nachsendeauftraggebern selbst gelegen, weil diese z. B. die Einwilligungsklausel übersehen und deshalb nicht gestrichen hatten oder weil es V erständnis- und damit Aus-

Abbildung 3 und 4 (zu Nr. 12.1)

Nachsendeverfahren bei der Deutschen Post AG

füllprobleme bei dem Vordruck gab. Aufgrund des auch in diesen Punkten verbesserten neuen Formulars erwarte ich, dass sich künftig die Fehler beim Nachsendeauftragsverfahren deutlich reduzieren werden. Ich werde die Entwicklung dieses Bereiches jedoch verstärkt beobachten.

12.3 Paketabholung in einer Filiale der Post – was will die Post mit meinen Daten?

Seit Anfang Dezember 2001 speichert die Deutsche Post AG die Ausweisdaten des Empfängers einer Sendung, der diese nach einer Benachrichtigung in einer Postfiliale abholt. Die Deutsche Post AG nutzt dami t eine bereits seit 1996 bestehende Möglichkeit, die korrekte Auslieferung von Paketen nachzuweisen. Dieses Verfahren hat zu einer V ielzahl von Eingaben an mich geführt, da die Petenten nicht verstehen, warum ihre Daten gespeichert und sie darüber in der Postfiliale auch nicht hinreichend informiert werden.

Nach § 8 der Postdienste-Datenschutzverordnung können die Postdienstunternehmen vom Empfänger einer Sendung verlangen, sich durch Vorlage eines gültigen Personalausweises,

Reisepasses oder durch ein sonstiges geeignetes Ausweispapier auszuweisen, wenn dies erforderlich ist, um die ordnungsgemäße Ausführung der Dienstleistung sicherzustellen. Hierbei darf die Deutsche Post AG die Art und Nummer des Ausweises, die ausstellende Behörde sowie das Ausstellungsdatum zum späteren Beweis der ordnungsgemäßen Auslieferung der Sendung gegenüber dem Absender speichern. Das vor geschriebene besondere Beweissicherungsinteresse der Deutschen Post AG, aber auch aller anderen Postdienstunternehmen, liegt u. a. in haftungsrechtlichen Gründen. So würde z. B. bei dem Verlust einer Sendung die vorliegende Benachrichtigungskarte alleine nicht als Beweis vor Gericht angesehen, mit der möglichen Folge der Haftung der Deutschen Post AG. Durch die Speicherung der Daten des Ausweises soll die Ausl ieferung einer Postsendung genau und rechtlich einwandfrei nachvollzogen werden können. Darüber hinaus handelt es sich dabei auch um eine Vorbeugemaßnahme der Deutschen Post AG gegen Diebstahl innerhalb des eigenen Betriebes. Es soll verhindert werden, dass Mitarbeiter der Deutschen Post AG fingierte Daten angeben, um die ordnungsgemäße Auslieferung einer Sendung vorzutäuschen. Letztlich liegt dies auch im Interesse des Absenders und des Empfängers einer Postsendung.

Eine Verwendung der erhobenen Daten ist nur zulässig, um einen Beweis über die ordnungs gemäße Auslieferung einer Sendung zu erbringen. Die Ausweisnummer darf keinesfalls so verwendet werden, dass m it ihrer Hilfe ein Abruf personenbezogener Daten aus Dateien oder eine V erknüpfung von Dateien möglich ist. Außerdem sind die Daten spätestens sechs Monate nach Ablauf der gesetzlichen oder vertraglichen Verjährungsfristen, die sich aus dem BGB oder den AGB der Postdienstunterne hmen ergeben, zu löschen. In der Regel löscht die Deut sche Post AG die Daten nach spätestens dreieinhalb Jahren.

Zeitweise war es in einzelnen Filialen der Deutschen Post AG möglich, auch die Daten anderer Abholer von Sendungen einzusehen. Dies war möglich, weil diese Daten in den zu unterschreibenden Abhollisten of fen eingetragen waren. Ich habe dieses V erfahren gerügt und erreicht, dass heute diese Möglichkeit nicht mehr besteht. Aus datenschutzrechtlicher Sicht bestehen keine Bedenken gegen das von der Deutschen Post AG gewählte Verfahren.

12.4 Tausch einer Briefmarke – und dafür den Ausweis?

Am 30. Juni 2002 haben die Briefmarken der Deutschen Post AG mit reinen DM-W erten ihre Gültigkeit verloren. Somit dürfen Briefe und Pakete seit dem 1. Juli nur noch mit Briefmarken frankiert werden, die entweder neben dem DM-Wert noch eine Wertangabe in Euro enthalten oder nur mit reinen Euro-Werten versehen sind.

Die Deutsche Post AG hatte ohne eine rechtliche V erpflichtung den Besitzern von Briefmarken mit reinen DM-Werten den kostenlosen Umtausch der Marken angeboten. Hierzu mussten die Briefmarken bis zu einem W ert von 50 DM – selbst wenn es sich um nur eine einzige Marke mit einem Wert von 10 Pfennig handelte – auf einem eigens entwickelten Vordruck der Deutschen Post AG unter Angabe des Namens und der Anschrift des Umtauschenden aufgeklebt werden. Ferner wurde zu Legitimationszwecken die Vorlage eines geeigneten Ausweispapiers (z. B. eines Personalausweises oder eines Reisep asses) verlangt, um sicherzustellen, dass Name und Anschrift des Umtauschenden korrekt auf dem Vordruck angegeben waren. Da die umgetauschten Briefmarken stichprobenartig auf Fälschungen überprüft wurden, konnte durch die Angabe der persönlichen Daten auf den Vordrucken bei fehlerhaften Umtauschvorgängen der Umtauschende zweifelsfrei identifiziert werden. Eine Erfassung oder gar Speicherung der Ausweisdaten erfolgte nur bei einem konkreten Fälschungs- oder Manipulationsverdacht (wenn z. B. Kopien von Briefmarken auf den Umtauschbögen aufgeklebt wurden).

Alle Umtauschbögen wurden in so genannte Safebags eingelegt, die bis zur Abholung verschlossen aufbewahrt wurden. Danach wurden sie weiterhin gesichert in einer zentralen Stelle bis zum 31. Dezember 2002 für Prüfzwecke bereit gehalten.

Die Deutsche Post AG verpflichtete sich, die Daten auf den Umtauschbögen nicht zu speichern oder für andere Zwecke (z. B. Werbung) zu verwenden. Nach Ablauf der Umtauschaktion und stichprobenartigen Überprüfung der Unterlagen wurden diese vernichtet. Wenn es auch im Einzelfall unbefriedigend war, beim Umtausch einer kleinen Menge von Briefmarken persönliche Daten preisgeben zu müssen, war das Verfahren datenschutzrechtlich unbedenklich.

12.5 Postöffnung durch Zoll oder Post – dürfen die das überhaupt?

Immer wieder erreichen mich Anfragen besor gter Bürger, die sich darüber beklagen, dass an sie gerichtete Post geöf fnet würde.

Dabei handelt es sich zum einen um Auslandssendungen, die auf dem Luftweg nach Deutschland gelangen und zum anderen um so genannte entgeltbegünstigte Briefsendungen. Was den ersten Bereich anlangt, dürfen nach § 5 Zollverwaltungsgesetz diese Sendungen stichprobenartig geöf fnet werden, um deren Inhalt auf Einh altung der gesetzlichen Bestimmungen der Bundesrepublik Deutschland zu prüfen (z. B. in Bezug auf gefährliche Güter, das Arzneimittelgesetz oder auf mögliche Einfuhrverbote). Zur V ornahme der so genannten Beschau öffnet der Mitarbeiter des Postdienstunternehmens vor den Augen de s Zollbeamten – dieser darf aus haftungsrechtlichen Gründen die Sendungen nicht selbst öffnen – die Sendung in der Beschaustelle. Nach der Beschau werden die Sendungen vor den Augen des Zollbeamten wieder verschlossen. Der Zoll erteilt den Empfängern keinen Hinweis, aus welchen Gründen die Sendungen stichprobenartig geöffnet wurden. Aus datenschutzrechtlicher Sicht ist dieses Verfahren nicht zu beanstanden, weil weder Zoll noch Postdienstunternehmen rechtlich verpflichtet sind, auf die Sendungsöffnung hinzuweisen. Dies wäre allerdings aus Gründen der T ransparenz wünschenswert. Auf meine Empfehlung legt die Deutsche Post AG den Sendungen aus Drittländern – also außerhalb der Europäischen Union – inzwischen einen entsprechenden Hinweiszettel bei.

Der zweite Bereich, in dem Sendungen geöffnet werden, sind – wie schon angesprochen – die so genannten entgeltbegünstigten Briefsendungen von Großkunden der Deutschen Post AG. Hierbei handelt es sich um Massensendungen, wie z. B. Kontoauszüge einer Bank oder Beitragsrechnungen von Versicherungen, die durch die Deutsche Post AG zu ermäßigten Entgelten befördert werden. Nach § 39 Postgesetz

(PostG) dürfen diese Sendungen geöffnet werden, um das Vorliegen der tarifrechtlichen Voraussetzungen für den Versand zu günstigeren Konditionen zu prüfen. Die Einhaltung der Vertragsbedingungen durch den Absender einer Sendung wird von der Deutschen Post AG bei Einlieferung der Briefe stichprobenartig nach den Vorgaben einer innerbetrieblichen Anweisung geprüft: Kontrolliert werden die Einlieferungslisten, die Maschinenlesbarkeit der Sendung, die Inhalts-, Formats- und Gewichtsgleichheit sowie die Freimachung. Vom Mitarbeiter der Deutschen Post AG sind zur Prüfung mindestens drei Sendungen zu ziehen und mit den Vorgaben der AGB zu vergleichen. Die Petenten bezweifeln die Rechtmäßigkeit dieser Prüfungen und bemängeln, dass die Deutsche Post AG außer einem Aufdruck auf den geöffneten Sendungen „zu Prüfzwecken geöffnet" keinen Hinweis auf die rechtlichen Grundlagen für die Prüfung beilegt. Die Deutsche Post AG ist nach § 39 PostG zur Vornahme der Prüfungen jedoch berechtigt, sodass kein datenschutzrechtlicher Verstoß vorliegt. Auf meine Bitte hin prüft die Deutsche Post AG derzeit, ob in Zukunft den geprüften Sendungen ein Hinweis auf die Rechtmäßigkeit der Öffnung beigelegt wird.

12.6 Postzustellungsaufträge – darf die Post gegen meinen Willen zustellen?

Ein Petent hatte Anfang des Jahres 2002 die Annahme einer amtlich zuzustellenden Sendung verweigert. Der Zusteller der Deutschen Post AG hatte die Sendung daraufhin offen auf dem Grundstück abgelegt, auf dem er den Petenten angetroffen hatte. Die förmliche Zustellung von Schriftstücken richtete sich in diesem Fall nach den Vorschriften der Zivilprozessordnung (ZPO) in der bis zum 30. Juni 2002 gültigen Fassung. Amtliche Zustellungen erfolgten hiernach auch durch die Deutsche Post AG. Die Zustellung konnte an jedem Ort erfolgen, an dem die Person, der zugestellt werden sollte, angetroffen wurde. Im Fall einer grundlos verweigerten Annahme des Schriftstückes war nach § 186 ZPO das zu übergebende Schriftstück am Ort der Zustellung zurückzulassen. Dies konnte somit auch durch die offene Auslegung einer Sendung auf dem Grundstück des vorgesehenen Empfängers erfolgen. Der Zusteller der Deutschen Post AG hatte also im Fall des Petenten gesetzmäßig gehandelt, obwohl aus datenschutzrechtlicher Sicht zumindest die Einlegung der Sendung in einen Hausbriefkasten wünschenswert gewesen wäre.

Erfreulicherweise ist durch die Änderung der ZPO ab 1. Juli 2002 eine deutliche Verbesserung des Datenschutzes erreicht worden. Nach § 179 ZPO ist im Gegensatz zur alten Regelung die Sendung in der Wohnung bzw. den Geschäftsräumen zurückzulassen. Falls dies nicht möglich ist, muss die Sendung zurückgesandt werden. Die Sendung gilt mit der Annahmeverweigerung als zugestellt. Die offene Auslegung einer Sendung auf einem Grundstück ist künftig ein datenschutzrechtlicher Verstoß.

12.7 Was sich bei der Deutschen Post AG sonst noch so tut

In den letzten beiden Jahren stellte die Deutsche Post AG einige weitere interessante Produkte vor.

Eines dieser Produkte ist die so genannte PACKSTATION. Es handelt sich hierbei um ein insbesondere für Berufstätige nützliches Verfahren zur Paketzustellung, bei dem die Sendungen nicht mehr zu Hause abgeliefert, sondern über einen an einem gut erreichbaren Platz aufgestellten Paketausgabeautomaten ausgegeben werden. Der Empfänger kann rund um die Uhr bestimmen, wann er die für ihn bestimmte Sendung abholt. Um diese Möglichkeit nutzen zu können, muss er sich bei dem System PACKSTATION anmelden. Hierbei werden sein Name, Vorname, die vollständige Hausanschrift sowie die Mobilrufnummer oder die E-Mail-Adresse registriert. Für evtl. notwendige Rückfragen wird zusätzlich eine Sicherheitsfrage vereinbart. Bei einer Anmeldung über das Internet werden als freiwillige Angaben weiter das Geburtsdatum, die Festnetzrufnummer und die Faxnummer erbeten. Zur Bestätigung erhält der Empfänger zwei Briefe von der Deutschen Post AG. In dem ersten Brief befinden sich seine Magnetstreifenkarte, die so genannte Goldcard mit der für ihn eingerichteten Postnummer, der PACKSTATION-Aufkleber für den heimischen Briefkasten und ein Plan mit den Standorten der Automaten. Der zweite Brief enthält die zur eindeutigen Identifizierung zusammen mit der Postnummer notwendige PACKSTATION-PostPIN. Der Empfänger kann jetzt seine Pakete an die PACKSTATION liefern lassen; er wird hierüber per SMS oder E-Mail informiert. Am Automaten gibt er die Goldcard und seine PIN ein und erhält sein Paket. Eine Weitergabe der personenbezogenen Daten an Dritte erfolgt nicht. Die Deutsche Post AG nutzt die Daten lediglich zur Markt- und Meinungsforschung, wenn der Empfänger bei der Registrierung hiergegen nicht widersprochen hat. Die bei der Auslieferung eines Pakets anfallenden Daten werden von der Deutschen Post AG zu Beweiszwecken maximal für den Zeitraum der gesetzlichen Verjährungsfrist von drei Jahren gespeichert. Die Teilnahme am Verfahren kann jederzeit widerrufen werden. Aus datenschutzrechtlicher Sicht gibt es an dem Verfahren nichts auszusetzen.

Ein weiteres neues Produkt der Deutschen Post AG ist die so genannte POSTCARD für die bargeldlose Zahlung der Produkte und Dienstleistungen der Deutschen Post AG (z. B. Kauf von Briefmarken, Infopost, Postwurfsendungen usw.). Es handelt sich quasi um eine Kreditkarte zur Bezahlung von Leistungen der Deutschen Post AG. Zur Teilnahme erteilt der Kunde der Deutschen Post AG einen Auftrag, in dem er seine persönlichen Daten (Name, Anschrift, Kontonummer und Bankverbindung für den Lastschrifteinzug) und das Kartenlimit angibt. Die AGB sehen nur zum Zweck der Bonitätsprüfung eine Weitergabe der erhobenen Daten an die Creditreform Bonn Himstedt KG vor. Auch dieses Verfahren hat die Deutsche Post AG mit mir abgestimmt.

Ebenfalls interessant ist das so genannte PostIdent-Verfahren. Es handelt sich hierbei um eine Identitätsprüfung nach den Vorgaben des Geldwäschegesetzes, die die Deutsche Post AG im Rahmen einer Auftragsdatenverarbeitung nach § 11 BDSG vornimmt. Kunden der Deutschen Post AG sind z. B. Direktbanken, die auf diesem Weg zweifelsfrei die Identität von Neukunden klären lassen können. Das nach meiner Kenntnis am häufigsten verwendete Verfahren ist PostIdent 3 zur Identifikation in einer Filiale der Deutschen Post AG. Aufgrund eines Kontoeröffnungsantrages sendet die Bank dem Neukunden Unterlagen zur Identitätsfeststellung zu. Bei diesen Unterlagen befindet sich ein Coupon, den der Kunde zwecks Identifizierung in einer Filiale der

Deutschen Post AG vorlegen muss. Auf dem Coupon sind die Anschrift und die Postkundennummer der Bank und die Referenznummer des Neukunden angegeben. Unter Vorlage des Personalausweises oder Reisepasses werden die Daten des Kunden in der Postfiliale geprüft. Die Referenznummer, die Angaben zur Person sowie die weiteren Ausweisdaten werden nun direkt per EDV in ein PostIdent-Formular übertragen. Der Kunde bestätigt die Angaben anschließend durch seine eigenhändige Unterschrift, die mit der des Ausweises verglichen wird. Die erfolgte Identifizierung bestätigt der Filialmitarbeiter durch seine Unterschrift. Das ausgefüllte und unterschriebene Formular wird an die Bank gesandt. Die erfassten Daten werden nicht gespeichert. Daneben gibt es noch die Verfahren PostIdent 1 und 2, bei denen die Identifikation an der Wohnanschrift des Neukunden direkt durch den Zusteller erfolgt. Diese Verfahren bieten z. B. über die Identifikation hinaus noch die Möglichkeit, sich die Kenntnisnahme der AGB der Bank durch den Neukunden bestätigen zu lassen. Auch bei diesen Verfahren bietet die Deutsche Post AG einen lückenlosen Nachweis über den Lauf des Identifikationsverfahrens.

13 Bundeskriminalamt

13.1 Rasterfahndung – Nach den Terroranschlägen des 11. September 2001 wieder aktuell

Die Terroranschläge in den USA vom 11. September 2001 und die Erkenntnis, dass einige der daran beteiligten Terroristen sich zeitweise auch in Deutschland unerkannt aufgehalten hatten, führte nicht nur zu gesetzgeberischen Initiativen (s. Nr. 2). Wegen der fortdauernden Bedrohungslage sahen es Bund und Länder zudem als erforderlich an, nach weiteren potenziellen Anhängern des islamischen Terrorismus, so genannten „Schläfern", in Deutschland zu fahnden. Als hierfür allein geeignete Maßnahme wurde die Rasterfahndung zu Zwecken der Gefahrenabwehr in Betracht gezogen. Damit rückte eine Fahndungsmethode wieder in den Blickpunkt des polizeilichen Interesses, die im Rahmen der polizeilichen Arbeit seit der Fahndung nach den terroristischen Gewalttätern der „Rote Armee Fraktion" Ende der 70er-/Anfang der 80er-Jahre kaum noch eine Rolle zu spielen schien.

Die polizeiliche Rasterfahndung ist ein von den Polizeibehörden durchgeführter automatisierter Datenabgleich bestimmter, auf den Täter bzw. auf den potenziellen Täter vermutlich zutreffender Prüfungsmerkmale mit Datenbeständen nicht polizeilicher Stellen. Ziel ist es zum einen, Personen auszuschließen, auf die die Merkmale nicht passen, bzw. die Zahl der verdächtigen Personen durch das Herausfiltern derjenigen mit tätertypischen Merkmalen zu beschränken. Die Rasterfahndung dient außerdem dem Zweck, weitere für die Ermittlungen bedeutsame Prüfungsmerkmale festzustellen. Die rechtsstaatliche Problematik dieser Methode liegt vor allem in der Einbeziehung einer Vielzahl unverdächtiger Personen, die sich durch bestimmte Merkmale oder Verhaltensweisen, die nach der polizeilichen Fahndungshypothese auch beim Täter vorliegen könnten, auszeichnen. Erst die Rasterfahndung beseitigt für die Mehrzahl der Betroffenen die entstandenen Verdachtsmomente.

Als Folge der Terroranschläge in den USA beschlossen die Gremien der Ständigen Konferenz der Innenminister und -senatoren der Länder (IMK), Rasterfahndungsmaßnahmen auf der Grundlage der jeweiligen landesgesetzlichen Regelung in den Ländern durchzuführen und beauftragten das BKA in dessen Funktion als Zentralstelle der Polizeien des Bundes und der Länder damit, hierbei unterstützend tätig zu werden. In der Folgezeit haben die Länder personenbezogene Daten bei Universitäten, Einwohnermeldeämtern und dem Ausländerzentralregister erhoben und die Datenbestände anschließend anhand bestimmter, zuvor festgelegter Rasterkriterien gegeneinander „gerastert". Der daraus resultierende Datenbestand wurde dem BKA übermittelt und von diesem in eine zuvor errichtete Verbunddatei eingestellt. Um den von den Ländern vorgerasterten Personenkreis durch weitere Kriterien in Anlehnung an die Täterprofile der in Deutschland zeitweise wohnhaften Attentäter vom 11. September 2001 einzuschränken, sollte der in der Verbunddatei eingestellte Grunddatenbestand mit anderen Datenbeständen abgeglichen und dabei eine inhaltliche Informationsanreicherung bzw. -verdichtung der Länderdatensätze erfolgen. Diese Aufgabe sollte gemäß dem o. a. Beschluss der Gremien der IMK das BKA in seiner Funktion als Zentralstelle mit dort vorhandenen Datenverarbeitungskapazitäten übernehmen.

Das Erheben der genannten Abgleichsdatenbestände sollte arbeitsteilig durchgeführt werden: Sofern entsprechende Informationen z. B. von Bundesbehörden oder von Bundesverbänden der Industrie zu erlangen waren, sollte das BKA die entsprechenden Daten erheben. Anderenfalls sollte die Erhebung durch die Länder im Wege der Rasterfahndung zu präventiv-polizeilichen Zwecken auf der Grundlage der einschlägigen Regelungen der Landespolizeigesetze erfolgen.

Das BKA hat in der Folgezeit auf der Grundlage des § 7 Abs. 2 Satz 2 BKA-Gesetz nach seinen Angaben ca. 4 000 Institutionen und Firmen um Übersendung von Personaldaten gebeten. Auf diese Ersuchen hin haben 212 Institutionen dem BKA entsprechende Daten zur Verfügung gestellt. Die übrigen, für den Datenabgleich für erforderlich erachteten Abgleichsdateien sind von den Ländern in der oben beschriebenen Weise erhoben worden. Aufgabe des BKA war es schließlich, die von ihm erhobenen bzw. ihm von den Ländern zur Verfügung gestellten Abgleichsdateien elektronisch für den Datenabgleich aufzubereiten und den Abgleich mit dem in der Verbunddatei gespeicherten Datenbestand durchzuführen. Über die dabei festgestellten Namensidentitäten wird das jeweilige Land unterrichtet und ihm der betreffende Abgleichsdatensatz zur Verfügung gestellt. Dem Land obliegt es, im Rahmen der polizeilichen Sachbearbeitung festzustellen, ob die „Namensidentität" auch zu einer „Personenidentität" mit der betreffenden Person in der Verbunddatei führt. In diesem Fall wird der betreffende Datensatz in der Verbunddatei von dem Land gekennzeichnet und vermerkt, woraus sich die Personenidentität ergibt. Bei Redaktionsschluss zu diesem Tätigkeitsbericht war der beschriebene Datenabgleich im BKA allerdings noch nicht abgeschlossen.

Die öffentliche Diskussion der Rasterfahndungsmaßnahmen in einigen Ländern, aber auch zahlreiche Nachfragen betroffener nicht öffentlicher Stellen bei mir zur Rechtmäßigkeit des Ersuchens des BKA um Übermittlung von Personaldaten, gaben mir Veranlassung, die vom BKA geleistete Unterstützungstätigkeit bezüglich der von den Ländern

durchgeführten Rasterfahndungsmaßnahmen datenschutzrechtlich zu kontrollieren.

Dabei habe ich festgestellt, dass sich das BKA bei der Durchführung der o. g. Unterstützungsmaßnahmen im Rahmen der ihm durch das BKA-Gesetz eingeräumten Befugnisse zur Erfüllung seiner Zentralstellenaufgabe gemäß § 2 i. V. m. § 7 BKA-Gesetz gehalten hat. Das gilt sowohl für das Führen der o. g. Verbunddatei, in welcher der von den Ländern vorgerasterte Grunddatenbestand gespeichert wird, als auch für die Durchführung des Datenabgleichs auf der Grundlage des § 28 BKA-Gesetz. Auch das Ersuchen des BKA gegenüber diversen nicht öffentlichen Stellen um Übermittlung von Personaldaten war formell rechtmäßig. Nach der zu diesem Zeitpunkt geltenden Fassung des § 7 Abs. 2 Satz 2 BKA-Gesetz konnte das BKA Daten erheben, wenn die Polizeien des Bundes und der Länder nicht über die erforderlichen Daten verfügt haben. Da die vom BKA erhobenen Abgleichsdaten zum damaligen Zeitpunkt weder beim Bund noch bei den Ländern existierten und die Landeskriminalämter diese absprachegemäß nicht erheben wollten, lagen die Voraussetzungen der subsidiären Erhebungsbefugnis des BKA nach dem Wortlaut des Gesetzes vor. Personenbezogene Daten können auf der Grundlage des § 7 Abs. 2 Satz 2 BKA-Gesetz nicht zwangsweise erhoben werden. Ich habe das BKA deshalb darauf hingewiesen, im Rahmen seiner Ersuchen an diverse nicht öffentliche Stellen die Freiwilligkeit der Datenübermittlung ausdrücklich hervorzuheben.

Es ist gleichwohl fraglich, ob es der Intention des Gesetzgebers entsprach, dem BKA mit § 7 Abs. 2 Satz 2 BKA-Gesetz eine Befugnis zur massenhaften Erhebung personenbezogener Daten von Unverdächtigen nach dem Muster von Rasterfahndungen in den Ländern einzuräumen. Während der jeweilige Landesgesetzgeber Voraussetzungen und Schranken für Rasterfahndungsmaßnahmen detailliert und normenklar geregelt hat – in einigen Ländern unterliegt deren Anordnung dem Richtervorbehalt und der jeweilige Landesdatenschutzbeauftragte ist von der Durchführung der Maßnahme zu unterrichten – besteht das einzige Korrektiv einer Datenerhebung durch das BKA gemäß § 7 Abs. 2 Satz 2 BKA-Gesetz in der Erforderlichkeit für die Erfüllung seiner jeweiligen Zentralstellenaufgabe. Zwar liegt der wesentliche qualitative Unterschied zu den Rasterfahndungen in den Ländern zum Zwecke der Gefahrenabwehr darin, dass personenbezogene Daten auf der Grundlage des § 7 Abs. 2 Satz 2 BKA-Gesetz vom BKA nicht zwangsweise erhoben werden können. In den Fällen, in denen nicht öffentliche Stellen auf das Ersuchen des BKA hin personenbezogene Daten über ihr Personal übermittelt haben, konnte auf die Anordnung einer Rasterfahndung auf landesgesetzlicher Rechtsgrundlage und auf die erforderliche Prüfung, inwieweit deren Voraussetzungen vorliegen, aber verzichtet werden. Im Hinblick darauf, dass infolge der Terroranschläge in den USA nach Angaben des BKA unverzüglich konkrete Maßnahmen zur Identifizierung ggf. weiterhin in Deutschland aufhältiger potenzieller islamischer Terroristen getroffen werden mussten, habe ich meine Bedenken gegen die vom BKA durchgeführten Datenerhebungsmaßnahmen zurückgestellt. Der Versuch des BKA, auf der Grundlage des § 7 Abs. 2 Satz 2 BKA-Gesetz über die Bundesverbände bestimmter sicherheitsempfindlicher Wirtschaftbereiche rasch an die für die Durchführung des Abgleichs erforderlichen Datenbestände zu kommen, schien eine geeignete Maßnahme zu sein, zumal sie vom Wortlaut des BKA-Gesetzes gedeckt war. Der Umstand, dass nur wenige Unternehmen dem BKA Personaldaten übermittelt haben, der Großteil der in den Datenabgleich einzubeziehenden Datenbestände damit von den Landeskriminalämtern im Wege der Rasterfahndung nach dem jeweiligen Landespolizeirecht erhoben werden musste, stellt die Geeignetheit dieser zwischen Bund und Land abgestimmten Vorgehensweise im Ergebnis jedoch infrage. Vor diesem Hintergrund sollte künftig auf eine massenhafte Erhebung personenbezogener Daten durch das BKA, deren rechtsstaatliche Problematik – vergleichbar der Rasterfahndung – in der Einbeziehung einer Vielzahl von Unverdächtigen liegt, verzichtet werden. Für die Durchführung derartiger Maßnahmen stellen die hierfür jeweils geschaffenen landesgesetzlichen Regelungen zur Rasterfahndung eine rechtsstaatlich solidere Grundlage dar als die derzeit geltenden Normen des BKA-Gesetzes.

Bedauerlich ist, dass die Rasterfahndungen nach mehr als einem Jahr seit dem Beginn dieser Maßnahme noch nicht abgeschlossen werden konnten, mit der Folge, dass weder die Grunddatenbestände noch die erhobenen Abgleichsdatensätze bisher gelöscht werden können. Ich halte es im Hinblick auf die rechtsstaatliche Problematik der Rasterfahndung für geboten, künftig derartige Maßnahmen zügiger durchzuführen.

13.2 Auswertedateien – neue Wege der Datenverarbeitung im BKA

Das BKA hat im Berichtszeitraum mit der Errichtung so genannter Auswertedateien neue Wege in der polizeilichen Datenverarbeitung beschritten. Auswertedateien stellen eine Art „Vordatei“ dar, in der sämtliche Informationen zu bestimmten, vom BKA durchgeführten Projekten vorläufig gespeichert und anschließend auf ihre Relevanz für polizei- oder ermittlungstaktisches Vorgehen bewertet werden. Der neue Dateityp ist insbesondere dadurch gekennzeichnet, dass der Personenkreis, über den Daten gespeichert werden, allein durch den jeweiligen Zweck der Datei begrenzt wird, eine Qualifizierung der personenbezogenen Merkmale nach den Kriterien des § 8 Abs. 1 bis 5 BKA-Gesetz (u. a. Beschuldigte, Verdächtige, Zeugen) hingegen nicht erfolgt. Die Zulässigkeit der Datenverarbeitung wird dabei allein auf die Rechtsgrundlage des § 7 Abs. 1 BKA-Gesetz gestützt, wonach das BKA personenbezogene Daten speichern, verändern und nutzen kann, soweit dies zur Erfüllung seiner jeweiligen Aufgabe als Zentralstelle erforderlich ist.

Die vom BKA betriebenen Auswertedateien können gemäß ihrer Zweckbestimmung grob in drei Gruppen unterteilt werden: Auswertedateien zu eigenen Ermittlungsverfahren des BKA, projektbezogene Auswertedateien sowie Auswertedateien, mit deren Hilfe das BKA in seiner Funktion als Zentralstelle bestimmte gesellschaftliche bzw. gesellschaftspolitische Entwicklungen unter polizeifachlichen Gesichtspunkten untersucht. Bei den Auswertedateien zu eigenen Ermittlungsverfahren des BKA handelt es sich im Ergebnis nicht um eine Datei dieses neuen Typs. Vielmehr sind sie, ebenso wie die Spudok-Dateien, eine Erscheinungsform des Dateityps „Amtsdatei des BKA“. Ich bin mit dem BKA deshalb darin einig, dass sich die Regelungen der jeweiligen Errichtungsanordnung an den Bestimmungen der §§ 483 ff. Strafprozessordnung auszurichten haben, da diese Art von „Auswertedatei“ der Unterstützung des BKA bei dessen

Aufgabenwahrnehmung auf dem Gebiet der Strafverfolgung gem. § 4 BKA-Gesetz dient. Auch gegen die projektbezogenen Auswertedateien (siehe hierzu auch Nr. 13.2.1) bestehen keine grundlegenden datenschutzrechtlichen Bedenken.

Datenschutzrechtlich problematischer ist die V erarbeitung personenbezogener Daten in den übrigen Auswertedateien, die das BKA zur Erfüllung seiner Zentralstellenaufgabe führt (siehe hierzu auch Nr. 13.2.2). Der Umstand, dass der Kreis der von der Speicherung in der Auswertedatei Betroffenen allein durch den ohnehin stets zu beachtenden Grundsatz der Erforderlichkeit für die Erfüllung der Zentralstellenaufgabe des BKA gem. § 7 Abs. 1 BKA-Gesetz sowie durch den Zweck der jeweili gen Auswertedatei bestimmt wird, wiegt hier besonders sc hwer. Denn anders als bei den Auswertedateien, die auf der Grundlage der Strafprozessordnung geführt werden, handelt es sich hier um eine reine Vorsorgedatei. Zudem kann ich nicht erkennen, dass die in den jeweiligen Dateien gesp eicherten personenbezogenen Daten – wie bei den projektbezogenen Auswertedateien – innerhalb einer kurzen Frist auf polizeiliche Relevanz hin aktiv überprüft werden. Um den Kreis der von der Speicherung in einer Auswertedatei betrof fenen Personen, gegen die offensichtlich weder Straf fälligkeitsprognosen gestellt werden können noch ein Tatverdacht zu begründen ist, sachgerecht einzugrenzen, halte ich es für erforderlich, den Zweck der jeweiligen Auswertedatei in der Errichtungsanordnung präzise zu bestimmen und die Verwendung der erhobenen Daten hierauf zu beschränken. Anderenfalls wären entsprechende personenbezogene Speicherungen wegen Verstoßes gegen das Verbot der Datensammlung auf Vorrat unzulässig. Ich habe meine Bedenken gegen die Zulässigkeit dieser Auswertedateien zu rückgestellt. Zum einen sind die Anhörungsverfahren gem. § 34 Abs. 1 Satz 2 BKA-Gesetz zu den betref fenden Errichtungsanordnungen noch nicht abgeschlossen. Dem Ge sichtspunkt des Persönlichkeitsschutzes soll nach den vorliegenden Entwürfen zudem dadurch Rechnung getragen werden, dass Übermittlungen von personenbezogenen Daten aus den Auswertedateien an andere Stellen grundsätzlich solange unzulässig sind, wie eine Kategorisierung der gespeicherten Personen nach den Regelungen des § 8 Absätze 1 bis 5 BKA-Gesetz nicht möglich ist. Darüber hinaus soll der Zugriff auf die Dateien auf einen begrenzten Personenkreis im BKA beschränkt und die Aussonderungsprüffristen für die Datensätze auf zwei bzw . drei Jahre bemessen werden.

Ich stehe dem Bemühen der Po lizei, neue Datenverarbeitungsformen zu nutzen, um Straftaten wirksamer verfolgen und verhüten zu können, aufgeschlossen gegenüber , insbesondere wenn sich die bisherigen Datenverarbeitungsinstrumente als nicht ausreichend erwiesen haben sollten. Soweit dabei personenbezogene Daten verarbeitet und genutzt werden, sind jedoch die einschlägigen gesetzlichen Regelungen sowie die Anforderungen, di e das Bundesverfassungsgericht an die zulässige Einschränkung des Rechts auf informationelle Selbstbestimmung gestellt hat, zu beachten. Inwieweit dem Rechnung getragen wird und worin unter dem Gesichtspunkt der Erforderlichkeit der zusätzliche Erkenntnisgewinn gegenüber den auf der Grundlage des § 8 Absätze 1 bis 5 BKA-Gesetz zu führenden Dateien zur V orsorge für die künftige Strafverfolgung liegt, kann erst eine systematische datenschutzrechtliche Kontrolle der Auswertedateien ergeben.

13.2.1 Auswertedatei „Infoboard Schleusung“ – intensive Zusammenarbeit zwischen Polizei und Nachrichtendiensten

Ein Beispiel für die vom BKA betriebenen projektbezogenen Auswertedateien, die der Unterstützung der projektbezogenen Zusammenarbeit des BKA mit Nachrichtendiensten, polizeilichen und anderen öf fentlichen Stellen dienen, ist die Datei „Infoboard Schleusung“. Das damit unterstützte Projekt ist der Infoboard „Schleuserkriminalität über die tschechische Republik“, an dem sich neben dem BKA das Bundesamt für Verfassungsschutz, der Bundesnachrichtendienst, die Grenzschutzdirektion, das Zollkriminalamt, die Landeskriminalämter Bayern und Sachsen, das Landesamt für V erfassungsschutz Bayern sowie das Bundesverwaltungsamt und das Bundesamt für die Anerkennung ausländischer Flüchtlinge beteiligen. Die von den Projektteilnehmern angelieferten Date n werden in der Auswertedatei „Infoboard Schleusung“ gespeichert und nach bestimmten Fallkomplexen ausgewertet. Ziel ist es, neue Erkenntnisse für polizei- und ermittlungstaktisches Vorgehen zu gewinnen und unbedeutende Informationen auszuscheiden. Der Vorteil der bisher eher formlosen Zusammenarbeit zwischen den Projektteilnehmern besteht nach Aussage des BKA darin, dass innerhalb des Infoboards die Kenntnisse der am Projekt beteiligten Stellen vor Ort im BKA im Rahmen regelmäßig tagender Grem ien zusammengeführt werden. Das Projekt startete im September 2001 und war zunächst auf sechs Monate befris tet mit der Möglichkeit einer begrenzten Verlängerung.

Ich habe gegen das Führen derartiger Auswertedateien keine grundlegenden datenschutzrechtlichen Bedenken. Voraussetzung ist jedoch, dass es bei der zeitlich befristeten und projektgebundenen V erarbeitung der personenbezogenen Daten bleibt. Zudem muss gewährleistet sein, dass die am Projekt beteiligten Stelle n bei der Anlieferung ihrer Informationen an das BKA den Rahmen der ihnen durch die einschlägigen Gesetze einge räumten Übermittlungsbefugnisse nicht verlassen. Insbesondere ist das für die informationelle Zusammenarbeit zwischen Polizei und Nachrichtendiensten maßgebliche T rennungsgebot strikt einzuhalten. Ich stimme mit dem BKA sch ließlich darin überein, dass eine Überführung der im Proj ekt zusammengetragenen Erkenntnisse in die Dateien des polizeilichen Informationssystems des Bundes und der Lände r erst nach Abschluss der Auswertung und Feststellung der polizeilichen Relevanz zulässig ist; zumal die verstä rkte Zusammenarbeit des BKA insbesondere mit anderen Sicherheitsbehörden zwangsläufig dazu führt, dass das BKA in größerem Maße als bisher nachrichtendienstliche Informationen erhält. Inwieweit die Ziele, die mit dem Infoboard verfolgt werden sollten, erreicht wurden, ist noch of fen. Zwischenzeitlich sind zwei weitere Projekte dieser Art gestartet worden. Das BKA beabsichtigt, einen Erfahrungsbericht nach Abschluss des Projekts zu erstellen, der mir bei Redaktionsschluss zu diesem Tätigkeitsbericht jedoch noch nicht vorlag.

13.2.2 Auswertedatei „Global“ – wirksames Instrument zur Verhinderung gewalttätiger Demonstrationen oder Vorratsdatensammlung über Globalisierungsgegner?

Die zahlenmäßig größte Gruppe von Auswertedateien bilden die Dateien, mit deren Hi lfe das BKA in seiner Funk-

tion als Zentralstelle der Polizeien des Bundes und der Länder Informationen über bestimmte gesellschaftliche bzw. gesellschaftspolitische Erscheinungen bzw. Entwicklungen (z. B. Globalisierungsgegner, islamische Fundamentalisten, rechte Kameradschaften) unter polizeifachlichen Gesichtspunkten auswertet. Dadurch sollen Erkenntnisse insbesondere für Maßnahmen der Verbrechensverhütung gewonnen werden. Zu diesem Zweck werden in den jeweiligen Auswertedateien Personendaten anhand von Berichten, Meldungen und sonstigen Informationen, z. B. auch polizeiliche Erkenntnisanfragen, unabhängig davon gespeichert, ob zum Zeitpunkt der Speicherung strafrechtlich oder polizeirechtlich relevante Erkenntnisse zu der betroffenen Person vorliegen.

Zu dieser Kategorie von Auswertedateien gehört auch die Datei „Global". Sie ist vor dem Hintergrund der zum Teil gewalttätigen Auseinandersetzungen bei Demonstrationen von Globalisierungsgegnern anlässlich des EU-Gipfels in Göteborg und des Weltwirtschaftsgipfels der G8-Staaten in Genua im Sommer 2001 eingerichtet worden. Die Datei dient dem Erkennen von Zusammenhängen in Bezug auf Ereignisse, Institutionen bzw. Gruppierungen sowie Personen im Zusammenhang mit gewalttätigen Aktionen und anderen Straftaten militanter Globalisierungsgegner. Gespeichert werden Meldungen sowie Erkenntnisse, die im unmittelbaren oder mittelbaren Zusammenhang mit einschlägigen Straftaten stehen. Datenschutzrechtlich problematisch ist hier vor allem der von der Speicherung betroffene Personenkreis, der allein durch die genannte Zweckbeschreibung bestimmt wird. Die in der Errichtungsanordnung zu der Datei gewählte Formulierung halte ich vor dem Hintergrund des § 34 Abs. 1 Nr. 3 BKA-Gesetz, wonach in einer Errichtungsanordnung der Personenkreis, über den Daten gespeichert werden sollen, konkret festzulegen ist, für zu undifferenziert und zu unbestimmt. Ziel dieser Regelung ist es, den Betroffenen das Auffinden der für sie relevanten Daten zu ermöglichen. Im Rahmen des Anhörungsverfahrens zu der Errichtungsanordnung habe ich deshalb darauf gedrungen, den Personenkreis, über den Daten gespeichert werden sollen, möglichst präzise zu beschreiben. Dabei muss gewährleistet sein, dass nur polizeirelevante Informationen zur Speicherung in der Datei führen; wohingegen Informationen über sonstiges Verhalten, z. B. über die bloße Teilnahme an einer derartigen Demonstration, hierfür nicht ausreichen. Aus meiner Sicht ist es zudem geboten, dass das BKA die ihm jeweils übermittelte personenbezogene Information zügig auf ihre polizeiliche Relevanz hin überprüft und nicht die Aussonderungsprüffrist von drei Jahren abwartet, um feststellen zu können, ob sich die Information in diesem Zeitraum entsprechend verdichtet hat. Das Anhörungsverfahren zu der Errichtungsanordnung war bei Redaktionsschluss zu diesem Tätigkeitsbericht noch nicht abgeschlossen.

13.3 DNA-Analyse-Datei

Ein Schwerpunkt meiner Kontrolltätigkeit beim Bundeskriminalamt betraf die datenschutzrechtliche Kontrolle der dort geführten DNA-Analyse-Datei, bezogen auf die DNA-Identifizierungsmuster, die von Bundesstellen erhoben bzw. in die Datei eingestellt wurden. Von den über 100 000 Datensätzen, die zum Zeitpunkt der Kontrolle im Juni 2001 in der DNA-Analyse-Datei gespeichert waren, stammten lediglich 173 DNA-Identifizierungsmuster von Polizeistellen des Bundes, die alle durch das BKA eingestellt worden waren. Der überwiegende Teil der Datensätze ist – wie auch bei den anderen Dateien des polizeilichen Informationssystems des Bundes und der Länder – von den Polizeidienststellen der Länder erhoben und in der DNA-Analyse-Datei gespeichert worden. Nach meinen Feststellungen hat das BKA bei der Erhebung von DNA-Identifizierungsmustern und deren Speicherung in der DNA-Analyse-Datei die in den §§ 81a ff. Strafprozessordnung (StPO) normierten Voraussetzungen in der Regel beachtet. Abweichungen ergaben sich vor allem in zwei Punkten:

Unter den vom BKA in der Datei gespeicherten Datensätzen befand sich auch eine größere Anzahl von DNA-Identifizierungsmustern, die von Dienststellen des Bundesgrenzschutzes und der Zollfahndung erhoben und vom BKA in Amtshilfe in die DNA-Analyse-Datei eingestellt worden waren.

Ich habe diese Praxis wegen Verstoßes gegen die einschlägigen Regelungen des BKA-Gesetzes gem. § 25 Abs. 1 BDSG beanstandet. Der Kreis der Teilnehmer am polizeilichen Informationssystem mit dem Recht, Daten einzugeben und abzurufen, wird durch § 11 Abs. 2 BKA-Gesetz in Verbindung mit der für jede automatisierte Datei des polizeilichen Informationssystems zu erstellenden Errichtungsanordnung festgelegt. Bei der dabei unter dem Gesichtspunkt der Erforderlichkeit zu treffenden Entscheidung ist danach zu differenzieren, welche Behörde vor dem Hintergrund ihres Aufgabenbereichs und der Art der in der jeweiligen Datei gespeicherten Informationen Zugriff auf diesen Bestand erhalten soll. Die entsprechende Regelung in der Errichtungsanordnung ergeht gem. § 34 BKA-Gesetz mit Zustimmung der Länder und nach meiner vorherigen Anhörung. Als Ergebnis dieses Verfahrens, über das ich mehrfach berichtet habe (zuletzt 18. TB Nr. 11.6), ist in der Errichtungsanordnung zur DNA-Analyse-Datei festgelegt worden, dass nur das BKA und die Landeskriminalämter im Rahmen ihrer jeweiligen Zuständigkeit gewonnene Daten in die Datei eingeben dürfen. Die Teilnahme von Dienststellen des Bundesgrenzschutzes und der Zollfahndung an dieser Verbundanwendung ist bei Festlegung des Teilnehmerkreises – offenbar wegen des spezifischen Zuständigkeitsbereichs dieser Bundespolizeien – als nicht erforderlich im Sinne von § 11 Abs. 2 Satz 1 BKA-Gesetz beurteilt worden. Jedenfalls habe ich während des Anhörungsverfahrens zu der Errichtungsanordnung, das sich über mehr als ein Jahr hingezogen hat, von derartigen Überlegungen keine Kenntnis erhalten.

Die genannten Regelungen des BKA-Gesetzes beruhen auf dem Prinzip, dass die eingabe- bzw. abrufberechtigte Behörde gem. § 12 Abs. 2 BKA-Gesetz die datenschutzrechtliche Verantwortung u. a. für die Rechtmäßigkeit der Erhebung und die Zulässigkeit der Eingabe zu tragen hat. Insbesondere der erste Aspekt setzt notwendig voraus, dass die betreffende Behörde die Daten selbst erhoben hat, die Umstände der Informationsgewinnung also kennt und beeinflussen konnte. Nach meinen Feststellungen lagen dem BKA zu den von ihm eingegebenen Datensätzen des Bundesgrenzschutzes und der Zollverwaltung nur selten Informationen vor, aus denen sich die Umstände der Datenerhebung hinreichend beurteilen ließen. In den meisten Fällen musste das BKA darauf vertrauen, dass die DNA-Identifizierungsmuster entsprechend den gesetzlichen Vorgaben der §§ 81a ff. StPO erhoben worden waren. Sinn und Zweck der

datenschutzrechtlichen Verantwortung liefen damit ins Leere. Der vom BKA gewählte Weg, DNA-Datensätze des Bundesgrenzschutzes und der Zollverwaltung als eigene Daten im Wege der Amtshilfe in der DNA-Analyse-Datei zu speichern, wird damit besonders fragwürdig.

Ein weiterer Mangel bestand darin, dass zahlreiche von BGS-Dienststellen erhobene DNA-Identifizierungsmuster nicht den gesetzlichen Anforderungen entsprachen. Das Bundesgrenzschutzamt Weil am Rhein, von dem der überwiegende Anteil der BGS-Datensätze stammte, hatte die insbesondere zu Zwecken der Identitätsfeststellung in künftigen Strafverfahren gem. § 81g StPO dienenden DNA-Identifizierungsmuster ohne die erforderliche richterliche Anordnung gem. § 81g Abs. 3 i. V. m. § 81f. StPO erhoben; also nur auf der Grundlage der Einwilligung des Betroffenen.

Hinsichtlich der Delikte, die vom Bundesgrenzschutzamt Weil am Rhein im konkreten Fall zum Anlass einer DNA-Analyse genommen worden waren, u. a. Urkundenfälschung und illegale Schleusung, habe ich in zudem Zweifel an der jeweiligen Erforderlichkeit derartiger Maßnahmen. Zwar sieht der Gesetzgeber in den §§ 81a, 81e StPO die generelle Nutzungsmöglichkeit der molekular genetischen Untersuchung zur Aufklärung der Täterschaft in einem strafrechtlichen Ermittlungsverfahren vor. Zum Zwecke der Identifizierung in künftigen Strafverfahren wird diese Nutzungsmöglichkeit aber auf Straftaten von erheblicher Bedeutung eingeschränkt (§ 81g StPO), weil mit der Speicherung dieser Muster in einer Vorsorgedatei ein weiterer Eingriff in das informationelle Selbstbestimmungsrecht verbunden ist.

Zudem entfällt die Erforderlichkeit eines DNA-Identifizierungsmusters bei solchen Delikten, bei denen der Täter im Zusammenhang mit einer künftigen Straftat nicht typisch Identifizierungsmaterial am Tatort hinterlässt. Insbesondere bei Delikten der Urkundenfälschung und der Schleuserkriminalität scheint mir dies der Fall zu sein.

Die datenschutzrechtliche Kontrolle der DNA-Analyse-Datei hat dazu geführt, dass im Oktober 2002 der Präsident des Bundeskriminalamts eine geänderte Fassung der Errichtungsanordnung zur DNA-Analyse-Datei im Wege der Sofortanordnung erlassen hat. Unter anderem sind danach auch der Bundesgrenzschutz und der Zoll befugt, DNA-Identifizierungsmuster auf konventionellem Wege zur Speicherung in der DNA-Analyse-Datei anzuliefern. Nach Angaben des BKA enthielt die DNA-Analyse-Datei am 26. November 2002 insgesamt 236 347 DNA-Identifizierungsmuster. Hiervon stammen 513 Datensätze vom BKA, 165 Datensätze vom Bundesgrenzschutz sowie 25 Datensätze von Dienststellen der Zollverwaltung. Ohne dem Ergebnis des mit mir noch gem. § 34 Abs. 1 Satz 2 BKA-Gesetz durchzuführenden Anhörungsverfahrens zu der geänderten Errichtungsanordnung vorzugreifen, ist diese Regelung im Grundsatz zu begrüßen, löst sie doch den gesetzwidrigen Rückgriff auf die Amtshilfe ab.

Zwischen dem BMI und mir besteht jedoch weiterhin ein Dissens in der Frage der rechtswirksamen Einwilligung des Betroffenen in die Erstellung eines DNA-Musters zu Zwecken der Identifizierung in künftigen Strafverfahren und dessen Speicherung in der DNA-Analyse-Datei. Unter Hinweis auf die Errichtungsanordnung zur DNA-Analyse-Datei ist nach Auffassung des BMI dies unter der Voraussetzung zulässig, dass die Einwilligung die Anforderungen des § 4a BDSG erfüllt. Dem liege die überwiegende Auffassung in der Literatur zugrunde, dass eine dem Richter vorbehaltene Entscheidung nur dann erforderlich sei, wenn keine wirksame Einwilligung in die Untersuchung erklärt worden sei.

Demgegenüber unterliegt nach übereinstimmender Auffassung der Landesbeauftragten für den Datenschutz und mir die Erstellung eines DNA-Identifizierungsmusters zum Zweck der Identitätsfeststellung in künftigen Strafverfahren gem. § 81g Abs. 1 und 3 i. Vm. § 81f Abs. 1 StPO dem Richtervorbehalt, mit der Folge, dass die anderslautende Regelung in der Errichtungsanordnung zur DNA-Analyse-Datei unwirksam ist (siehe 18. TB Nr 11.6). In der Begründung des Gesetzentwurfs, der zur Einführung des § 81g StPO geführt hat (Bundestagsdrucksache 13/10751), wird hierzu ausgeführt, dass der Richtervorbehalt als verfahrenssichernde Maßnahme gewährleiste, dass die im Rahmen von § 81g Abs. 1 StPO zu stellende Gefahrenprognose vom Richter getroffen werde. Das Erstellen eines DNA-Identifizierungsmusters und dessen Speicherung in der DNA-Analyse-Datei allein auf der Grundlage der Einwilligung des Betroffenen führt hingegen zum Wegfall dieser gesetzlich vorgesehenen Prognose, die aus Gründen der Verhältnismäßigkeit im Zusammenhang mit der Nutzung der DNA-Analyse in künftigen Strafverfahren in die Regelung des § 81g StPO Eingang gefunden hat. Der Richtervorbehalt hat darüber hinaus auch eine regulierende Wirkung: Werden DNA-Muster nur auf Basis der Einwilligung des Betroffenen gewonnen, besteht die Gefahr, dass dies zu einer latenten Erweiterung des Anwendungsbereichs des § 81g StPO führt, da zweifelhaft ist, ob in allen diesen Fällen der Richter der Durchführung einer molekulargenetischen Untersuchung zum Zwecke der Identifizierung in künftigen Strafverfahren unter dem Gesichtspunkt der Erforderlichkeit zugestimmt hätte.

Es besteht kein Zweifel, dass die DNA-Analyse und die Nutzung des DNA-Identifizierungsmusters geeignete Maßnahmen zur Verhütung und Verfolgung von Straftaten sind. Die Aufklärung insbesondere vieler Kapitalverbrechen in der jüngsten Vergangenheit hat das anschaulich gezeigt. Vor diesem Hintergrund sind Überlegungen im politischen Raum, den Anwendungsbereich des § 81g StPO auszudehnen, verständlich und nicht von vorneherein als abwegig zu bezeichnen (siehe Nr. 8.2.3.4). Sollte sich der Gesetzgeber dafür entscheiden, die Nutzung von DNA-Identifizierungsmustern gem. § 81g StPO zu erweitern, wäre dies der geeignete Zeitpunkt, durch eine entsprechende gesetzliche Regelung klarzustellen, dass der richterliche Anordnungsvorbehalt der §§ 81f Abs. 1, 81g Abs. 3 StPO als Bestimmung einer ausschließlichen Zuständigkeit im Zusammenhang mit der Erstellung eines DNA-Identifizierungsmusters zum Zwecke der Identifizierung in künftigen Strafverfahren zu verstehen ist. Eine diesbezügliche Klarstellung halte ich nicht nur aus den oben genannten Gründen für geboten. Sie würde auch die teils unterschiedliche Praxis im Bund, aber auch in den Ländern, bei der Erstellung von DNA-Identifizierungsmustern gem. § 81g StPO vereinheitlichen.

13.4 Gewalttäterdateien – Rechts – Links – Ausländer – angemessene Reaktion auf die politisch motivierte Kriminalität?

Die deutliche Zunahme rechtsextremer Straftaten in Deutschland im Jahre 2000, insbesondere der dabei zu verzeichnende Anstieg politisch motivierter Gewalttaten, veranlasste die

Ständige Konferenz der Innenminister und -senatoren der Länder (IMK) im November 2000 dazu, verschiedene Maßnahmen zur Bekämpfung rechtsextremistischer, antisemitistischer und fremdenfeindlicher Kriminalität zu erörtern. Neben der Verwendung des personengebundenen Hinweises „REMO“ für Straftäter, bei denen Anhaltspunkte vorliegen, dass sie Straftaten aus rechts orientiert politisch motivierten Beweggründen begangen haben, in den INPOL-Dateien „Personenfahndung“, „Kriminalaktennachweis“ und „Erkennungsdienst“ wurde insbesondere zur Verhinderung rechtsorientiert politisch motivierter Gewalttaten beschlossen, die bundesweite Datei „Gewalttäter rechts“ einzurichten. Darüber hinaus wurde beschlossen, rechte Störer im Rahmen der Gefahrenabwehr auf Länderebene zu speichern. Auf Initiative Bayerns kam die IMK schließlich überein, diese Maßnahmen auch auf linksorientiert politisch motivierte Straftäter und Straftäter politisch motivierter Ausländerkriminalität zu erstrecken. Hierzu sollten die personengebundenen Hinweise „LIMO“ bzw. „AUMO“ verwendet werden sowie entsprechende „Gewalttäterdateien“ und Störerdateien auf Länderebene eingerichtet werden.

Der Personendatenbestand der „Gewalttäterdateien“ soll vorerst durch eine entsprechende Anlass/Zweck-Kombination über die Datei „Personenfahndung“ zugänglich gemacht werden. Aus Sicht der IMK sind politisch motivierte Straftaten wegen ihrer besonderen Bedeutung zudem grundsätzlich bundesweit zu erfassen.

Nach Aussage des BMI war Ziel dieser Maßnahmen, jedem Polizeibeamten im Bund und in den Ländern für die Sachbearbeitung und für polizeiliche Kontrollen vor Ort entsprechende personenbezogene Informationen über politisch motivierte Kriminalität zur Verfügung stellen zu können, mithilfe derer geeignete polizeipräventive und/oder -repressive Maßnahmen ergriffen werden können. Die bisherigen Datenverarbeitungsmöglichkeiten hätten dies im Hinblick auf die geltenden Bestandsführungs- und Zugriffsregelungen nicht gewährleistet: So stünde der Bestand der bereichsspezifischen INPOL-Datei zum Polizeilichen Staatsschutz wegen der Sensibilität der darin enthaltenen, z. T. unbewerteten Daten nur den Staatsschutzdienststellen des Bundes und der Länder zur Verfügung. Zudem gäbe der personengebundene Hinweis in INPOL über die jeweilige politische Motivation des Täters dem Polizeibeamten vor Ort nur insoweit die entsprechende Information, als diese Person auch zur Fahndung ausgeschrieben wäre. Erst durch die Einrichtung der o. a. „Gewalttäterdateien“ und deren Abbildung in der Datei „Personenfahndung“ würde erreicht, dass bei jeder Fahndungsabfrage vor Ort politisch motivierte Gewalttäter bzw. gewaltbereite Personen einer polizeilichen Kontrolle unterzogen werden könnten, unabhängig davon, ob zu ihnen eine aktuelle Fahndungsnotierung besteht.

Meine ursprünglich gehegten Zweifel an der Erforderlichkeit und Verhältnismäßigkeit des von der IMK beschlossenen Maßnahmenkatalogs habe ich vor diesem Hintergrund zurückgestellt. Gleichwohl werfen die beschlossenen Einzelmaßnahmen eine Reihe von datenschutzrechtlichen Fragen auf.

Über die datenschutzrechtlichen Aspekte der Einführung des personengebundenen Hinweises „REMO“ habe ich bereits in meinem 18. TB (Nr. 11.1) berichtet. Die dort dargelegten Bedenken habe ich auch hinsichtlich der Einführung der personengebundenen Hinweise „LIMO“ und „AUMO“ in den Dateien „Personenfahndung“, „Kriminalaktennachweis“ und „Erkennungsdienst“.

Im Zusammenhang mit den Dateien „Gewalttäter Rechts“, „Gewalttäter Links“ und „Straftäter politisch motivierter Ausländerkriminalität“ stößt vor allem die vorgesehene Speicherung personenbezogener Daten zu so genannten sonstigen Personen i. S. v. § 8 Abs. 5 BKA-Gesetz auf datenschutzrechtliche Bedenken. Bei dieser Personengruppe handelt es sich weder um Beschuldigte noch um Tatverdächtige. Für eine Verarbeitung personenbezogener Daten zu diesen Personen setzt § 8 Abs. 5 BKA-Gesetz deshalb eine auf der Grundlage bestimmter Tatsachen gestützte Straffälligkeitsprognose voraus. Weil die Einschätzung der politischen Motivation einer Person unsicher und die Prognose, ob der Betroffene Straftaten von erheblicher Bedeutung begehen wird, die im ursächlichen Zusammenhang mit seiner politischen Orientierung stehen, ohnehin schwierig ist, sehe ich die Gefahr, dass – mangels anderer Anhaltspunkte – bereits eine bloße Störung als alleinige Grundlage für die zu treffende Prognose herangezogen werden könnte. Dies könnte dazu führen, dass eine Vielzahl unbedeutender Störer oder sogar friedlicher Demonstranten in einer Verbunddatei des polizeilichen Informationssystems des Bundes und der Länder geführt werden, die auf die Verfolgung und Verhütung von Straftaten von länderübergreifender, internationaler oder erheblicher Bedeutung abzielt. Zwar konnte im Rahmen der Erörterungen der Errichtungsanordnungen zu den jeweiligen Gewalttäterdateien erreicht werden, dass das Aussonderungsprüfdatum für sonstige Personen auf zwei Jahre festgelegt wird, mit der Folge, dass mit Ablauf dieser Frist die Aktualität des betreffenden Datensatzes und die Rechtmäßigkeit seiner weiteren Speicherung überprüft werden müssen. Meinem Vorschlag, aus Gründen der Verhältnismäßigkeit von einer Speicherung dieses Personenkreises ganz abzusehen und ihn allenfalls in den auf Länderebene errichteten Störerdateien zu erfassen, wurde allerdings nicht gefolgt.

Vor dem Hintergrund, dass in den Gewalttäterdateien nur politisch motivierte Straftäter gespeichert werden sollen, die eine besondere Gewaltbereitschaft erkennen lassen, bedauere ich zudem, dass der in der jeweiligen Errichtungsanordnung aufgeführte Straftatenkatalog auch Straftatbestände enthält, die keinen Bezug zur Gewaltkriminalität aufweisen. Beispielhaft gilt dies für den Straftatbestand des Diebstahls (§ 242 des Strafgesetzbuches). Durch einen nachträglich eingefügten Zusatz in der jeweiligen Errichtungsanordnung, wonach auch bei diesem Straftatbestand aufgrund bestimmter Tatsachen eine Gewaltbereitschaft des Täters erkennbar sein muss, ist der erforderliche Bezug zur Gewaltkriminalität zumindest verdeutlicht worden.

Für problematisch halte ich schließlich, dass nach der Errichtungsanordnung nur der Zweck der jeweiligen Datei festgelegt werden muss. Für den Anwender entsteht der Eindruck, dass in jedem Fall personenbezogene Daten von Beschuldigten oder Verdächtigen in die Datei eingestellt werden sollen, sofern sie sich auf die dort aufgezählten Straftatbestände beziehen. Die Speicherung personenbezogener Daten in einer beim BKA geführten Verbunddatei i. S. v. § 11 Abs. 1 BKA-Gesetz ist aber nur zulässig, soweit dies für das BKA nach Maßgabe des § 2 Abs. 1 BKA-Gesetz zur Verhütung und Verfolgung von Straftaten länderübergreifender, internationaler oder erheblicher Bedeutung

in Wahrnehmung seiner Zentralstellenfunktion für die Polizeien des Bundes und der Länder erforderlich ist. Nur insofern kann eine bundesweite Verfügbarkeit personenbezogener Daten, die einen Eingriff besonderer Intensität in das Persönlichkeitsrecht darstellt, als verhältnismäßig angesehen werden. In der Gesetzesbegründung zu § 2 Abs. 1 BKA-Gesetz hat der Gesetzgeber dazu ausgeführt, dass die INPOL-Relevanz in jedem konkreten Einzelfall gegeben sein müsse. Für die Feststellung einer Straftat von erheblicher Bedeutung komme es nicht auf den abstrakten Charakter eines Straftatbestandes, sondern vielmehr auf Art und Schwere der konkreten Tat an. Dabei muss es sich bei der Anlasstat um ein Delikt handeln, welches mindestens der mittleren Kriminalität zuzurechnen ist. Vor diesem Hintergrund sind die in dem Straftatenkatalog u. a. aufgezählten Straftaten der Nötigung, des gefährlichen Eingriffs in den Straßenverkehr, des Hausfriedensbruchs, des Diebstahls oder des Widerstands gegen Vollstreckungsbeamte nur in Ausnahmefällen von erheblicher Bedeutung, sofern sie nicht länderübergreifend begangen wurden. Meinem Vorschlag, eine Modifizierung der Zweckbeschreibung der jeweiligen Datei dahin gehend vorzunehmen, dass die Voraussetzungen des § 2 Abs. 1 stärker zum Ausdruck kommen, wurde nicht gefolgt. Für die IMK und das BMI haben vielmehr politisch motivierte Gewalttaten grundsätzlich erhebliche Bedeutung i. S. v. § 2 Abs. 1 BKA-Gesetz und bedürfen daher der Abbildung in einer bundesweit zugänglichen Datei.

Die Problematik der Verbunddateien „Gewalttäter Rechts“, „Gewalttäter Links“ und „Straftäter politisch motivierter Ausländerkriminalität“ wird allein schon daran deutlich, dass das mit mir durchzuführende Anhörungsverfahren nach § 34 Abs. 1 BKA-Gesetz und das sich anschließende Länderbeteiligungsverfahren zu den jeweiligen Dateierrichtungsanordnungen erst am 4. Oktober 2002 abgeschlossen werden konnten. Dies obgleich die Amtsleitung des BKA bereits am 23. Januar 2001 die Einrichtung dieser Dateien per Sofortanordnung verfügt hatte. Mittlerweile enthält die Datei „Gewalttäter Rechts“ 1 807, die Datei „Gewalttäter Links“ 1 174 sowie die Datei „Straftäter politisch motivierter Ausländerkriminalität“ 338 Datensätze (Stand: jeweils 15. Oktober 2002).

Vor dem Hintergrund der von der IMK beschlossenen Maßnahmen zur Bekämpfung der politisch motivierten Kriminalität habe ich angeregt, den Katalog der bisher verwendeten personengebundenen Hinweise im Hinblick auf die Vermeidung von Redundanzen zu überarbeiten sowie zu überprüfen, inwieweit auf derzeit genutzte Dateianwendungen zur Abbildung der politisch motivierten Kriminalität verzichtet werden kann. Ich begrüße es, dass die IMK entsprechende Beschlüsse gefasst hat.

13.5 Gipfeltreffen in Göteborg und in Genua 2001 – Rolle des BKA

Die Berichterstattung anlässlich des Europäischen Rates in Göteborg und des Weltwirtschaftsgipfels der G8-Staaten in Genua im Sommer 2001 über die von Bund und Ländern durchgeführten Maßnahmen zur Verhinderung von Ausschreitungen deutscher Staatsangehöriger sowie Eingaben hiervon Betroffener an mich und die Landesbeauftragten für den Datenschutz haben mich veranlasst, die vom BKA in diesem Zusammenhang ergriffenen Maßnahmen zu überprüfen.

Das BKA ist gem. § 3 BKA-Gesetz Nationales Zentralbüro Deutschland für die Internationale Kriminalpolizeiliche Organisation (IKPO-Interpol). In dieser Funktion obliegt ihm der polizeiliche Nachrichtenaustausch mit ausländischen Polizei- und Justizbehörden. Nach Maßgabe des § 14 BKA-Gesetz erfolgen Datenübermittlungen an ausländische Stellen insbesondere zur Straftatenverhütung und zur Gefahrenabwehr, aber auch im Rahmen der Rechtshilfe.

In Erfüllung dieser Aufgabe wurden nach Mitteilung des BKA im Zusammenhang mit dem Weltwirtschaftsgipfel G8 in Genua den zuständigen italienischen Behörden im Vorfeld Daten von 191 deutschen Staatsangehörigen übermittelt, die in Dateien des polizeilichen Informationssystems des Bundes und der Länder gespeichert waren. Die Auswahl der übermittelten Personendatensätze sei auf der Grundlage der beim BKA vorliegenden Erkenntnisse mit Globalisierungsbezug erfolgt und habe sich auf Beschuldigte und auch sonstige Personen im Sinne von § 8 Abs. 5 BKA-Gesetz bezogen. Dagegen seien im Vorfeld des EU-Gipfels in Göteborg keine Personendaten übermittelt worden. Dies sei erst dann geschehen, als schwedische Behörden, z. B. aus Anlass einer Fahrzeug- oder Personenkontrolle, eine Erkenntnisanfrage zu deutschen Staatsangehörigen an das BKA gerichtet hätten.

Ich habe gegen die Übermittlung personenbezogener Informationen an ausländische Polizeibehörden zum Zwecke der Verhinderung und Ahndung von Ausschreitungen bei Großveranstaltungen keine Einwände, wenn die diesbezüglichen Voraussetzungen des BKA-Gesetzes erfüllt sind. Jedoch müssen die Daten in den Dateien des polizeilichen Informationssystems – in der Regel handelt es sich dabei um Erkenntnisse des polizeilichen Staatsschutzes – zum Zeitpunkt ihrer Übermittlung aktuell und noch zulässig gespeichert sein. Bei der Bearbeitung von Auskunftsbegehren von Personen, die im Vorfeld der Veranstaltungen in Göteborg und Genua von polizeilichen Maßnahmen betroffen waren, haben meine Länderkollegen und ich festgestellt, dass dies nicht immer der Fall war. Unter anderem war hierfür die unterlassene Pflege des Datenbestandes in den betreffenden Dateien, die durch die zum Teil zu langen Aussonderungsprüffristen begünstigt wird, die Ursache. In den von mir bearbeiteten Fällen lag die datenschutzrechtliche Verantwortung für diese Versäumnisse allerdings bei dem Land, das den betreffenden Datensatz in die Datei eingestellt hatte. Gleichwohl stellt sich die Frage nach der Verantwortung des BKA in seiner Funktion als Zentralstelle, wenn es derartige Datensätze an ausländische Stellen übermittelt. Ich stimme mit dem BKA darin überein, dass es sich im Zusammenhang mit einer Datenübermittlung nach § 14 Abs. 1 BKA-Gesetz grundsätzlich darauf verlassen muss, dass die in den Dateien des polizeilichen Informationssystems eingestellten Daten rechtmäßig erhoben worden sind und deren Speicherung zum Zeitpunkt der Übermittlung noch zulässig ist. Aus der dem BKA vom Gesetzgeber in § 14 Abs. 7 BKA-Gesetz übertragenen Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten an öffentliche Stellen außerhalb des Geltungsbereichs des BKA-Gesetzes folgt aber eine umso höhere Überprüfungs- und Sorgfaltspflicht, je sensibler die Daten sind, die übermittelt werden sollen. Dies gilt insbesondere für Dateien des polizeilichen Staats-

schutzes, in denen auch so genannte weiche Daten verarbeitet werden und auf die wegen ihres sensiblen Charakters bereits im Inland Zugriffsbeschränkungen zugunsten bestimmter Spezialdienststellen bestehen. Eine genauere Überprüfung ist besonders dann geboten, wenn Anhaltspunkte dafür bestehen, dass der zu übermittelnde Datensatz unzulässig gespeichert ist. Ich habe gegenüber dem BKA deutlich gemacht, dass dies künftig stärker zu beachten ist.

Datenschutzrechtlich problematisch sind auch die Datenverarbeitungsmaßnahmen des BKA im Nachgang zu den Ereignissen bei den Gipfeltreffen in Göteborg und Genua. Dem BKA wurden von den schwedischen bzw. italienischen Behörden personenbezogene Daten von Personen, die einer polizeilichen Kontrolle unterzogen worden waren, sowie von Personen, gegen die vor Ort Ermittlungsverfahren wegen strafbarer Handlungen eingeleitet worden waren, übermittelt. Nach Auskunft des BKA seien Daten von Personen, gegen die Ermittlungsverfahren eingeleitet worden waren, vom BKA u. a. in der Verbunddatei des polizeilichen Staatsschutzes gespeichert worden. Daten zu Personen, die lediglich einer polizeilichen Kontrolle unterzogen, gegen die aber keine weiteren strafprozessualen Maßnahmen durchgeführt worden waren, seien ausschließlich in die Auswertedatei „Global“ (s. Nr. 13.2.2) eingestellt worden. Ich habe insbesondere Zweifel an der Zulässigkeit der zuletzt genannten Maßnahmen. Die Speicherung von Personen allein aufgrund des Umstandes, dass sie einer Personenkontrolle unterzogen und zu ihnen Erkenntnisanfragen an das BKA gerichtet worden sind, ist weder mit dem Zweck der Datei „Global“ vereinbar noch ist dies erforderlich zur Erfüllung der Zentralstellenaufgabe des BKA. Ziel der Auswertedatei „Global“ ist es, Informationen über Ereignisse sowie Personen im Zusammenhang mit gewalttätigen Aktionen und anderen Straftaten militanter Globalisierungsgegner auszuwerten, um den Polizeien des Bundes und der Länder bei der Verfolgung und Verhütung der Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung neue Bekämpfungsansätze zu vermitteln. Dies wird von mir nicht infrage gestellt. Die damit verbundenen Speicherungen dürfen jedoch nicht solche Personen umfassen, zu denen die Erkenntnisanfragen der ausländischen Polizeibehörden keinen polizeirelevanten Bestand in Deutschland erbracht haben, die also lediglich von ihrem Recht auf Demonstrationsfreiheit Gebrauch gemacht haben. Die Speicherung dieses Personenkreises in einer polizeilichen Datei ist nicht zulässig, selbst wenn daraus keine Datenübermittlungen an andere Stellen stattfinden.

Im Hinblick auf die Aufgabe des BKA als Zentralstelle der Polizeien des Bundes und der Länder kann es erforderlich werden, von deutschen Staatsbürgern im Ausland begangene Straftaten in den Dateien des polizeilichen Informationssystems nach Maßgabe des § 2 Abs. 1 BKA-Gesetz zu speichern, um künftig gleichgelagerte oder ähnliche Straftaten im In- oder Ausland verhüten zu können. Dabei ist allerdings immer auf den konkreten Einzelfall abzustellen. Eine Körperverletzung oder eine Sachbeschädigung, die im Inland lediglich regionale Bedeutung hätte, wird nicht dadurch zu einer INPOL-relevanten Straftat im Sinne von § 2 Abs. 1 BKA-Gesetz, weil sie im Ausland begangen worden ist. Maßgebend müssen die Umstände des Einzelfalls unter Beachtung des Verhältnismäßigkeitsgrundsatzes bleiben. Vor diesem Hintergrund kann es gerechtfertigt sein, Personen, die an gewalttätigen Demonstrationen in Göteborg und in Genua teilgenommen haben und gegen die seitens der schwedischen bzw. italienischen Behörden Ermittlungsverfahren eingeleitet worden sind, in den Verbunddateien des polizeilichen Staatsschutzes zu speichern. Eine besondere Interessenabwägung ist aber dort zu treffen, wo die Umstände, die zu den Anschuldigungen geführt haben – wie bei den Festnahmen von Demonstranten in der „Diaz-Schule“ in Genua – zweifelhaft sind. In diesen Fällen hielte ich es für angemessen, wenn die betreffenden Personen zunächst nur für eine kurze Dauer in den betreffenden Dateien gespeichert würden und vor deren weiterer Verlängerung zunächst Informationen über den Stand des der jeweiligen Speicherung zugrunde liegenden Ermittlungsverfahrens bei den Behörden eingeholt werden müssten. Aus Sicht des BKA wäre es mit einem unverhältnismäßigen Aufwand verbunden, regelmäßig nach dem Sachstand im Ausland eingeleiteter Ermittlungsverfahren fragen zu müssen. Hierzu bestehe auch keine gesetzliche Verpflichtung. In der Regel erfolge eine Nachfrage durch ein Auskunftsersuchen des Betroffenen. Ergäben sich daraus Anhaltspunkte für eine Löschung, käme das BKA dieser Verpflichtung gem. § 32 Abs. 2 BKA-Gesetz nach.

Diese Vorgehensweise des BKA wird bei künftigen „Gipfeltreffen“ insbesondere im Hinblick auf ihre Bedeutung in der Praxis einer eingehenden Beobachtung zu unterziehen sein.

13.6 Rechtstatsachensammelstelle des BKA ohne Impulse

Auch im Berichtszeitraum hat die Arbeit der beim BKA eingerichteten Rechtstatsachensammelstelle keine neuen Impulse erhalten. Gleiches gilt für den Gesprächskreis „Rechtstatsachen“, der zuletzt im März 1999 zu einem Meinungsaustausch über Initiativen auf dem Gebiet der Rechtstatsachenforschung zusammengetroffen ist. Von der Arbeit der Rechtstatsachensammelstelle des BKA und meiner Absicht, Gespräche mit dem BMI über geeignete Schritte zur Verbesserung der Situation zu führen, habe ich im 18. TB (Nr. 11.9) berichtet. In diesen Gesprächen habe ich vorgeschlagen, das aus dem Jahre 1995 stammende Themenraster, welches der bei der Rechtstatsachensammelstelle geführten Bund/Länder-Fallsammlung zugrunde liegt, der neueren Entwicklung im repressiven und präventiv-polizeilichen Bereich und den damit verbundenen Datenerhebungsbefugnissen der Polizei anzupassen. Zudem halte ich es für erforderlich, dass sich künftig alle Länderpolizeien wieder regelmäßig und umfassend an der Informationsanlieferung beteiligen. Schließlich sollte es der Rechtstatsachensammelstelle über das Sammeln von Rechtstatsachen hinaus erlaubt werden, eigene Analysen des Informationsmaterials, statistische Auswertungen oder Schwerpunktbildungen innerhalb der angelieferten Falldarstellungen vorzunehmen. Nur so lassen sich aus meiner Sicht aussagekräftige empirische Erkenntnisse als Basis für Gesetzesinitiativen und -evaluationen durch den Gesetzgeber gewinnen. Langfristiges Ziel muss es aus meiner Sicht sein, die bestehenden Befugnisse der Polizeien zu Eingriffen in das Persönlichkeitsrecht ergebnisoffen und ggf. durch eine unabhängige Forschungseinrichtung auf Grundlage der zusammengetragenen Rechtstatsachen überprüfen zu lassen. Das BMI hat – allerdings unter Hinweis auf die Zuständigkeit der Länder für den Bereich der präventiv-polizeilichen

Eingriffsbefugnisse – meinen Vorschlägen im Wesentlichen zugestimmt. Geschehen ist gleichwohl wenig. Zwar hat der Arbeitskreis II der Ständigen Konferenz der Innenminister und -senatoren der Länder im Oktober 2001 beschlossen, das Themenraster der Rechtstatsachensammelstelle des BKA zu aktualisieren. Ob auch die Ankündigung des BMI, das BKA mit Vorschlägen zur Reform der Rechtstatsachensammlung im Verbund von Bund und Ländern zu beauftragen sowie meine Vorschläge den Innenministern der Länder unterbreiten zu wollen, in die Tat umgesetzt wurde, ist mir nicht bekannt. Meine Sachstandsanfragen gegenüber dem BMI zu diesem Thema sind bisher unbeantwortet geblieben. Die ebenfalls vom BMI vorgesehene Fachtagung im Herbst 2001 zu Fragen der Rechtstatsachensammlung, bei deren Vorbereitung auch ich mit einbezogen werden sollte, ist aber offenbar nicht durchgeführt worden.

Der Gesetzgeber hat zunehmend die Bedeutung der Evaluierung von Gesetzen, insbesondere bei Eingriffsbefugnissen in die Persönlichkeitsrechte der Bürger, anerkannt. Beginnend mit den Berichtspflichten gem. § 100e Strafprozessordnung im Zusammenhang mit der akustischen Wohnraumüberwachung (siehe auch Nr. 8.4) sind im Terrorismusbekämpfungsgesetz erstmals die Voraussetzungen für eine Erfolgskontrolle und die Verpflichtung zur Evaluierung gesetzlich geregelt worden (s. Nr. 2.3.1). Das informationelle Selbstbestimmungsrecht wird aber auch durch die präventiv-polizeilichen Eingriffsbefugnisse sowie die darauf beruhenden Datenerhebungs- und -verarbeitungsbefugnisse tangiert. Auch wenn Polizeiangelegenheiten im Wesentlichen in die Zuständigkeit der Länder fallen, zeigen die verschiedenen Formen der Zusammenarbeit von Bund und Ländern bei der polizeilichen Datenverarbeitung, dass die Evaluierung dieser Befugnisse auch eine Angelegenheit des Bundes ist. Der Umstand, dass die Rechtstatsachensammelstelle im BKA seit ihrer Gründung lediglich befugt ist, die ihr angelieferten rechtstatsächlichen Informationen zu registrieren und zu dokumentieren und seit Jahren keine Initiativen festzustellen sind, diesen Zustand zu verbessern, verdeutlicht, dass zu dem Thema der Evaluierung polizeilicher Eingriffsbefugnisse noch erhebliche Anstrengungen unternommen werden müssen.

13.7 Geldwäschebekämpfungsgesetz

Die Ereignisse vom 11. September 2001 (siehe Nr. 2) führten auch zu verstärkten Bemühungen der Bundesregierung, die Geldwäschebekämpfung effizienter zu gestalten, verbunden mit dem weiteren Ziel, die Finanzströme des internationalen Terrorismus offen zu legen. Ferner war Deutschland gehalten, die Umsetzung der novellierten Geldwäscherichtlinie 2001/97/EG des Europäischen Parlaments und des Rates vom 4. Dezember 2001 zur Änderung der Geldwäscherichtlinie aus dem Jahr 1991 voranzutreiben. Daraus entstand der Entwurf eines Geldwäschebekämpfungsgesetzes unter Federführung des BMI, der schließlich am 18. August 2002 als Gesetz zur Verbesserung der Bekämpfung der Geldwäsche und der Bekämpfung der Finanzierung des Terrorismus (Geldwäschebekämpfungsgesetz) in Kraft trat (BGBl. I S. 3105f). Das Gesetz beinhaltet neben Änderungen des Geldwäschegesetzes auch Änderungen des Zollverwaltungsgesetzes, des Gesetzes über das Kreditwesen und des BKA-Gesetzes.

Die Vorschläge zur Änderung des Geldwäschegesetzes sind sowohl für die verpflichteten Stellen – wegen ihrer Anforderungen –, aber auch aus datenschutzrechtlicher Sicht nicht unproblematisch. Ich hatte schon in früheren Tätigkeitsberichten (s. u. a. 18. TB Nr. 11.5) darauf hingewiesen, dass die Einbeziehung der Daten von Personen, gegen die sich kein konkreter strafrechtlicher Anfangsverdacht im Sinne des § 152 Abs. 2 Strafprozessordnung erhärten lässt, in die beim BKA geführte Geldwäschedatei verstärkter datenschutzrechtlicher Beobachtung bedarf.

Unter dieser Prämisse habe ich gegen einige Vorschläge der Bundesregierung im o. g. Gesetzentwurf erhebliche datenschutzrechtliche Bedenken vorgebracht. So sieht das Gesetz u. a. eine erweiterte Identifizierungspflicht bei der Aufnahme von Geschäftsbeziehungen vor. Hier habe ich bemängelt, dass die Feststellung der Identitätsangaben, soweit dies durch eine Kopie des Ausweisdokuments erfolgt, auch ohne Einwilligung des Betroffenen erfolgen darf, was zur Speicherung von mehr personenbezogenen Daten führt, als für diesen Zweck erforderlich ist. Ich habe ferner gerügt, dass die Einbeziehung von Angehörigen der freien Berufe, u. a. Rechtsanwälte, Notare, Wirtschaftsprüfer usw., in den Kreis der anzeigepflichtigen Stellen nach § 3 Geldwäschegesetz (GwG) mit den für diese Berufsgruppen geltenden Verschwiegenheitspflichten nicht vereinbar ist. Diesen Zielkonflikt hat der Gesetzgeber für die Angehörigen der vorgenannten Berufsgruppen dadurch gelöst, dass sie von der Anzeigepflicht befreit sind, soweit sie ihre Informationen bei der Rechtsberatung oder Prozessvertretung des Mandanten erhalten haben. Im Übrigen leiten sie die Anzeige an die für sie zuständige Bundesberufskammer. Das schon bisher bestehende Verbot einer Unterrichtung der Betroffenen über eine Anzeige oder ein eingeleitetes Strafverfahren bleibt bestehen.

Gegen die Beauftragung des Bundeskriminalamtes als Financial Intelligence Unit-FIU – i. S. der FATF – für die Bundesrepublik Deutschland, das auch den Datenaustausch mit den entsprechenden Geldwäschezentralstellen anderer Staaten übernimmt, habe ich keine grundlegenden datenschutzrechtlichen Bedenken erhoben. Für weiterhin bedenklich halte ich jedoch die Regelung, wonach Geldwäscheverdachtsanzeigen nicht nur den zuständigen Strafverfolgungsbehörden, sondern zeitgleich in Kopie dem Bundeskriminalamt „Zentralstelle für Verdachtsanzeigen“ zu übermitteln sind. Damit erhält das BKA ungefilterte Informationen aus Verdachtsanzeigen, ohne dass die strafrechtliche Relevanz dieser Angaben von den zuständigen Behörden zuvor überprüft worden ist. Das BKA darf diese Verdachtsanzeigen nach § 5 GwG sammeln und auswerten. Hierunter fällt auch der Abgleich mit anderen beim BKA geführten Dateien, was eine erhebliche Ausweitung der Zentralstellenkompetenz des BKA darstellt. Damit wird meine Besorgnis verstärkt, dass in der Geldwäschedatei beim Bundeskriminalamt jahrelang Daten über Personen gespeichert werden, die weder als Beschuldigte noch als Verdächtige im Sinne des § 8 BKA-Gesetz anzusehen sind. Daran ändert auch der Umstand nichts, dass in § 11 Abs. 9 GwG erweiterte Mitteilungspflichten der Staatsanwaltschaft gegenüber dem Bundeskriminalamt über den Ausgang von Strafverfahren in Fällen von Geldwäscheverdachtsanzeigen statuiert werden. Betrachtet man die bisherigen Auswertungen zu strafrechtlichen Ermittlungen in Geldwäschefällen, so ist nicht auszuschließen, dass ein erheblicher Anteil der wegen Geldwäscheverdachts angezeigten Personen rein zur Vorsorge in polizeilichen Dateien jah-

relang erfasst bleiben. Mit dieser Blickrichtung werde ich die Geldwäschedatei einer datenschutzrechtlichen Kontrolle unterziehen.

13.8 INPOL-neu: Neuer Anlauf

Das Projekt der Fortentwicklung des polizeilichen Informationssystems von Bund und Ländern – INPOL-neu – hat im April 2001 eine Zäsur erfahren:

Im Rahmen der zu diesem Zeitpunkt vor gesehenen Einführung wurde festgestellt, dass die für das System bestimmte Software im Hinblick auf das Antwort-Zeit-V erhalten bei Erkenntnisabfragen den polizeifachlichen Anforderungen nicht entsprach. Zwar konnten die Schwächen der Software in der Folgezeit behoben werden, doch wurden wegen des komplexen Entwicklungsansatzes der INPOL-neu Konzeption weitere Realisierungsrisiken gesehen. Diese bestanden unter anderem darin, alle INPOL-Daten nur einmal in einer Datenbank zu erfassen mit der Folge, dass die Polizeibehörden in Bund und Ländern INPOL-neu hätten gleichzeitig in Betrieb nehmen müssen, um Zugang zu der Datenbank zu erhalten. Bund und Länder verständigten sich daher auf eine Alternativplanung, die zu einer Neuausrichtung der ursprünglichen Projektstrategie führte. Die durch Beschluss der Ständigen Konferenz der Innenminister und -senatoren der Länder festgelegten Eckpunkte des neuen Konzepts sehen nunmehr in mehreren Schritten die Entwicklung von zwei Datenbanken – einer operativen und einer so genannten dispositiven – vor. Die operative Datenbank, die vorrangig realisiert werden soll, ist sp eziell auf polizeiliche Standardabfragen (Erkenntnisabfragen, Fahndung) zugeschnitten und soll 80 % der Anwendunge n abdecken. Daneben soll die auf komplexe Recherche- und Analysezwecke zugeschnittene dispositive Datenbank in einem späteren Entwicklungsschritt verwirklicht werden, wobei die im Rahmen des ursprünglichen Projekts bereits entwickelten Systemkomponenten genutzt werden sollen. Die neue Produktversion von INPOL-neu soll zudem sicherst ellen, dass sich die Länder entsprechend der von ihnen erzielten Realisierungsfortschritte individuell auf das neue INPOL-System aufschalten können bei gleichzeitiger Beibehaltung der Funktionalität von INPOL-aktuell bis zu diesem Zeitpunkt. Bei ihrer Planung gehen BMI und BKA davon au s, dass am 16. August 2003 INPOL-aktuell abgeschaltet werden kann.

Die mit der Realisierung de s überarbeiteten Konzepts INPOL-neu verbundenen Neuerungen zeichnen sich bereits ab: So soll die Benutzeroberfläche für die Nutzer des Systems mittels Internettechnologi e modernisiert werden. Zudem wird angestrebt, Personendaten um Lichtbilder zu erweitern, so genannte Kombi-Abfragen z. B. zu Schengen und INPOL in einer Auskunft zu ermöglichen sowie Falldatengruppen zu eröffnen, in denen Informationen zu Personen und Sachen mit einem bestimmten Fall verbunden werden können.

Die Datenschutzbeauftragten des Bundes und der Länder haben die bisher gut zehnjäh rige konzeptionelle Arbeit am Projekt INPOL-neu fortlaufend begleitet. Über die dabei aufgetretenen datenschutzrechtlichen Probleme habe ich regelmäßig berichtet (zuletzt 18. TB Nr. 11.2). Auch wenn die nunmehr beschlossene Revision des Entwicklungskonzepts faktisch einen Neustart des Projekts INPOL-neu bedeutet, behalten die von den Datenschutzbeauftragten in der V ergangenheit zum Projekt INPOL-neu gefassten Beschlüsse und ergänzend erteilten Hinweise zum großen Teil ihre Aktualität. Dies gilt z. B. für den Umfang der Protokollierung von Abrufen aus dem polizeilichen Informationssystem (17. TB Nr. 11.9) oder die Abbildung der kriminellen Historie zu einer Person (18. TB Nr. 11.2.2). Die Datenschutzbeauftragten des Bundes und der Länder werden auch weiterhin die mit der Neuausrichtung des Projekts INPOL-neu angestrebten Veränderungen im polizeilichen Informationssystem des Bundes und der Länder unter datenschutzrechtlichen Gesichtspunkten bewerten. Hierüber werde ich auch künftig regelmäßig berichten.

13.9 AFIS – Automatisiertes Fingerabdruckidentifizierungssystem

Rund zehn Jahre nach Einführung des automatisierten Fingerabdruckidentifizierungssystems AFIS, das die kriminalistische Arbeit der deutschen Polizei entscheidend verbessert hat, ist beim Bundeskriminalamt und den Landeskriminalämtern ein neues Verfahren eingeführt worden, das die Identifizierung von Straftätern auch mithilfe von Handflächenabdrucken ermöglichen soll. Während bisher nur Fingerabdrucke und Fingerabdruckspuren zur Identifizierung ausgewertet wurden, sollen zukünftig auch Handflächenabdrucke und Handflächenspuren den Täter überführen helfen. Dies wird erleichtert mittels des neuen Verfahrens „METAMORPHO“. Die Auswertung der Handflächen, in Er gänzung der bisherigen zehn Fingerkuppen, bringt nach Auffassung der Polizei einen bedeutenden Fortschritt, zumal ein beträchtlicher Teil der hinterlassenen Spuren von Handflächen stammen soll.

Nicht zuletzt können mit „MET AMORPHO“ auch Handflächenspuren verglichen werden, die bereits in der Vergangenheit am T atort gesichert, aber nicht automatisiert ausgewertet werden konnten. Zu diesem Zweck ist noch im Jahre 2002 ein Kontingent von ca. 500 000 Handflächenabdrucken, die von den Ländern stammen, bei der amerikanischen Tochter eines französischen Unternehmens digitalisiert worden, um anschlie ßend in AFIS eingestellt zu werden. Die Einspeisung in AFIS war zum 23. Januar 2003 abgeschlossen. Dies bedeutet, dass lediglich ein Drittel des insgesamt vorhandenen Materials – wahrscheinlich infolge haushaltsrechtlicher Zwänge – kodiert wurde, wobei sich der auf die einzelnen Länder entfallende Anteil nach einem bestimmten Schlüssel richtet. Die Landeskriminalämter können nun mit Handflächenspuren in diesem Datenbestand recherchieren.

Ich habe eher zufällig von diesem neuen Verfahren Kenntnis erlangt, nachdem ein Pilotversuch mit entsprechendem Spurenmaterial aus Sachsen bereits abgeschlossen war. Der Vertrag zur retrograden Erfassung der Abdrucke aus den übrigen Ländern wurde dann im September 2002 vom Beschaffungsamt des BMI mit dem französischen Unternehmen abgeschlossen. Genau genommen handelt es sich um die Aktualisierung und Ergänzung eines bereits aus dem Jahre 1992 stammenden V ertrages zur Einführung von AFIS. Auf meine Frage, warum ich bei dieser Aktion, die heikle datenschutzrechtliche Fragen, insbesondere wegen der Verbringung und Verarbeitung des sensiblen Materials in die USA aufwirft, nicht beteiligt worden bin, wurde vom BMI auf meine damalige umfangreiche Beteiligung bei der Ausarbeitung des ursprünglichen V ertragswerkes in den

Jahren 1991/92 verwiesen. Dies ist in der Tat zutreffend, doch hätte mich das BMI bei einer so weitreichenden Aktion vorab beteiligen müssen, zumal meine Kontrollfunktion seinerzeit im Vertragstext ausdrücklich festgeschrieben worden war. Diese Passage ist auch heute noch in Kraft. Ich habe gegenüber dem BMI darauf hingewiesen, dass das neue Verfahren eine Anpassung der bestehenden Errichtungsanordnungen (vgl. 18. TB Nr. 11.7) und ggf. auch der „Erkennungsdienstlichen Richtlinien" erforderlich macht. Über die Auswirkungen der neuen Methode auf den Persönlichkeitsschutz werde ich mich in angemessener Zeit nach Aufnahme des Wirkbetriebes unterrichten lassen. Im Übrigen gehe ich davon aus, in wichtigen Angelegenheiten der Informationstechnik in Zukunft durch das BMI/BKA rechtzeitig unterrichtet zu werden.

Beim Verfahren AFIS ist – parallel zur Einführung von Eurodac (vgl. Nr. 7.2.1) – mit weiteren Änderungen zu rechnen. So haben bereits erste Feldversuche mit der so genannten „Livescan"-Technologie im Polizeibereich stattgefunden. Damit werden Fingerabdrucke in Zukunft digital, also nicht mehr mit der – auch den Laien vertrauten – Druckerschwärze aufgenommen und in AFIS eingespielt. Das oben erwähnte „METAMORPHO"-Verfahren wird dabei die Anbindung solcher „Livescan"-Stationen an das weiterhin vom BKA betriebene AFIS ermöglichen. Damit wird langfristig die beim BKA vorgehaltene Sammlung von Fingerabdruckblättern obsolet werden; an ihre Stelle wird eine „papierlose" Sammlung treten.

14 Bundesgrenzschutz

14.1 Datenschutzrechtliche Kontrollen beim BGS – Datenschutz weiterhin verbesserungsbedürftig

Auch im Berichtszeitraum habe ich wieder bei mehreren Bundesgrenzschutzämtern die Datenverarbeitung zu polizeilichen Zwecken sowohl unter rechtlichen als auch unter technisch-organisatorischen Gesichtspunkten einer datenschutzrechtlichen Kontrolle unterzogen. Besonderes Augenmerk habe ich dabei erneut auf die Verarbeitung personenbezogener Daten im Bundesgrenzschutzaktennachweis (BAN) gelegt. Vielfach stellten sich dabei die gleichen Probleme heraus, die ich bereits in früheren Berichten über datenschutzrechtliche Kontrollen angesprochen hatte (s. 18. TB Nr. 12.2).

Nach meinen Feststellungen ist der BAN zum Teil auch zweckentfremdet genutzt worden: Dies betrifft die Erfassung von Personen, für die eine Verpflichtungserklärung nach dem Ausländergesetz (AuslG) abgegeben wurde, sowie von Drittstaatsangehörigen, die vom BGS rückgeführt wurden. In beiden Fällen ist der Nachweis personenbezogener Akten im BAN weder zur Erfüllung der dem BGS obliegenden Aufgaben auf dem Gebiet der Strafverfolgung noch auf dem Gebiet der Gefahrenabwehr gemäß der Zweckbeschreibung der Datei BAN zulässig. Da die Verpflichtung gemäß § 34 Abs. 1 AuslG grundsätzlich gegenüber der Ausländerbehörde zu erklären ist, wird der Bundesgrenzschutz in den Fällen, in denen diese bei der Einreise abgegeben wird, lediglich in Amtshilfe für die zuständige Behörde tätig. Gleiches gilt im Fall der Rückführung von Drittstaatsangehörigen. Gemäß § 63 AuslG sind die Ausländerbehörden generell zuständig für alle aufenthaltsrechtlichen Maßnahmen nach dem Ausländergesetz. Hierzu gehören u. a. die Abschiebung einschließlich deren Vorbereitung und Durchführung. Nur sofern die Ausländerbehörde die Rückführung mit eigenen Mitteln durchführen kann, obliegt diese gem. § 63 Abs. 4 AuslG den Grenzschutzbehörden. Diese werden somit nicht in Erfüllung ihrer polizeilichen Aufgaben nach dem BGS-Gesetz tätig, sondern in Amtshilfe für die jeweilige Ausländerbehörde zur Vollstreckung einer verwaltungsrechtlichen Entscheidung.

Ein weiteres Problem im Zusammenhang mit der Führung des BAN besteht in der Speicherung von Datensätzen, an denen auch Informationen über eine erkennungsdienstliche Behandlung oder eine Haftverbüßung eines Betroffenen hängen. Dies führt auch zu einer Speicherung dieser Daten im polizeilichen Informationssystem INPOL. Obwohl die betreffenden Datensätze im BAN wegen des Ablaufs der nach der Errichtungsanordnung festgelegten Aufbewahrungsfrist hätten gelöscht werden müssen, wurden sie von der betreffenden BGS-Dienststelle mit dem Hinweis auf die für die INPOL-Dateien geltenden längeren Aussonderungsprüffristen weiter vorgehalten. Ich habe die unterbliebene Löschung der Datensätze und Vernichtung der Akten gemäß § 25 BDSG beanstandet. Es ist zutreffend, dass aus systemtechnischen Gründen Informationen über eine erkennungsdienstliche Behandlung oder einen Haftaufenthalt in den hierzu beim BKA geführten INPOL-Dateien abgebildet und gespeichert werden. Die Speicherdauer wird zwar grundsätzlich durch die zulässige Höchstfrist bestimmt. Systemkonventionen zu INPOL ändern jedoch nichts an der datenschutzrechtlichen Verantwortung des Datenbesitzers für die Rechtmäßigkeit der Erhebung und Speicherung dieser Daten sowie für deren Berichtigung bzw. Löschung nach Maßgabe der für ihn geltenden Rechtsvorschriften. So hat der BGS gemäß § 35 Abs. 2 Nr. 2 BGS-Gesetz unter anderem in Dateien gespeicherte personenbezogene Daten zu löschen, sofern deren Kenntnis zur Erfüllung der ihm obliegenden Aufgaben nicht mehr erforderlich ist. Diese Verpflichtung obliegt gemäß § 32 Abs. 9 BKA-Gesetz auch dann dem BGS als Teilnehmer von INPOL, wenn in diesen Datensätzen – wie dargestellt – Informationen über erkennungsdienstliche Behandlungen oder Haftverbüßungen stehen und dies zu einer Speicherung in den entsprechenden INPOL-Dateien führt. Der BGS hat in diesen Fällen das BKA als Zentralstelle des polizeilichen Informationswesens von der Löschung seines Datensatzes zu unterrichten. Es liegt in der Verantwortung des BKA zu entscheiden, inwieweit die erkennungsdienstlichen bzw. Haftdaten zur Aufgabenerfüllung des BKA als Zentralstelle weiterhin gespeichert werden müssen. Ich habe in diesem Zusammenhang angeregt, durch interne Verfahren sicherzustellen, dass in solchen Fällen künftig die Speicherfristen, die vom BGS als Datenbesitzer nach der Errichtungsanordnung des BAN vergeben werden, Beachtung finden. Dies könnte aus meiner Sicht dadurch gewährleistet werden, dass im Rahmen eines Wiedervorlagesystems entsprechend den vergebenen Aussonderungsprüffristen die Akten bei Erreichen der Frist dem zuständigen polizeilichen Bearbeiter zur Entscheidung über die weitere Aufbewahrung bzw. Speicherung in der Datei BAN vorgelegt werden.

Das BMI hat das Ergebnis der datenschutzrechtlichen Kontrollen in den vergangenen Jahren zum Anlass genommen, in mehreren Erlassen gegenüber den Grenzschutzpräsidien darauf zu drängen, die von mir dargelegten Mängel abzu-

stellen und dafür Sorge zu tragen, dass künftig die Regelungen des Datenschutzes stringenter als bisher beachtet werden. Besonders hervorzuheben ist, dass bis zur Änderung der Errichtungsanordnung für den BAN zudem über gangsweise Regelungen erlassen worden sind, die eine datenschutzkonforme Nutzung der Datei gewährleisten sollten. Auch begrüße ich es, dass das BMI in diesem Zusammenhang die Position der behördlichen Beauftragten für den Datenschutz im BGS gestärkt hat, indem es die Grenzschutzpräsidien gebeten hat, für eine kontinuierliche Besetzung dieser Stellen zu sorgen und die behördlichen Datenschutzbeauftragten bei allen Maßnahmen mit datenschutzrechtlichem Bezug mit einzubeziehen.

Im Zusammenhang mit der datenschutzrechtlichen Kontrolle eines Bundesgrenzschutzamtes in Baden-Württemberg habe ich festgestellt, dass auf regionaler Ebene zwischen diesem Amt und der dortigen Landespolizei ein umfassender Informationsaustausch stattfindet. Dieser ist, zumindest was die Datenübermittlung durch BGS-Stellen betrifft, nicht mit den einschlägigen Bestimmungen des Bundesgrenzschutzgesetzes in Einklang zu bringen. Die Dienststellen des Bundesgrenzschutzes erfassen personenbezogene Daten im Rahmen strafrechtlicher Ermittlungsverfahren grundsätzlich im BAN oder, sofern die Voraussetzungen des § 2 Abs. 1 BKA-Gesetz vorliegen, im Kriminalaktennachweis. Gemäß § 32 Abs. 1 BGS-Gesetz kann der Bundesgrenzschutz zudem an Behörden des Polizeivollzugsdienstes personenbezogene Daten übermitteln, soweit dies zur Erfüllung polizeilicher Aufgaben erforderlich ist. Dabei ist in jedem Einzelfall zu prüfen, inwieweit das Erfordernis der Aufgabenerfüllung bei der übermittelnden BGS-Stelle oder bei der Empfängerbehörde erfüllt ist. Die Übermittlung muss darüber hinaus dem Grundsatz der Verhältnismäßigkeit genügen. Bei dem betreffenden Grenzschutzamt wurden jedoch nach meinen Feststellungen alle personenbezogenen Daten Beschuldigter und Verdächtiger aus strafrechtlichen Ermittlungsverfahren unterschiedslos an das Landeskriminalamt Baden-Württemberg übermittelt; und dies in Kenntnis der Tatsache, dass diese Daten dort in der Personenauskunftsdatei der Landespolizei gespeichert werden und somit für sämtliche Polizeidienststellen des Landes abrufbar bereitstehen. Diese Form der Datenübermittlung entspricht nicht dem Gebot der Verhältnismäßigkeit und ist insoweit nicht mit § 32 Abs. 1 BGS-Gesetz vereinbar. Auch der Einwand des betreffenden Bundesgrenzschutzamtes, die Datenübermittlung erfolge ausschließlich für Zwecke der polizeilichen Kriminalstatistik, greift nicht durch. Soweit die Übermittlung personenbezogener Daten für Zwecke der polizeilichen Kriminalstatistik auf der Grundlage von § 30 Abs. 1 BKA-Gesetz erfolgt, hat die Übermittlung der Daten grundsätzlich in anonymisierter Form an das BKA zu erfolgen. Soweit eine Anonymisierung aus technischen Gründen derzeit nicht realisiert und das Verfahren zur Pseudonymisierung der Daten noch nicht eingesetzt werden kann, ist jedenfalls darauf zu achten, dass diese Daten ausschließlich zweckgebunden verarbeitet werden. Das LKA Baden-Württemberg übernimmt in diesen Fällen quasi die Funktion einer „treuhänderischen Datenweitergabe“, da die Statistik durch das BKA erstellt wird. Ich habe die dargestellte Form der unterschiedslosen Datenübermittlung gemäß § 25 Abs. 1 BDSG als einen Verstoß gegen § 32 Abs. 1 BGS-Gesetz beanstandet. Zudem habe ich angeregt, diese Form der Datenübermittlung unverzüglich einzustellen. Soweit personenbezogene Daten für statistische Zwecke über das LKA an das BKA weitergegeben werden, ist das LKA auf die zweckgebundene Nutzung der Daten hinzuweisen. Dabei ist sicherzustellen, dass die Polizeidienststellen des Landes Baden-Württemberg, denen Zugriff auf die Personenauskunftsdatei des LKA gewährt ist, diese Daten nicht mehr zur Kenntnis nehmen können.

Nach Mitteilung des BMI hat das LKA Baden-Württemberg diesem Verfahrensvorschlag vorläufig zugestimmt. Es hält jedoch die Erfassung der von dem betreffenden Bundesgrenzschutzamt übermittelten personenbezogenen Daten als eigene Datensätze der baden- württembergischen Polizei weiterhin für zulässig und beabsichtigt, die Thematik in den Gremien der Ständigen Konferenz der Innenminister und -senatoren der Länder zu behandeln. Sollte danach das LKA Baden-Württemberg zu der ursprünglichen Verfahrensweise zurückkehren und sich nicht an die vorgegebene Zweckbindung halten, wäre im Hinblick auf die datenschutzrechtliche Verantwortung des BGS als übermittelnde Stelle gemäß §§ 32, 33 BGS-Gesetz eine Übermittlung personenbezogener Daten, versehen mit einem Vermerk, dass diese ausschließlich für Zwecke der polizeilichen Kriminalstatistik zu verwenden sind, nicht zulässig.

14.2 Projektgruppe „Mehr Datenschutz“ beim BGS – Auf der Suche nach neuen Datenschutzkonzepten

Die datenschutzrechtlichen Kontrollen mehrerer Grenzschutzämter in den vergangenen Jahren haben gezeigt, dass die dabei festgestellten Mängel strukturell vergleichbare Fragestellungen hinsichtlich der Umsetzung datenschutzrechtlicher Vorgaben für den Geschäftsbereich des BGS insgesamt aufwerfen. Ich habe daher gegenüber dem BMI die Durchführung eines Pilotprojektes angeregt, in dessen Rahmen Wege gesucht werden sollen, datenschutzrechtliche Verfahren bei der polizeilichen Aufgabenwahrnehmung zu optimieren und neue Verfahren zu erproben.

Ich begrüße es, dass das BMI meine Anregung aufgegriffen und im Mai 2002 das Bundesgrenzschutzamt Schwandorf mit der Durchführung eines Pilotprojekts beauftragt hat. Ziel ist es, in einzelnen Teilprojekten der polizeilichen Datenverarbeitung rechtliche und technisch-organisatorische Lösungen zu erarbeiten und diese bei Bedarf auf alle Bundesgrenzschutzämter zu übertragen. Das Pilotprojekt mit der Bezeichnung „Datenschutz und BGS – bessere Lösungen für Grundrechtsschutz“ wird von einer Projektarbeitsgruppe durchgeführt, der neben Mitarbeitern des Bundesgrenzschutzamtes Schwandorf auch Vertreter des Grenzschutzpräsidiums Süd, der Grenzschutzdirektion sowie der Grenzschutzschule Lübeck angehören. Ich nehme in beratender Funktion an den Erörterungen der Arbeitsgruppe teil.

Als erstes Teilprojekt befasst sich die Projektgruppe mit der Neukonzeption des Bundesgrenzschutzaktennachweises (BAN). Dabei wird auf der Grundlage der derzeitigen Datenverarbeitungs- und Nutzungsmöglichkeiten im BAN ein Modell entwickelt, das sowohl den polizeilichen als auch den datenschutzrechtlichen Anforderungen Rechnung tragen soll. Die Arbeiten an dem Konzept waren bei Redaktionsschluss noch nicht abgeschlossen.

Von der Arbeit der Projektgruppe verspreche ich mir wichtige Impulse für eine stetige Verbesserung der datenschutzrechtlichen Rahmenbedingungen im Zusammenhang mit

der polizeilichen Aufgabenwahrnehmung durch die Dienststellen des BGS. Auch in den kommenden Jahren werde ich die Mitglieder der Projektgruppe bei der Erörterung datenschutzrechtlicher Aspekte der polizeilichen Datenverarbeitung beratend unterstützen.

14.3 Gemeinsames Zentrum der deutsch-französischen Polizei- und Zollzusammenarbeit in den Grenzgebieten

Im Februar 2002 habe ich im Gemeinsamen Zentrum der deutsch-französischen Polizei- und Zollzusammenarbeit in Offenburg einen Beratungs- und Kontrollbesuch durchgeführt. Gegenstand des Besuchs war die polizeiliche Datenverarbeitung im Gemeinsamen Zentrum, soweit Bundesstellen daran beteiligt sind.

Die Tätigkeit des Gemeinsamen Zentrums beruht auf dem Abkommen vom 9. Oktober 1997 zwischen Deutschland und Frankreich über die Zusammenarbeit der Polizei- und Zollbehörden in den Grenzgebieten (Mondorfer Abkommen). Ziel des Abkommens ist es, die Zusammenarbeit der Behörden mit polizeilichen und zollrechtlichen Aufgaben bei der Gefahrenabwehr sowie der Verhütung und Verfolgung von Straftaten auszubauen. Dem seit drei Jahren bestehenden Gemeinsamen Zentrum kommt in diesem Zusammenhang eine Schlüsselrolle zu. In ihm arbeiten Angehörige der Polizeien und der Zollverwaltung Deutschlands und Frankreichs räumlich unmittelbar zusammen, um in Angelegenheiten, die die Grenzgebiete betreffen, Informationen auszutauschen, zu analysieren und weiter zu steuern. Dem Gemeinsamen Zentrum gehören für die deutsche Seite Vertreter des Bundesgrenzschutzes, des Zolls sowie der Landeskriminalämter von Baden-Württemberg und Rheinland-Pfalz an. Deutsche, das französische Grenzgebiet betreffende Informationsersuchen werden dabei von französischen Bediensteten des Gemeinsamen Zentrums bearbeitet; französische Ersuchen entsprechend von deutschen Bediensteten. Hierzu greifen die Bediensteten auf die jeweils eigenen nationalen Polizei- bzw. Zollinformationssysteme zurück. Die Informationsvermittlung wird in einem Tagebuch nachgewiesen. Dabei werden personenbezogene Daten verarbeitet. Das Tagebuch enthält unter anderem Angaben über den Grund des Ersuchens sowie – in Stichworten – darüber, welches Ergebnis an die ersuchende Stelle übermittelt wurde. Die angelegten Tagebuchblätter werden elektronisch in der automatisierten Datei „Tagebuch“ gespeichert und sind dort von jedem Bediensteten des Gemeinsamen Zentrums abrufbar. Die Tagebucheintragungen in der Datei werden automatisch zwei Jahre nach Aufnahme des Ersuchens gelöscht sowie das Tagebuchblatt vernichtet. Zum Zeitpunkt meines Kontrollbesuchs waren in der Datei ca. 8 000 Datensätze gespeichert. Nach Angaben der Bediensteten des Gemeinsamen Zentrums wird das „Elektronische Tagebuch“ nicht nur zur Vorgangsverwaltung bzw. zu befristeten Dokumentationszwecken geführt. Die darin gespeicherten personenbezogenen Daten werden vielmehr auch zur Erfüllung weiterer polizeilicher Aufgaben im Zusammenhang mit der Gefahrenabwehr sowie der Verhütung und Verfolgung von Straftaten in den Grenzgebieten genutzt.

Ich habe gegen den Betrieb einer gemeinsamen Datei „Elektronisches Tagebuch“ keine Einwände. Es müssen jedoch die datenschutzrechtlichen Voraussetzungen hierfür geschaffen werden. Dies ist bislang nicht der Fall. Da das Mondorfer Abkommen das Führen einer gemeinsamen polizeilichen Datei durch die in das Gemeinsame Zentrum entsandten Behördenvertreter nicht regelt, kommen als Rechtsgrundlage hierfür – soweit der BGS und der Zoll sich daran beteiligen – die einschlägigen Regelungen des Bundesgrenzschutz-Neuregelungsgesetzes sowie des Zollfahndungsdienstgesetzes in Betracht. Danach ist für jede Datei, die für die Erfüllung polizeilicher Aufgaben genutzt wird, zwingend eine Errichtungsanordnung zu erstellen, in der unter anderem auch die Speicherfristen für die darin eingestellten Datensätze bestimmt werden müssen.

Datenschutzrechtlich problematisch ist zudem die nicht konsequent durchgeführte Trennung von polizeilichen und zollrechtlichen Vorgängen im Gemeinsamen Zentrum. Im Hinblick auf die gem. § 30 der Abgabenordnung (AO) gebotene Wahrung des Steuergeheimnisses müssen Informationsvorgänge, die zollrechtliche Angelegenheiten betreffen, getrennt von Vorgängen aufbewahrt werden, die sich auf polizeiliche Angelegenheiten beziehen. Zwar werden Informationsersuchen, die Angelegenheiten des Zolls betreffen, ausschließlich von deutschen bzw. von französischen Zollbeamten im Gemeinsamen Zentrum bearbeitet. Auch werden die von den deutschen und französischen Zollbediensteten angelegten Tagebuchblätter sowie die übrigen, bei der Erarbeitung von Informationsersuchen anfallenden Unterlagen getrennt von den übrigen polizeilichen Unterlagen geführt und sind nur für Zollbedienstete zugänglich. Gleichwohl werden diese Tagebuchblätter aber zusammen mit den polizeilichen Vorgängen in der gemeinsam betriebenen Datei „Elektronisches Tagebuch“ abgebildet und sind dort für alle Bediensteten des Gemeinsamen Zentrums zugänglich. Ich bin mir mit dem Bundesministerium der Finanzen darin einig, dass dies mit den gesetzlichen Anforderungen des § 30 AO nicht im Einklang steht. Der getrennten Aktenablage folgend halte ich es daher für geboten, auch jeweils für Polizei- und Zollangelegenheiten getrennte Dateien anzulegen, auf die jeweils nur die zuständigen deutschen bzw. französischen Behördenvertreter Zugriff haben.

Das Gemeinsame Zentrum der deutsch-französischen Polizei- und Zollzusammenarbeit leistet nach meinem Eindruck einen wichtigen Beitrag für eine intensive Zusammenarbeit der Polizei- und Zollbehörden beider Länder unterhalb der Kooperationsebene nach dem Schengener Durchführungsübereinkommen, in dem Informationsersuchen der einen und der anderen Seite schneller und effektiver vermittelt werden können. Zweifellos führt dies zu einer Verbesserung der Maßnahmen bei der Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung sowie bei der Verhütung und Verfolgung von Straftaten in den Grenzgebieten. Zugleich ist es aber unabdingbar, auch die datenschutzrechtlichen Rahmenbedingungen für die Tätigkeit des Gemeinsamen Zentrums zu regeln und seinen Mitarbeitern hierfür die notwendige Unterstützung zu gewähren. Dies gilt vor allem dann, wenn im Gemeinsamen Zentrum neben der eigentlichen Informationsvermittlung zwischen verschiedenen deutschen und französischen Dienststellen auch eine eigenständige personenbezogene Datenverarbeitung mittels eines lokalen Netzwerkes betrieben werden soll. Eine klare Regelung der datenschutzrechtlichen Aspekte der Tätigkeit des Gemeinsamen Zentrums ist auch im Hinblick darauf wichtig, dass dies Modellcharakter für andere geplante bzw. bereits realisierte Zentren bilateraler Polizei- und Zollkoo-

perationen im deutschen Grenzgebiet hat. Umso bedauerlicher ist es, dass mir bis jetzt weder der Entwurf einer Errichtungsanordnung für die Datei „Elektronisches T agebuch" vorgelegt werden konnte, noch Lösungsvorschläge unterbreitet wurden, wie den gesetzlichen Anforderungen zur Wahrung des Steuergeheimnisses nach Maßgabe des § 30 AO Rechnung getragen werden soll.

15 Zollfahndung

15.1 Zollfahndungsneuregelungsgesetz verabschiedet – Konsequenzen für die Steuerfahndung?

Am 24. August 2002 ist das Gesetz zur Neuregelung des Zollfahndungsdienstes, dessen Schwerpunkt das Gesetz über das Zollkriminalamt (ZKA) und die Zollfahndungsämter bildet, in Kraft getreten (BGBl. 2002 I S. 3202). Neben der Regelung von Aufgaben und Befugnissen des ZKA und der Zollfahndungsämter wurden mit dem Gesetz die für die Tätigkeit dieser Behörden erforderlichen bereichsspezifischen Datenschutzbestimmungen geschaffen. Die Bundesregierung setzt damit auch für den Bereich dieser Bundespolizei die V orgaben des V olkszählungsurteils für eine verfassungskonforme Ausgestaltung des Rechts auf informationelle Selbstbestimmung um. Sie kommt damit einer entsprechenden Forderung des Deutschen Bundestages nach (vgl. 18. TB Nr. 13.1).

Die Bestimmungen des Gesetzes orientieren sich an den Befugnisregelungen für das Bundeskriminalamt nach dem Bundeskriminalamtgesetz (BKA-Gesetz) sowie für den Bundesgrenzschutz nach dem Bundesgrenzschutzneuregelungsgesetz (BGS-Gesetz). So nimmt das ZKA unter anderem die Aufgabe einer Zentralstelle innerhalb des Zollfahndungsdienstes wahr und führt in dieser Funktion ein Zollfahndungsinformationssystem. Dem Zollkriminalamt sowie den Zollfahndungsämtern werden darüber hina us umfangreiche Befugnisse zu besonderen Datenerhebungen eingeräumt.

An der Ausarbeitung des Gesetzentwurfs war ich von Beginn an beteiligt. Im Mittel punkt standen dabei insbesondere die Datenerhebungs- und V erarbeitungsbefugnisse für das ZKA und die Zollfahndungsämter. Im Laufe der Erörterungen konnte unter anderem erreicht werden, dass die Anforderungen für eine Datenerhebung mit besonderen Mitteln verschärft wurden. Sie sind nunmehr nur zulässig zur V erhütung von Straftaten von erheblicher Bedeutung, soweit Anhaltspunkte für eine gewe rbs-, gewohnheits- oder bandenmäßige Begehungsweise vorliegen. Zudem sind die Befugnisse des ZKA bei Sicherungs- und Zeugenschutzmaßnahmen konkreter gefasst worden.

Für problematisch halte ich die dem ZKA eingeräumte Befugnis, personenbezogene Daten aus der Beobachtung bestimmter Verkehre (Waren, Kapital, Dienstleistungen) und aus der Marktbeobachtung auch zur Erfüllung seiner übrigen Aufgaben zu nutzen. Für ebenso problematisch halte ich die Möglichkeit, personenbezogene Daten im Zusammenhang mit der Verfolgung von Ordnungswidrigkeiten längere Zeit zu speichern. V ergleichbare Regelungen finden sich weder im BKA- noch im BGS-Gesetz. Das BMF hat hierzu auf das vielschichtige Aufgabenspektrum des ZKA hingewiesen: Die Verhütung und Verfolgung von Straftaten und Ordnungswidrigkeiten, die Aufdeckung unbekannter Straftaten und die Durchführung unabhängiger Marktbeobachtungen im Einzelfall. Der V erhütung und Verfolgung von Ordnungswidrigkeiten im Zuständigkeitsbereich der Zollverwaltung käme zudem besondere Bedeutung zu, vor allem im Hinblick auf Häufigkeit und Ahndung mit Geldbußen von zum Teil erheblicher Höhe.

Vor diesem Hintergrund habe ich meine Bedenken gegen das Gesetzesvorhaben zurückgestellt. Die Praxis muss zeigen, inwieweit bei der Ausübung dieser Befugnisse durch die Dienststellen der Zollfahndung dem Grundsatz der V erhältnismäßigkeit Rechnung getragen wird. Ich habe angeregt, zumindest die Aussonderungsprüf fristen für gespeicherte personenbezogene Da ten aus Ordnungswidrigkeiten entsprechend deren Unwertgehalt unterschiedlich festzulegen.

Insgesamt begrüße ich die gesetzliche Regelung der Aufgaben und Befugnisse im Bereic h der Zollfahndung als zwingende Konsequenz des V olkszählungsurteils. Hierdurch ist eine nicht länger hinnehmbare Rechtslücke geschlossen worden. Für den Bürger ist nunmehr klarer erkennbar, unter welchen Voraussetzungen und in welchem Umfang er Einschränkungen seines Rechts auf informationelle Selbstbestimmung durch den Zollfahndungsdienst hinnehmen muss. Zudem wird die datenschutzrechtliche Beratung und Kontrolle dieser Bundesverwaltung auf eine tragfähige Grundlage gestellt.

Im Zusammenhang mit der V orbereitung des Zollfahndungsneuregelungsgesetzes und im Hinblick auf die Rechtsprechung des Bundesfinanzhofs zu einzelnen Maßnahmen im Rahmen der Steuerfahndung habe ich gegenüber dem BMF die Frage aufgeworfen, ob nicht auch für die Steuerfahndung, deren Maßnahmen mit massiven Eingrif fen für den Betroffenen bereits im V orfeld eines Anfangverdachts verbunden sein können, eine bereichsspezifische Rechtsgrundlage anstelle der Generalklauseln nach der Abgabenordnung erforderlich ist. Das BMF hat mir signalisiert, dass mögliche zusätzliche gesetzliche Regelungen zur Definition der Aufgaben und Befugnisse der Steuerfahndung im V orfeld eines steuerstrafrechtlichen Anfangsverdachts und zur vorbeugenden Bekämpfung von Steuerdelikten in einer Bund/Länder-Arbeitsgruppe auch unter Datenschutzgesichtspunkten behandelt werden. Darüber hinaus wurde mir in Aussicht gestellt, mich über das Er gebnis der Arbeitsgruppe zu unterrichten. Bis Redaktionsschluss dieses Tätigkeitsberichts habe ich leider noch keine weitere Antwort vom BMF erhalten. Ich halte die Angelegenheit weiterhin für regelungsbedürftig.

15.2 Bargeldkontrollen an den Grenzen

Im Berichtszeitraum haben sich erneut Bürger, die sich durch Bargeldkontrollen an den Grenzübergängen (s. 18. TB Nr. 13.5) oder in Zügen der Deutschen Bahn AG in ihrem Persönlichkeitsrecht beeinträchtigt fühlten, mit der Bitte um Überprüfung an mich gewandt. Dies, obwohl das BMF durch mehrere Erlasse die Befugnisse der zuständigen Zollbehörden bei der Durchführung solcher Kontrollen auch bezüglich der Weitergabe der dabei gewonnenen Erkenntnisse, insbesondere an die Steuerbehörden, klargestellt hat. Danach dürfen die Bediensteten des Zolls Reisende in vermeintliche Steueroasen nicht von vornherein einem Generalverdacht und entsprechenden Maßnahmen – ungeachtet des V erhältnismäßigkeitsprinzips – aussetzen. Reisende müssen aber auf

Verlangen von Zoll- oder BGS-Bediensteten mitgeführte Zahlungsmittel ab 15 000 Euro anzeigen.

Die einschlägigen Aufgaben und Befugnisse der Zollbehörden wie auch des BGS zur Überwachung des grenzüberschreitenden Bargeldverkehrs, die bis dato in §§ 12a bis d Finanzverwaltungsgesetz geregelt waren, sind durch Artikel 1 Nr. 15 des Gesetzes zu r Änderung des Finanzverwaltungsgesetzes und anderer Gesetze vom 14. Dezember 2001 (BGBl. I S. 3714 f.) aufgehoben und zugleich durch Artikel 7 Nr. 1 und 2 des selben Gesetzes als §§ 3a bis c (für die Aufgaben) und §§ 12a bis c (für die Befugnisse) in das Zollverwaltungsgesetz (ZVG) integriert worden. Primäre Aufgabe der Grenzbeamten ist nach dem Gesetz weiterhin die Bekämpfung der Geldwäsche durch Aufspüren von Gewinnen aus schweren Straftaten und damit zusammenhängend die Bekämpfung der or ganisierten Kriminalität durch zollamtliche Überwachung des grenzüberschreitenden Verkehrs, auch an den Grenzen innerhalb der Gemeinschaft. Die Übermittlung personenbezogener Daten an andere Finanzbehörden ist zulässig, soweit ihre Kenntnis zur Durchführung eines Verwaltungsverfahrens in Steuersachen oder eines Strafverfahrens wege n einer Steuerstraftat oder eines Bußgeldverfahrens von Bedeutung sein kann. Eine Ausdehnung der Untersuchung auf andere Unterlagen, z. B. auf Bankunterlagen, ist auf der Grundlage des § 12a ZVG nicht zulässig. Es ist zu hof fen, dass sich das Kontrollverhalten an den Grenzen mit der Diskussion um die Einführung einer Abgeltungsteuer entspannen wird und damit auch die Eingriffe in Grundrechts positionen der Reisenden abnehmen werden.

15.3 Dateibank „ZAUBER“ beim Bundesamt für Finanzen

Im Jahre 2002 habe ich der Pr esse entnommen, dass beim Bundesamt für Finanzen eine neue Datenbank unter der Bezeichnung „ZAUBER“ (**Z**entrale Datenbank zur Speicherung und **A**uswertung von **U**msatzsteuer-**B**etrugsfällen und **E**ntwicklung von **R**isikoprofilen) geführt wird. Ich habe daraufhin das BMF um Auskunft und Abdruck einer V erfahrensbeschreibung gem. § 4e BDSG gebeten. Nach wiederholten Erinnerungen und einer daraufhin erfolgten Beanstandung meinerseits wegen V erletzung der Mitwirkungspflicht (vgl. § 25 BDSG i. V. m. § 24 Abs. 4 BDSG) hat mir das Ministerium den Betrieb einer solchen Datenbank bestätigt, die seit Januar 2001 existiere. Ziel dieser Anwendung ist insbesondere die Bekämpfung des Umsatzsteuerbetrugs, z. B. durch Geltendmachung unberechtigter Vorsteuererstattung. In der Datenbank werden auch Betrugsfälle über aufgedeckte Schei nunternehmen, umsatzsteuerliche Hinterziehungsfälle nach § 370 Abgabenordnung (AO) sowie Erwerbsfälle von Kfz au s dem Ausland oberhalb einer bestimmten Kaufsumme erfasst. Es werden darüber hinaus Fälle mit einem umsatzsteuerlichen Mehrer gebnis ab 125 000 Euro aufwärts aus steuerlichen Prüfungen usw. gesammelt.

Dem Verfahren nach handelt es sich um eine Art V erbunddatei, in die Daten durch di e zuständigen Finanzbehörden der Länder eingestellt und abgerufen werden. Bezüglich der Daten über umsatzsteuerliche Mehrergebnisse sei die Abfrageberechtigung jedoch auf die Bediensteten der Steuerfahndung beschränkt. Im Übrigen sei die Einrichtung einer Datei über strafrechtliche Vorermittlungen von den Finanzbehörden derzeit nicht geplant.

Ungeachtet der Stellungnahme des BMF habe ich weiterhin Zweifel an der Zulässigkeit der Datei. Dies gilt u. a. für die angeführte Rechtsgrundlage des § 88a AO, soweit dort auch Ergebnisse strafrechtlicher Ermittlungen Eingang finden. Ich habe ferner die Frage aufgeworfen, in welchem Verhältnis der strafrechtliche Datenteil dieser Datenbank zum länderübergreifenden Zentralen Staatsanwaltschaftlichen Verfahrensregister nach §§ 492 f. der Strafprozessordnung steht. Darüber hinaus bleibt zu klären, wie mit Daten aus eingestellten Strafverfahren umgegangen wird; denn in der Verfahrensbeschreibung nach § 4e BDSG ist eine allgemeine Höchstspeicherfrist von zehn Jahren vor gesehen. Diese lange Speicherdauer erscheint mir im Hinblick auf das Erforderlichkeitsprinzip bedenklich. Ich finde es im übrigen unverhältnismäßig, alle Mehrer gebnisse aus Umsatzsteuerprüfungen über 125 000 Euro in die Datei einzustellen, auch wenn keinerlei Anhaltspunkte für Umsatzsteuermanipulationen vorhanden sind. Bei Redaktionsschluss war der Meinungsaustausch mit dem BMF noch nicht abgeschlossen. Eine Prüfung de r Datei beim Bundesamt für Finanzen habe ich eingeplant.

16 Wachsende polizeiliche Zusammenarbeit in Europa

16.1 Europol

Die gemeinsame Kontrollinstanz von Europol (vgl. 18. TB Nr. 11.11) hat im Berichtszeitraum ca. zehn Sitzungen abgehalten. Sie wird ihre Aktivitäten in einem Tätigkeitsbericht dokumentieren, der Anfang 2003 erscheinen soll. Einen Schwerpunkt ihrer beratenden Tätigkeit bildeten die V erhandlungen über den Abschluss eines Zusatzabkommens zwischen Europol und den USA über den Austausch personenbezogener Daten im Anschluss an die Ereignisse vom 11. September 2001. Der V ertrag, der am 20. Dezember 2002 unterzeichnet wurde, ergänzt das Abkommen über den Austausch strategischer Informationen vom 6. Dezember 2001. So dringlich dieser V ertrag über die polizeiliche Zusammenarbeit der Partner war , ergaben sich aus datenschutzrechtlicher Sicht doch erhebliche Hindernisse. Diese leiteten sich aus dem Recht auf den Schutz des Persönlichkeitsrechts des Einzelnen ab, das in den USA mangels gesetzlicher Regelungen kaum de n europäischen Maßstäben entspricht, wie sie insbesondere in der Europaratskonvention 108 nieder gelegt sind. Die gemeinsame Kontrollinstanz, die durch zwei V ertreter an den V ertragsverhandlungen beteiligt war , hat deshalb auf der vertraglichen Fixierung datenschutzrechtlicher Grundsätze bestanden. Dazu zählen insbesondere das Zweckbindungsprinzip, die Weiterübermittlung der empfangenen Daten seitens der Vertragsparteien an Drittstaaten/Drittstellen nur mit schriftlicher Einwilligung sowie die V erpflichtung zur Datenlöschung, wenn die Daten nicht mehr erforderlich sind. Ferner dürften die Regelungen mit den USA keine präjudizierende Wirkung auf ähnliche Abkommen von Europol mit anderen Drittstaaten entfalten. Der Vollzug des Abkommens bedürfe darüber hinaus einer fortdauernden Überwachung. Die Vertragsparteien haben sich zudem verpflichtet, das Abkommen zwei Jahre nach seinem In-Kraft-Treten einer Evaluation zu unterziehen.

Der Beschwerdeausschuss (vgl. 17. TB Nr. 11.3, 18. TB Nr. 11.11) hatte sich im Berichtszeitraum erstmals mit zwei Beschwerden Betroffener auseinander zu setzen, von denen ein Verfahren zum Abschluss gebracht worden ist. Auch hierzu wird in dem o. g. Bericht Stellung bezogen. Schon jetzt lässt sich feststellen, dass die eingeleiteten Verfahren, auch im Hinblick auf die Beteiligung der Beschwerdeführer, recht schwerfällig verlaufen. Der Ausschuss hat deshalb mit der Beratung interner Richtlinien begonnen, die das Beschwerdeverfahren unter Wahrung der Rechte der Beteiligten effizienter gestalten sollen.

Drei Jahre nach Aufnahme des Wirkbetriebs bei Europol am 1. Juli 1999 zeichnet sich im Rat der Wunsch nach einer Änderung des Europol-Übereinkommens vom 26. Juli 1995 ab. Dies fand Eingang in eine Initiative des Königreichs Dänemark für einen Rechtsakt des Rates zur Erstellung eines Protokoll zur Änderung des Europol-Übereinkommens. Der Entwurf enthält zahlreiche Änderungen des Vertrages, beginnend mit einer erweiterten Zielbeschreibung von Europol (Artikel 2) bis zu einer Zusammenarbeitsregelung mit Eurojust (Artikel 42). Etliche dieser Vorschläge sind auch von datenschutzrechtlicher Relevanz. Die gemeinsame Kontrollinstanz hat am 3. Oktober 2002 eine umfassende Stellungnahme zu der dänischen Initiative abgegeben, die sowohl dem Rat als auch dem Europäischen Parlament zugänglich gemacht wurde. Unbeschadet dieser Stellungnahme, auf die im Tätigkeitsbericht der gemeinsamen Kontrollinstanz eingegangen wird, habe ich mich gegenüber der Bundesregierung ebenfalls zu dem Entwurf einer Stellungnahme der deutschen Delegation in den Ratsgremien geäußert. Dabei habe ich darauf hingewiesen, dass es bei der Fortschreibung des Europol-Übereinkommens nicht nur um die Interessen Europols und der Mitgliedsstaaten, ein effizientes Europäisches Polizeiamt und eine verbesserte Kooperation mit den Mitgliedsstaaten zu schaffen, sondern auch um den Schutz des Persönlichkeitsrechts der Betroffenen geht. Die Initiative enthält jedoch auch Vorschläge, die aus datenschutzrechtlicher Sicht zu begrüßen sind. Dazu zählen eine Änderung des Verfahrens bei der Protokollierung von Abrufen zum Zweck einer besseren Kontrolle der Zugriffe auf das Europol-Informationssystem, des Weiteren die Anwendung der datenschutzrechtlichen Grundsätze auf die Informationsverarbeitung, auch soweit diese in Akten erfolgt. Hingegen sind aus datenschutzrechtlicher Sicht erweiterte Zugriffsrechte auf die in Artikel 10 geregelten vertraulichen Analysedateien bei Europol kritisch zu sehen. Bei Redaktionsschluss hatte der Rat noch keine abschließende Entscheidung über die dänische Initiative getroffen. Auch die Stellungnahme des Europäischen Parlaments zu dem Projekt lag zu diesem Zeitpunkt noch nicht vor.

16.2 Schengen

16.2.1 SIS II

Bereits in meinem 18. TB (Nr. 11.10.1) habe ich über Pläne zur Fortentwicklung des Schengener Informationssystems (SIS) berichtet. Hierfür gibt es mehrere Gründe. Zum einen stößt das bestehende SIS nach dem Beitritt der skandinavischen EU-Mitgliedsstaaten und der Assoziierung von Norwegen und Island im Berichtszeitraum an seine Kapazitätsgrenzen; es bedarf also einer Lösung, sobald die MOE-Staaten sowie Zypern der Gemeinschaft beitreten und am Schengener Besitzstand teilnehmen. Dabei könnte auch die jüngste Entwicklung im Bereich der Informationstechnologie zur Umrüstung genutzt werden; denn immerhin beruht die Systemarchitektur des aktuellen SIS weitgehend auf der IuK-Technik des Standes vor etwa 15 Jahren.

Auf der anderen Seite gibt es vermehrt Wünsche der Anwender in Bezug auf neue Funktionalitäten des Systems. Dabei geht es um eine Erweiterung des Kreises zugriffsberechtigter Behörden (u. a. Europol) auf bestimmte SIS-Daten. Auch soll der Umfang der in das System einzugebenden Datenkategorien ergänzt werden. Langfristig streben die EU-Mitgliedsstaaten auf diese Weise eine Änderung des SIS von einer herkömmlichen polizeilichen Ausschreibungsdatei mit ausländerrechtlichen Elementen zu einem umfassenden polizeilichen Informationssystem an, auf das ggf. auch die Justiz und andere Behörden Zugriff erhalten sollen. Zudem ist im Aktionsplan der EU vom 21. September 2001 über die Terrorismusbekämpfung darauf hingewiesen worden, dass das SIS ausgebaut werden müsse.

Vor diesem Hintergrund sind unter spanischem EU-Vorsitz zwei Rechtsakte zur Änderung des Schengener Durchführungsübereinkommens (SDÜ) auf den Weg gebracht worden, der Entwurf eines Beschlusses und der Entwurf einer Verordnung zur Änderung des SDÜ. Der Grund für die Zweiteilung dieser Vorschläge, die teilweise parallele Regelungen enthalten, liegt in der Doppelfunktion des SIS. Dieses dient mit seinen Informationen einerseits der öffentlichen Sicherheit und Ordnung einschließlich der Sicherheit des Staates, andererseits soll es die Freiheit des Personenverkehrs innerhalb der Gemeinschaft gewährleisten. Es beruht also auf dem ersten und dem dritten Pfeiler der Union.

Die gemeinsame Kontrollinstanz von Schengen hat sich in einer von mir miterarbeiteten Stellungnahme teils kritisch zu den Änderungsvorschlägen geäußert. Diese Stellungnahme findet sich im nächsten Tätigkeitsbericht der gemeinsamen Kontrollinstanz.

Darüber hinaus habe ich mich gegenüber dem BMI zur Vorbereitung der Stellungnahme der deutschen Delegation in den Ratsgremien bezüglich der spanischen Initiativen wie folgt geäußert:

Zunächst habe ich den Sinn der Vorschläge im Hinblick auf die zeitlich noch ungewisse Erweiterung des aktuellen SIS I + zu einem künftigen SIS II infrage gestellt, zumal mir der Zusammenhang mit der Terrorismusbekämpfung eher vage erscheint. Auch ist es unter datenschutzrechtlichen Gesichtspunkten bedenklich, bereits jetzt über erweiterte Zugriffsberechtigungen und neue Funktionalitäten zu entscheiden, ohne dass nähere Festlegungen bezüglich der in das SIS einzustellenden Datenkategorien getroffen werden. Insbesondere habe ich Sorge, dass das SIS von einer polizeilichen Ausschreibungsdatei sukzessive zu einem umfassenden Informationssystem nicht nur für die Polizei, sondern auch für andere Behörden ausgebaut werden soll.

Im Rahmen der Vorschläge ist auch ein Zugriff von Europol und der nationalen Mitglieder von Eurojust auf bestimmte Ausschreibungskategorien im SIS vor gesehen. Solange jedoch Europol keine operativen Befugnisse erhält, ist aus datenschutzrechtlicher Sicht eine Erforderlichkeit des Zugriffs nicht ersichtlich. Dasselbe gilt für die nationalen Vertreter von Eurojust, solange deren Aufgaben nicht definitiv festgelegt sind. Bedenklich erscheint mir ferner, dass für Ausschreibungen zur verdeckten Registrierung nach Artikel 99 Abs. 3 SDÜ, die auf Veranlassung von Nachrichtendiensten

erfolgen, von der bisherigen Vorabkonsultation der anderen Vertragsparteien durch das ausschreibende Land abgesehen werden soll. Statt dessen ist nur noch eine Unterrichtung über solche sensiblen Maßnahmen vorgesehen.

Die Rechtsaktentwürfe enthalten jedoch auch aus datenschutzrechtlicher Sicht begrüßenswerte Vorschläge. So soll in Zukunft jede Übermittlung aus dem SIS zur Kontrolle der Zulässigkeit des Abrufs protokolliert werden. Bisher war nur eine Protokollierung von durchschnittlich jedem zehnten Abruf obligatorisch. Zudem wird eine normenklare Rechtsgrundlage für die Aktivitäten der nationalen SIRENE-Büros geschaffen. Beide Vorschläge entsprechen Forderungen der gemeinsamen Kontrollinstanz, die diese schon vor Jahren erhoben hat. Bei Redaktionsschluss war in den Ratsgremien und beim Europäischen Parlament über die Initiativen Spaniens noch nicht entschieden.

16.2.2 Neues Verfahren bei missbräuchlich verwendeter Identität bringt keine substanziellen Verbesserungen, dafür aber ein Mehr an zusätzlichen Daten

Weiterhin habe ich in meinem 18. TB unter Nr. 11.10.3 über eine datenschutzrechtlich bedenkliche Praxis in Fällen berichtet, in denen eine im SIS ausgeschriebene Person die Identität einer dritten unbescholtenen Person benutzt. Zu Problemen kann es für die unbescholtene Person dann kommen, wenn bei einer Personenkontrolle an der Grenze oder bei der Beantragung eines Visums festgestellt wird, dass deren Personalien als Alias-Personalien dem Datensatz einer anderen Person zugespeichert werden, die im SIS ausgeschrieben ist und sich durch Vorlage eines in Verlust geratenen oder gestohlenen Ausweispapiers der Identität der unbescholtenen Person bedient. In einem solchen „Trefferfall" hat die unbescholtene Person nachzuweisen, dass sie nicht mit der ausgeschriebenen Person identisch ist. Dies ist in der Regel mit Unannehmlichkeiten und mit zeitintensiven Identitätsfeststellungen verbunden.

Zur Lösung des Problems hatte das BKA bis Mitte des Jahres 2001 dem Betroffenen nach dessen erkennungsdienstlicher Behandlung eine so genannte Identitätsbescheinigung ausgestellt, mit der er seine wahre Identität im Falle einer polizeilichen Kontrolle nachweisen konnte. Gegen dieses Verfahren hatte ich trotz datenschutzrechtlicher Bedenken letztlich keine Einwendungen erhoben, da ich hierin eine Möglichkeit sah, die geschädigte Person möglichst zeitnah zu erkennen und deren Beeinträchtigungen so gering wie möglich zu halten.

Im Zusammenhang mit der Eingabe eines Petenten erlangte ich davon Kenntnis, dass seit 12. Juli 2001 ein mit allen Schengen-Vertragsstaaten abgestimmtes neues Verfahren praktiziert wird. Seither ist es möglich, bei Datensätzen, die nachweislich auf der missbräuchlichen Verwendung fremder Personalien beruhen, im SIS-Datensatz einen standardisierten Hinweis „Achtung: Diese Personalien, die einer existenten Person gehören, werden von der gesuchten Person vermutlich missbräuchlich verwendet. Zusatzinformationen liegen beim nationalen SIRENE-Büro vor" anzubringen. Ein solcher Hinweis wird jedoch erst dann angebracht, wenn zuvor eine Identitätskontrolle durch Vergleich von erkennungsdienstlichem Material – in der Regel Fingerabdrücken – durchgeführt wurde und zusätzliche personenbezogene Daten beim Betroffenen – bis hin zur Angabe der Namen der Eltern – erhoben wurden. Diese Angaben werden in ein so genanntes Q-Formular eingestellt, das an alle Schengen-Mitgliedsstaaten versandt wird. Der Betroffene wird auf die Freiwilligkeit seiner Angaben hingewiesen und hat zudem eine Einverständniserklärung abzugeben, dass die freiwillig abgenommenen Fingerabdrücke zu Vergleichszwecken im nationalen SIRENE-Büro beim BKA aufbewahrt werden dürfen. Vor der Aufnahme eines solchen Hinweises im SIS ist jedoch zu prüfen, ob die Fahndung als solche oder zumindest der den Geschädigten belastende Alias-Datensatz gelöscht werden kann.

Das Verfahren basiert auf Entscheidungen der zuständigen EU-Ratsgremien, die die Grundsätze für das Verfahren festgelegt haben. Damit verbunden war – so das BMI – die Absicht, die gemeinsame Kontrollinstanz von Schengen (GKI) über diese neue Übergangslösung zu unterrichten. Eine Beteiligung der GKI – wie auch eine Beteiligung meiner Behörde im nationalen Verfahren – ist jedoch bislang nicht erfolgt. Das BMI hat zugesagt, den Vorsitz der Ratsarbeitsgruppe SIS auf die Unterrichtung der GKI hinzuweisen. Die GKI hat sich in der Vergangenheit mehrfach mit dieser Problematik befasst und dabei eine gemeinsame Lösung bis zur Inbetriebnahme des SIS II gefordert. Eine nachträgliche Unterrichtung über ein bereits seit fast zwei Jahren praktiziertes schengenweit einheitliches Verfahren ist jedoch von einer gemeinsamen Lösung weit entfernt.

Ich verkenne zwar nicht die Verbesserungen, die das neue Verfahren in technischer und verwaltungsmäßiger Hinsicht gebracht hat, sehe jedoch in der neuen Regelung keine substanzielle datenschutzrechtliche Verbesserung. So werden für das so genannte Q-Formular zahlreiche Zusatzinformationen – wenn auch auf freiwilliger Basis – erhoben, von denen nach meiner Auffassung nicht jede im konkreten Einzelfall erforderlich ist. Die für das Formular zu erhebenden Daten müssen sich am jeweiligen Einzelfall orientieren. Nicht in jedem Falle sind z. B. die Namen der Eltern des Betroffenen zur Identitätsfeststellung erforderlich. Ferner sollten – stärker als dies in der Vergangenheit der Fall war – die Alias-Datensätze gelöscht werden, sodass es der Erstellung und Versendung des Q-Formulars erst gar nicht bedürfen würde. So halte ich z. B. aus Gründen des Verhältnismäßigkeitsprinzips eine Löschung dann für geboten, wenn das in Verlust geratene oder gestohlene Ausweisdokument in der Zwischenzeit sichergestellt worden ist und somit eine missbräuchliche Verwendung der falschen Identität faktisch ausgeschlossen ist.

Ich werde meine Bedenken zu dem neuen Verfahren und Vorschläge für eine datenschutzfreundlichere Lösung in der GKI, die hoffentlich bald beteiligt wird, weiterverfolgen.

16.2.3 Konsultationsverfahren nach Artikel 17 Abs. 2 SDÜ noch immer ohne ausreichende Rechtsgrundlage

Im Rahmen der Erteilung von Schengen-Visa können die Schengen-Mitgliedsstaaten bestimmen, dass bei Angehörigen bestimmter Länder vor einer Visumserteilung eine Konsultation der zentralen Behörde des eigenen Landes und ggf. der zentralen Behörden der anderen Staaten erfolgen muss. Zentrale Behörde in Deutschland ist das Auswärtige Amt wie in den meisten anderen Mitgliedsstaaten. Die Mitgliedsstaaten

staaten teilen einander mit, bei welchen Staatsangehörigen sie die Erteilung eines Sichtvermerks von einer solchen Konsultation abhängig machen wollen. Ein Visum kann in diesen Fällen nur erteilt werden, wenn von der konsultierten zentralen Behörde die Antwort „keine Bedenken" kommt, oder wenn binnen sieben Arbeitstagen keine Antwort vorliegt. Rechtsgrundlage für dieses Verfahren bildet Artikel 17 Abs. 2 SDÜ. Das Verfahren selbst ist für alle Schengen-Staaten in den „Gemeinsamen Konsularischen Instruktionen" geregelt.

Ich habe mich im Jahre 2002 beim AA in Berlin und in dessen Rechenzentrum in Bonn über das Verfahren informiert. Wie ich hierbei festgestellt habe, werden im nationalen Konsultationsverfahren durchschnittlich monatlich rund 50 000 Fälle abgewickelt. Das gesamte Nachrichtenaufkommen auf dem zentralen Server des AA (alle eingehenden Anfragen, Weiterleitungen, Antworten der Sicherheitsbehörden und der zentralen Behörden der anderen Staaten sowie die Rückantworten) liegt im Monatsdurchschnitt bei mehreren Hunderttausend Datensätzen. Das AA leitet die Anfragen der eigenen Auslandsvertretungen und die der zentralen Behörden der anderen Staaten an die Sicherheitsbehörden (BKA, BfV, BND und ZKA) weiter und vermittelt deren Antworten. Hierbei wird der anfragenden Behörde im Falle vorliegender Bedenken nur mitgeteilt, dass solche bestehen, nicht jedoch wer diese Bedenken geäußert hat und auch nicht deren Gründe. Die Informationsverarbeitung läuft vollautomatisch über das Mail-System VISION im Rechenzentrum des AA in Bonn ab, ohne dass es im Normalfall einer individuellen Bearbeitung bedarf. Das AA in Berlin hat lediglich lesenden Zugriff auf das System. Die Daten werden drei Monate nach Einleitung des Verfahrens automatisch gelöscht.

Nach dem Ergebnis dieser Informations- und Kontrollbesuche haben sich in verfahrensmäßiger Hinsicht keine datenschutzrechtlichen Probleme ergeben. Für eine abschließende Beurteilung werde ich das Konsultationsverfahren auch bei den im nationalen Verfahren beteiligten Sicherheitsbehörden kontrollieren.

Kritik habe ich jedoch erneut an der fehlenden Rechtsgrundlage für die Durchführung des in Artikel 17 Abs. 2 SDÜ lediglich institutionalisierten Konsultationsverfahrens geübt (vgl. 15. TB Nr. 23.2.1.2). Die Einverständniserklärung, die der Visumsantragsteller im Antrag auf Erteilung eines Schengen-Visums abgeben muss, kann die fehlende Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung der für die Durchführung des Verfahrens erforderlichen personenbezogenen Daten nicht ersetzen. Das AA hat hierzu erklärt, es werde die Schaffung einer Rechtsgrundlage für die Durchführung der Konsultationen in einem EU-Rechtsakt weiter verfolgen. Die EU-Kommission habe dieses Anliegen in ihren Arbeitsplan für das Jahr 2003 aufgenommen.

16.3 ZIS-Übereinkommen

16.3.1 Aktennachweissystem – Ergänzung des Zollinformationssystems

Das mit dem Übereinkommen über die Nutzung der Informationstechnologie im Zollbereich vom 26. Juli 1995 (vgl. zuletzt 18. TB Nr. 13.4) eingerichtete Zollinformationssystem (ZIS), das zu einer engeren Zusammenarbeit der Zollbehörden der EU-Mitgliedsstaaten im Rahmen der dritten Säule der EU (Inneres und Justiz) führen soll, hat auch im Berichtszeitraum seinen Wirkbetrieb nicht aufgenommen. Die Gründe hierfür sind technischer Natur, zumal die Übereinkunft über die vorläufige Anwendung des Übereinkommens zwischen einigen Mitgliedsstaaten der EU am 1. November 2000 in Kraft getreten ist.

Inzwischen haben die EU-Mitgliedsstaaten ihren Meinungsstreit darüber beigelegt, ob das ZIS als reine Ausschreibungsdatenbank oder gleichzeitig auch als Aktennachweissystem für Zwecke der Recherche genutzt werden kann. Auf Initiative der damaligen deutschen Präsidentschaft im 1. Halbjahr 1999 wurden Beratungen über eine als „Aktennachweissystem" bezeichnete automatisierte Datei geführt, die den für die Zollfahndung zuständigen Stellen der Mitgliedsstaaten Informationen über das Vorhandensein von Akten über abgeschlossene oder laufende Ermittlungsverfahren in den Mitgliedsstaaten zur Verfügung stellen soll. Ziel ist es, die für die Zollfahndung in den Mitgliedsstaaten zuständigen Stellen in die Lage zu versetzen, ihre Ermittlungen untereinander rasch abzustimmen und sich ggf. auf ein gemeinsames Vorgehen zu verständigen. Hierdurch soll insbesondere die Bekämpfung der organisierten und grenzüberschreitenden Kriminalität verbessert werden. Das Aktennachweissystem ergänzt damit die Datenbank des ZIS zur Koordinierung der Maßnahmen der Stellen, die für die Kontrolle des Personen- und Warenverkehrs zuständig sind (vgl. hierzu Nr. 9.10).

Als Rechtsgrundlage für das Aktennachweissystem wurde ein Protokoll zur Ergänzung des ZIS-Übereinkommens gewählt. Die Beratungen des Entwurfs in der zuständigen Ratsarbeitsgruppe sind nach Mitteilung des BMF, das mich stets an der Abstimmung der deutschen Verhandlungsposition beteiligt hat, abgeschlossen.

Ich begrüße den von den EU-Mitgliedsstaaten gewählten Weg, für das Aktennachweissystem eine vom ZIS rechtlich unabhängige Datenbank mit eigener Zweckbestimmung und eigenem Anwendungsbereich einzurichten. Auch gegen die im Protokoll vorgesehenen Regelungen habe ich keine Einwände: Der Umfang der im Aktennachweissystem zu speichernden personenbezogenen Daten ist auf das erforderliche Maß beschränkt; es gelten strenge Zweckbindungsregelungen; der Nutzerkreis ist eng begrenzt und die Dauer der vorgesehenen Speicherfristen trägt dem Stand des jeweiligen Ermittlungsverfahrens Rechnung.

Mit der zu erwartenden Annahme des Protokolls durch den Rat und vor dem Hintergrund der Schaffung der innerstaatlichen Voraussetzung durch bereichsspezifische Regelungen für den Zollfahndungsdienst (s. o. Nr. 15.1) dürften die Hindernisse für eine deutsche Ratifizierung des ZIS-Übereinkommens beseitigt sein. Mit der Vorlage eines entsprechenden Gesetzentwurfs der Bundesregierung nach Artikel 59 Abs. 2 GG ist im Laufe des Jahres 2003 zu rechnen.

16.3.2 Gemeinsame Aufsichtsbehörde für das ZIS – eine weitere Datenschutzinstanz im Dritten Pfeiler der EU

Am 7. März 2002 hat sich als weitere datenschutzrechtliche Aufsichtsbehörde neben der gemeinsamen Kontrollinstanz nach dem Schengener Durchführungsübereinkommen und derjenigen nach dem Europol-Übereinkommen die gemeinsame Aufsichtsbehörde gemäß Artikel 18 des ZIS-Übereinkommens konstituiert. Sie setzt sich aus je zwei Vertretern der

nationalen Kontrollinstanzen zusammen. Im Hinblick auf die ausschließliche Bundeszuständigkeit für den Bereich der Zollfahndung wird Deutschland dabei durch mich vertreten.

Die Gemeinsame Aufsichtsbehörde ist im Wesentlichen für die datenschutzrechtliche Kontrolle des ZIS sowie des Aktennachweissystems, insbesondere bezüglich des von der EU-Kommission betriebenen Zentralcomputers in Brüssel zuständig und prüft dabei auftretende Anwendungs- und Auslegungsschwierigkeiten. Im Hinblick auf die bisher fehlende technische Realisierung des Informationssystems ist das Gremium nur selten zusammengetreten. Es ist jedoch davon auszugehen, dass mit Aufnahme des Wirkbetriebes des ZIS und des Aktennachweissystems die Anforderungen an die Aufsichtsbehörde erheblich steigen werden.

16.4 Neapel II-Übereinkommen

In früheren Tätigkeitsberichten (vgl. u. a. 18. TB Nr. 13.3) habe ich verschiedentlich über das Neapel II-Übereinkommen der EU-Mitgliedsstaaten zur gegenseitigen Amtshilfe und Zusammenarbeit der Zollverwaltungen vom 18. Dezember 1997 berichtet. Ein entsprechendes Ratifizierungsgesetz nach Artikel 59 Abs. 2 Grundgesetz zu diesem Übereinkommen ist am 31. Januar 2002 vom Deutschen Bundestag gebilligt worden; es ist am 1. Juni 2002 in Kraft getreten. Das Übereinkommen bildet einen Meilenstein bei der Europäischen Kooperation im Bereich des Zolls in Ergänzung zu entsprechenden Regelungen in den Bereichen Justiz und Polizei (vgl. Nr. 16.2). Neben einer verbesserten und erweiterten Zusammenarbeit im Zollbereich erhalten die nationalen Zollverwaltungen dadurch die Möglichkeit zur grenzüberschreitenden Observation und zu weiteren grenzüberschreitenden Erhebungsbefugnissen. Nach Artikel 25 des Vertrages sind die Zollverwaltungen jedoch verpflichtet, in jedem Einzelfall den Schutz des Persönlichkeitsrechts zu gewährleisten. Im November 2002 hat die Bundesrepublik Deutschland die Beitrittsurkunde beim Verwahrer hinterlegt, sodass der Vertrag 90 Tage später mit denjenigen Staaten in Kraft treten kann, die ebenfalls von dieser Option Gebrauch machen. Dies sind derzeit sechs Staaten, darunter Frankreich und die Niederlande. Ich werde zu gegebener Zeit überprüfen, ob und wie die deutschen Zollbehörden die vorgenannten datenschutzrechtlichen Anforderungen bei der grenzüberschreitenden Zusammenarbeit beachten.

17 Verfassungsschutz

17.1 Änderung des Bundesverfassungsschutzgesetzes erweitert die Befugnisse des Bundesamtes für Verfassungsschutz

Kernpunkt des Terrorismusbekämpfungsgesetzes (TBG) vom 9. Januar 2002 (s. Nr 2.2) sind die Änderungen im Bundesverfassungsschutzgesetz (BVerfSchG – Artikel 1 TBG).

Dies beginnt mit der Erweiterung des Aufgabenbereichs des Bundesamtes für Verfassungsschutz nach § 3 Abs. 1 Nr. 4 BVerfSchG auf die Sammlung und Auswertung von Informationen über inländische Bestrebungen, die sich gegen den Gedanken der Völkerverständigung (Artikel 9 Abs. 2 GG), insbesondere gegen das friedliche Zusammenleben der Völker (Artikel 26 Abs. 1 GG) richten. Leider ist der Gesetzgeber meiner Anregung nach einer Konkretisierung dieser Rechtsbegriffe – wie in § 4 des Gesetzes für die anderen Schutzgüter – nicht gefolgt, was im Hinblick auf die nachfolgend skizzierten erweiterten Befugnisse des BfV nicht unbedenklich ist.

Besonders gravierend für das Persönlichkeitsrecht sind die neuen Befugnisse des BfV, gem. § 8 Abs. 5 bis 8 BVerfSchG Auskünfte bei Banken, Post-, Telekommunikations-, Teledienst- und Flugunternehmen über Bankkonten und Postfächer, über Transportleistungen, Telekommunikationsverbindungs- und Teledienstenutzungsdaten einzuholen. Die G10-Kommission wird – über ihren bisherigen Aufgabenbereich hinaus – beteiligt. Ich vertrete die Auffassung, dass aus der Erhebungsbefugnis des BfV nicht zwangsläufig eine entsprechende Auskunftspflicht der ersuchten nicht öffentlichen Stelle folgt. Vielmehr dürfen die Auskünfte nur erteilt werden, wenn die unterschiedlich ausgestalteten materiell-rechtlichen Voraussetzungen der Datenübermittlung bei den ersuchten Stellen gegeben sind. Gleichwohl habe ich erhebliche Bedenken gegen diese neuen Befugnisse, auch wenn sie nur Ersuchen im Einzelfall zulassen, weil es sich im Grunde um polizeiliche Befugnisse handelt und die Daten bei Vorliegen der Voraussetzungen an die Strafverfolgungsbehörden weitergegeben werden.

Des Weiteren wurde in § 9 Abs. 4 BVerfSchG erstmals eine gesetzliche Grundlage für den Einsatz des so genannten IMSI-Catcher durch den Verfassungsschutz geschaffen. Wegen der technischen Einzelheiten zu dieser Erhebungstechnik verweise ich auf die Ausführungen zu der Parallelregelung in § 100i Strafprozessordnung (s. Nr. 8.2.4). Meine Bedenken gegen die Regelung bestehen insbesondere darin, dass auch schutzwürdige Interessen Dritter durch solche Maßnahmen beeinträchtigt werden können. Immerhin ist es gelungen, im Verlaufe der Beratungen die Regelung durch verfahrenssichernde Vorkehrungen aus dem Artikel 10-Gesetz zu entschärfen.

Einer alten Forderung des Verfassungsschutzes folgend sind die Fristen für Datenspeicherungen aufgrund von § 3 Abs. 1 Nr. 3 (gewaltgeneigter Ausländerterrorismus) und Nr. 4 – neu – BVerfSchG (völkerrechtswidrige Bestrebungen) auf 15 Jahre verlängert bzw. neu festgelegt worden. In Anbetracht der Tatsache, dass diese Erkenntnisse vielfach nur auf tatsächlichen Anhaltspunkten für solche Bestrebungen beruhen, ist dies eine bedenkliche Verschlechterung für das Persönlichkeitsrecht Betroffener. Immerhin ist es trotz gegenteiliger Bemühungen der Sicherheitsbehörden gelungen, die gesetzliche Verpflichtung zur Prüfung der Datenspeicherung im Einzelfall bzw. spätestens nach fünf Jahren beizubehalten.

Schließlich ist in § 18 Abs. 1a – neu – BVerfSchG dem Bundesamt für die Anerkennung ausländischer Flüchtlinge und den Ausländerbehörden der Länder die Verpflichtung auferlegt worden, von sich aus die jeweils zuständige Verfassungsschutzbehörde über die ihnen bekannt gewordenen Informationen einschließlich personenbezogener Daten über Bestrebungen und Tätigkeiten nach § 3 Abs. 1 BVerfSchG zu unterrichten. Das gilt auch für einfache extremistische Bestrebungen, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung für die Aufgabenerfüllung des Verfassungsschutzes erforderlich ist. Dies bedeutet eine erhebliche Ausweitung der schon bestehenden Unterrichtungspflicht auf alle in § 3 Abs. 1 BVerfSchG genannten Schutzgüter bei gleichzeitiger Absenkung der Übermittlungsschwelle. Denn im Falle des § 18 Abs. 1 BVerfSchG

muss nur über bekannt gewordene T atsachen zu Spionageaktivitäten bzw. zu gewaltgeneigten Bestrebungen unterrichtet werden. Dadurch geraten vermehrt Asylbewerber und Ausländer, selbst wenn sie sich nur aktiv politisch betätigen, ins Visier der Verfassungsschutzbehörden. Insgesamt bedeuten die Neuregelungen im Bundesverfassungsschutzgesetz eine erhebliche zusätzliche Beeinträchtigung des Persönlichkeitsrechts Betroffener. Doch ist darauf hinzuweisen, dass die neuen Befugnisse nach Artikel 22 Abs. 2 TBG auf fünf Jahre befristet und überdie s vor Ablauf der Befristung zu evaluieren sind (s. Nr. 2.3.1).

17.2 Datenlöschung und Aktenvernichtung beim Bundesamt für Verfassungsschutz

17.2.1 Personenbezogene Daten in Akten unterliegen nach Löschung in NADIS-PZD einem absoluten Verwertungsverbot

Anders als in einer Reihe von Landesdatenschutz- und Landesverfassungsschutzgesetzen, in denen nach Löschung von personenbezogenen Daten in Dateien ausdrücklich auch die Vernichtung der dazu gehörenden Akten, die zur Aufgabenerfüllung nicht mehr erforderliche personenbezogene Daten enthalten, geregelt ist (z. B. § 11 Abs. 3 Verfassungsschutzgesetz NW, s. auch § 33 BKA-Gesetz), ist nach § 12 Bundesverfassungsschutzgesetz (BVerfSchG) und § 20 Abs. 2 BDSG eine Löschung/V ernichtung nur für personenbezogene Daten vorgesehen, die automatisiert bzw. in einer Datei verarbeitet werden. In Bezug auf Akten regelt § 13 BVerfSchG als Spezialvorschrift ausdrücklich nur deren Berichtigung und Sperrung; ebenso sehen § 20 Abs. 1 Satz 2 und Abs. 6 BDSG auch nur die Berichtigung und Sperrung von personenbezogenen Daten in Akten vor.

Unabhängig von der Frage einer rechtlichen V erpflichtung zur Vernichtung jedenfalls der Personenakten (P-Akten) nach einer Löschung von personenbezogenen Daten des Betroffenen im nachrichtendienstlichen Informationssystem-Personenzentraldatei (NADIS-PZD) – eine Forderung, die ich stets aufrecht erhalten ha be (s. 16. TB Nr. 14.5) – stimmen BMI und BfV mit mir überein, dass diese in jedem Fall zu vernichten sind. Hierzu ist eine V erfahrensregelung im BfV erlassen worden.

Für Aktenteile mit personenbezogenen Daten aus den umfangreicheren Sachakten – z. B. über bestimmte Beobachtungsobjekte – gilt dies entsprechend der getroffenen Vereinbarung unter Beachtung der Aktenvollständigkeit nur dann, wenn es möglich und vom Arbeitsaufwand vertretbar ist.

Ansonsten ist die Löschung des Datensatzes (z. B. durch Stempelaufdruck auf bzw. in der Sachakte) zu dokumentieren. Hiervon betroffene Daten gelten – ohne dass dieser Begriff in Verfahrensregelungen des BfV gebraucht wird – als „gesperrt“ (vgl. § 13 Abs. 2 Satz 2 BV erfSchG). Danach dürfen sie grundsätzlich nicht mehr genutzt oder übermittelt werden. Da die Speicherung als solche wegen des o. a. Sachzusammenhangs bestehen bleibt, muss sicher gestellt werden, dass sie für den Betrof fenen keine negativen Auswirkungen (mehr) haben kann.

Darüber hinaus unterliegen personenbezogene Daten eines Betroffenen, dessen Daten in NADIS-PZD gelöscht sind, einem absoluten Verwertungsverbot, auch wenn sie noch in Akten gleich welcher Art geführt werden. Dies ist ein Ausfluss des informationellen Selbstbestimmungsrechts, denn sie hätten an sich vernichtet werden müssen. Gleiches gilt auch, wenn sie in Sachakten als „gesperrt“ gelten. Unter das Verwertungsverbot fällt jede denkbare weitere Nutzung der Daten, insbesondere auch die Übermittlung an Dritte.

Die Rechte des Betrof fenen, namentlich seine Rechte auf Auskunft, Berichtigung und Löschung, bleiben unberührt. Dritten gegenüber dürfen weder die gesperrten Daten noch die Tatsache der „Sperrung“ mitgeteilt werden.

Ausnahmen vom Übermittlungs- und V erwertungsverbot sehe ich nur in eng begrenztem Rahmen. Sie sind unter strikter Beachtung des Grundsatzes der Verhältnismäßigkeit zulässig, soweit dies zum Schutz besonders hochwertiger Rechtsgüter unerlässlich ist und die Aufklärung des Sachverhalts ohne Heranziehung der Erkenntnisse aus Sachakten aussichtslos oder wesentlich erschwert wäre. Dies kann z. B. der Fall sein, wenn sich aus noch vorhandenen Unterlagen tatsächliche Anhalts punkte für noch nicht verjährte Straftaten i. S. d. § 138 Strafgesetzbuch (StGB) er geben. Hier ist auch der V erfassungsschutz – wie jedermann – an das Legalitätsprinzip gebunden. Bei solchen Straftaten, vor allem nach §§ 211, 212 StGB, ist dem Strafverfolgungsinteresse des Staates der Vorrang vor dem Interesse des Betroffenen am Schutz „seiner“ Daten zu geben.

Abgesehen von dem Anspruch des BMI als oberster Aufsichtsbehörde auf Vorlage aller Unterlagen des BfV , sehe ich sowohl beim Parlamentarischen Kontrollgremium, bei Parlamentarischen Untersuchungsausschüssen und auch bei Strafverfolgungsbehörden Einsichtsrechte nur im Rahmen der o. a. Ausnahmen.

Zusammen mit den Datenschutzbeauftragten der Länder habe ich mich vor diesem Hinter grund mit der o. a. Problematik der Behandlung von Unterlagen mit andernorts gelöschten Daten befasst; dazu ist am 24. Oktober 2002 ein gemeinsamer Beschluss ergangen (s. Anlage 25).

17.2.2 Muss das Bundesamt für Verfassungsschutz Akten an das Bundesarchiv abgeben?

Im Rahmen der Diskussion über die Behandlung von personenbezogenen Daten in Persone n- und Sachakten im Jahre 2001 hatte das BfV zu verstehen gegeben, dass es im Hinblick auf das von mir postulierte absolute V erwertungsverbot (s. Nr . 17.2.1) nunmehr die Anwendbarkeit des Bundesarchivgesetzes (BArchG) auf Unterlagen des BfV problematisiere. Das Bundesarchiv widersprach mit dem Hinweis auf die in § 2 BArchG geregelte Anbietungsverpflichtung von Behörden der Auf fassung des BfV, archivwürdiges Schriftgut unterliege ebenfalls dem V erwertungsverbot, das vom Bundesarchiv auch zu beachten sei. Da das Bundesarchiv der – irrigen – Auffassung war, ich würde die Meinung des BfV vertreten, hielt ich es für geboten, mit BMI, BfV und der für das Bundesarchiv zuständigen Beauftragten der Bundesregierung für Kultur und Medien die Frage der Geltung und Anwendungsbreite des BArchG im Hinblick auf die beim BfV gef ührten Unterlagen unter Einbeziehung des bisher durchgeführten Verfahrens zu erörtern. Dabei habe ich deutlich gemach t, dass das BArchivG auch auf das BfV Anwendung findet. Grund dafür ist das Fehlen einer expliziten Aktenvernichtungsregelung im BVerfSchG. Nach § 2 Abs. 7 BArchG bleiben Rechtsvorschriften über

die Vernichtung von Unterlagen unberührt. Das BVerfSchG regelt nur die Löschung personenbezogener Daten in Dateien (§ 12 Abs. 2), nicht ausdrücklich aber die Vernichtung in Akten. § 13 BVerfSchG gilt nur für die Berichtigung und Sperrung solcher Daten. Das BArchG ist daher anzuwenden; Personen- und Sachakten des BfV sind dem Bundesarchiv nach den Regelungen des BArchG anzubieten. Ich habe durchgängig die Auffassung vertreten, dass das BArchG „hinreichend normenklare Bestimmungen" mit gesetzlich präzise bestimmten Zwecken für eine zulässige Aufbewahrung personenbezogener Daten enthalte.

Zurzeit wird im BfV folgendes Verfahren angewandt:

Das BfV hat eine große Zahl von Akten – entsprechend einer Vereinbarung mit dem Bundesarchiv, die im Januar 2001 erneuert wurde – als „zeitgeschichtlich bedeutsam" eingestuft. Dabei handelt es sich insgesamt um Grundsatzakten, zu denen auch Arbeits- und Aktenpläne gehören, und um Personen- und Sachakten. Tatsächlich sind diese Unterlagen bisher nicht nach § 2 BArchG dem Bundesarchiv angeboten worden. Es handelt sich also noch um ein Verfahren im „Vorfeld" des BArchG, da auch das Bundesarchiv selbst die als zeitgeschichtlich bedeutsam gekennzeichneten Unterlagen noch nicht dahin gehend überprüft hat, ob ihnen nach § 3 BArchG „bleibender Wert für die Erforschung oder das Verständnis der deutschen Geschichte, die Sicherung berechtigter Belange der Bürger oder die Bereitstellung von Informationen für Gesetzgebung, Verwaltung und Rechtsprechung zukommt".

Die Tatsache, dass Akten mit personenbezogenen Daten im BfV auch nach Löschung der Daten des Betroffenen in Dateien (§ 12 Abs. 2 BVerfSchG) und trotz des Wegfalls der Erforderlichkeit für die Aufgabenerfüllung des BfV weiter aufbewahrt werden, stellt auch nach Auffassung des BMI einen fortdauernden Eingriff in das Persönlichkeitsrecht dar. Vor diesem Hintergrund habe ich die Ansicht vertreten, dass wegen der Geltung des BArchG eine Darstellung in den Dienstanweisungen der Abteilungen des BfV ausreiche; dort müsste die Pflicht zum Anbieten der Sach- und Personenakten nach Fortfall der Erforderlichkeit für die Aufgabenerfüllung des BfV einheitlich verdeutlicht werden. In der Vereinbarung mit dem Bundesarchiv und/oder in den Arbeitsplänen des BfV sollte eine Frist für die Prüfung nach § 2 BArchG enthalten sein, die wie folgt lauten könnte: „Wenn eine Akte insgesamt zur Erfüllung der Aufgaben nicht mehr erforderlich ist, ist binnen eines Jahres zu entscheiden, ob sie an das Bundesarchiv abzugeben ist. Wird sie nicht abgegeben, ist sie zu vernichten".

Zwar betrachte ich eine solche „unter gesetzliche" Verfahrensanweisung als ausreichend; ich würde aber aus Gründen der Normenklarheit einer bereichsspezifischen Vorschrift zur Anwendung des BArchG im BVerfSchG den Vorzug geben. Neben einer ggf. zu schaffenden Regelung zur Vernichtung der Akten wäre in § 13 BVerfSchG dann – vergleichbar etwa der Regelung in § 33 BKA-Gesetz – aufzunehmen, dass anstelle der Vernichtung eine Abgabe an das Bundesarchiv erfolgen muss, wenn den Unterlagen bleibender Wert i. S. v. § 3 BArchG zukommt. Ich habe vorgeschlagen, die o. a. Ein-Jahres-Frist in die gesetzliche Regelung aufzunehmen. Das BMI ist allerdings der Auffassung, die Befristung für die Abgabeentscheidung sollte lediglich in den Arbeitsplänen bzw. in der bilateralen Vereinbarung zwischen dem BfV und dem Bundesarchiv festgelegt werden.

Die Gespräche mit dem BMI und der Beauftragten der Bundesregierung für Kultur und Medien waren bei Redaktionsschluss noch nicht beendet. Ich bin allerdings optimistisch, dass es zu einer gesetzlichen Regelung kommen wird, die alle Seiten zufrieden stellt. Bis dahin sollte das Verfahren zwischen BfV und Bundesarchiv bereits entsprechend gestaltet werden.

17.3 Aktenvernichtung beim Bundesamt für Verfassungsschutz nunmehr durch eine neue Dienstanweisung klar geregelt

Aus gegebenem Anlass habe ich im Jahr 2001 die Vernichtung von Personenakten (P-Akten) nach Löschung der zugehörigen personenbezogenen Daten in der Personenzentraldatei des nachrichtendienstlichen Informationssystems (NADIS-PZD) geprüft. Hierbei stellte ich fest, dass das Verfahren der Aktenvernichtung insgesamt einer kritischen Überprüfung zu unterziehen war, da Teile von P-Akten, die ebenfalls hätten vernichtet werden müssen, nicht dem zur Vernichtung anstehenden Gesamtvorgang zugeführt worden waren. In einem Fall war z. B. der Hinweis auf die in einem anderen Bereich zuvor angelegte Teilakte bei der Aktenvernichtung von allen Beteiligten offenbar übersehen worden.

Aufgrund der festgestellten organisatorischen Mängel bei der Zusammenführung von Teilen von P-Akten und der Vernichtung dieser Akten hat – auf meine Veranlassung hin – das BfV ein verbessertes Verfahren entwickelt. Anfang 2002 wurde eine neue „Dienstanweisung für die Vernichtung von Gesamtakten" in Kraft gesetzt, die ich im Echtbetrieb überprüft habe. Durch diese Dienstanweisung scheint nunmehr sichergestellt zu sein, dass Akten, die nach Löschung der personenbezogenen Daten in NADIS-PZD zu vernichten sind, tatsächlich vollständig und fristgerecht vernichtet werden. Die von mir festgestellten Mängel werden aller Wahrscheinlichkeit nach in Zukunft nicht mehr auftreten.

Im BfV werden alle Akten nach und nach verfilmt. Bei der Vernichtung von Daten auf Rollfilmen stellt sich allerdings noch ein Problem. Daten auf Rollfilmen über Personen, deren Akten zu vernichten sind, werden im Zuge des Aktenvernichtungsverfahrens anstelle einer physischen Vernichtung nach Herausschneiden der entsprechenden Teile mit einem schwarzen Balken als „vernichtet" gekennzeichnet. Diese Filme werden nach und nach jahrgangsweise vom BfV überprüft; die Teile, die noch nicht zu vernichten sind, werden herausgeschnitten und archiviert. Die – durch einen schwarzen Balken bereits gekennzeichneten – „gelöschten" Daten werden bei diesem Arbeitsvorgang vernichtet.

Angesichts des nachvollziehbaren hohen Arbeitsaufwandes, der beim Herausschneiden und Vernichten der Teile im Zuge der konkret anstehenden Aktenvernichtung entstehen würde, habe ich gegen dieses Verfahren keine grundlegenden datenschutzrechtlichen Bedenken. Zwar sind die durch den schwarzen Balken als „vernichtet" gekennzeichneten Daten noch lesbar; ein gezieltes Recherchieren nach solchen Daten erscheint aber nahezu ausgeschlossen.

Ich habe das BMI in Anbetracht des größeren Arbeitsrückstandes des BfV bei der Überprüfung der Rollfilme gebeten, das BfV anzuhalten, diese Arbeiten beschleunigt fortzusetzen und mich über das Ergebnis zu unterrichten.

18 MAD

18.1 Änderung des MAD-Gesetzes

18.1.1 Gesetzesinitiative muss neu gestartet werden – Zugriff auf PERFIS weiterhin ohne gesetzliche Grundlage

In meinem 18. TB (Nr. 15.1) habe ich von einem Gesetzgebungsvorhaben zur Änderung des MAD-Gesetzes berichtet, das den automatisierten Zugriff des MAD-Amtes auf das Personalführungs- und Informationssystem der Bundeswehr (PERFIS – vgl. hierzu auch Nr. 30.2) auf eine spezialgesetzliche Grundlage stellen sollte. Diese ist erforderlich, da es sich beim Zugriff auf das Datenbankprogramm PERFIS um eine automatisierte Abfrage von Personaldaten handelt. Das davon betroffene Personaldatengeheimnis darf nur durchbrochen werden, wenn dies nach dem Bundesbeamtengesetz bzw. dem Soldatengesetz zulässig ist. Da dies bisher nicht der Fall ist, hatte ich seit langem eine spezialgesetzliche Regelung für diesen Zugriff auf PERFIS für Zwecke des MAD gefordert. In dem Entwurf eines Ersten Gesetzes zur Änderung des MAD-Gesetzes (Bundesratsdrucksache 1078/01 vom 21. Dezember 2001) waren meine datenschutzrechtlichen Forderungen berücksichtigt. Der Gesetzentwurf war das Ergebnis eingehender Beratungen des BMVg mit den beteiligten Ressorts und mir. Gegenüber früheren Entwürfen enthielt er deutliche Verbesserungen, wie z. B.

- die Auflistung von – nur noch – sieben unbedingt zur Identifizierung erforderlichen Personaldaten aus PERFIS (von insgesamt über 400 Datenfeldern);
- die Zweckbindung der Abrufe;
- die Vollprotokollierung aller Abrufe zu Kontrollzwecken;
- den Erforderlichkeitsgrundsatz im § 14 Abs. 2, wonach die Übermittlung von Informationen an den MAD nach § 10 Abs. 1 MAD-Gesetz nur rechtmäßig ist, wenn sie „erforderlich sein können“ (vorher: „dienlich sein können“);
- detaillierte Einzelheiten in der vom BMVg zu erlassenden Dienstvorschrift, bei der ich vor Erlass und auch vor jeder Änderung anzuhören bin.

Der Gesetzentwurf unterfiel der Diskontinuität, da er bis zum Ende der letzten Legislaturperiode nicht mehr verabschiedet wurde. Nach meinen Erkenntnissen lag dies in unterschiedlichen politischen Auffassungen zu dem ebenfalls in dem Entwurf geregelten Auslandseinsatz des MAD begründet. Bis Redaktionsschluss hat die Bundesregierung noch keinen neuen Gesetzesentwurf vorgelegt.

18.1.2 Änderung des MAD-Gesetzes durch das Terrorismusbekämpfungsgesetz

Durch das Terrorismusbekämpfungsgesetz (s. o. Nr. 2.2) ist die Aufgabenstellung des MAD wie beim BfV auf die Beobachtung von Bestrebungen, die gegen den Gedanken der Völkerverständigung, insbesondere gegen das friedliche Zusammenleben der Völker gerichtet sind, für den Personenkreis, für den er zuständig ist, erweitert worden. Weiter darf er nach § 10 Abs. 3 MAD-Gesetz bei Betreibern von Telekommunikationsdiensten und Telediensten Auskünfte über Telekommunikationsverbindungsdaten und Teledienstenutzungsdaten einholen. Seine Befugnisse bleiben damit hinter denen des BfV (§ 8 Abs. 5 bis 8 BVerfSchG, s. o. Nr. 17.1) und denen des BND (§ 2 Abs. 1a und § 8 Abs. 3a BND-Gesetz, s. u. Nr. 19.1) zurück. Wegen meiner grundsätzlichen Bedenken gegen diese neuen Befugnisse verweise ich auf die Ausführungen zu Nr. 17.1.

18.2 „Elektronisches Büro“ im MAD-Amt – ein Konflikt mit dem Datenschutz

BMVg und MAD-Amt haben mich frühzeitig an der Planung eines IT-Vorhabens beteiligt, das die Informationsverarbeitung des MAD durch ein Dokumentenmanagement-, ein Archiv- und ein Workflowsystem wesentlich verbessern und erweitern soll. Mit dem Projekt in einer Abteilung beginnend, sollen auch datenschutzrechtliche Anliegen wie Zugriffsschutz auf Daten und Protokollierungen zum Zweck nachhaltiger Kontrollmöglichkeiten verbessert werden.

Dabei tritt das Problem auf, dass die elektronische Speicherung und weitere Verarbeitung von Texten, Unterlagen und ganzen Akten zwangsläufig auch zur Speicherung und Weiterverarbeitung von Daten über Personen führt, die nicht die Speicherkriterien des MAD-Gesetzes erfüllen. So erfolgt etwa bei der elektronischen Speicherung von Medienberichten eine Erfassung von Personen, die nicht in den Zuständigkeitsbereich des MAD fallen (u. a. Randpersonen, Politiker, Wissenschaftler, Künstler). Solche Datensammlungen sind mit der geltenden Rechtslage nicht vereinbar. Damit stellt sich hier das gleiche Problem wie bei der Realisierung des „elektronischen Büros“ im BfV (s. 18. TB Nr. 14.1). Auch beim MAD-Amt will ich mich mit Blick auf die technische Entwicklung einer Übergangslösung, die die Speicherung und eingeschränkte weitere Verarbeitung und Nutzung dieser Datensammlungen ermöglicht, bis zum Erlass einer normenklaren Regelung nicht verschließen.

Zu dem hier interessierenden Punkt wurde mir erklärt, eine Recherchemöglichkeit werde nur bezüglich solcher Personen eingerichtet, für die der MAD zuständig ist, und die damit die Speicherkriterien nach dem MAD-Gesetz erfüllen. Bei einem gescannten Dokument soll für diesen Personenkreis ein separater Datensatz angelegt werden; nur insoweit sei eine Recherche möglich. Gegen ein solches Vorgehen hätte ich keine grundsätzlichen datenschutzrechtlichen Bedenken.

Weiter wollen BMVg und MAD-Amt dem Problem über eine dezidierte Protokollierung der Zugriffe auf besondere Dateien, d. h. in besonders geschützte Speicherbereiche, begegnen. Diese stehen den allgemeinen Anwendern nicht zur Verfügung, sondern nur dem Auditor, den behördlichen Datenschutzbeauftragten und den für die IT-Sicherheit Verantwortlichen. Meine Kontrollmöglichkeit bleibt davon unberührt. Die datenschutzrechtlich gebotenen Regelungen müssten im Rahmen einer Dateianordnung abschließend und für die Bearbeiter eindeutig festgelegt werden.

Ich habe dem BMVg mitgeteilt, dass ich gegen eine Weiterführung des Projekts unter Beachtung der o. g. Anforderungen keine grundlegenden Einwände habe. Bis zum Redaktionsschluss lagen mir allerdings die Feinkonzepte noch nicht vor, sodass eine abschließende Bewertung derzeit nicht möglich ist.

18.3 Datenschutzrechtliche Kontrolle

Im Berichtszeitraum habe ich eine datenschutzrechtliche Kontrolle bei der MAD-Stelle Düsseldorf – einer von 14 MAD-

Außenstellen – durchgeführt. Die MAD-Stellen erledigen im Wesentlichen Aufträge, die das MAD-Amt erteilt. Dabei handelt es sich in mehr als 90 % der Fälle um Mitwirkungen im Bereich der Sicherheitsüberprüfungen für die im Geschäftsbereich des BMVg tätigen Mitarbeiter (s. Nr. 20.3.2). Nach Erledigung der Aufträge werden die Akten an das MAD-Amt zurückgesandt; ein Aktenrückhalt erfolgt bei den Außenstellen nicht.

Zum Zeitpunkt der Kontrolle befanden sich bei der kontrollierten Stelle etwa 400 Aufträge in der Bearbeitung.

Für die Bearbeitung der Aufträge führt die MAD-Stelle eine automatisierte Datei, die lediglich der Vorgangssteuerung dient und die es dem MAD-Amt ermöglicht, für eine ausgeglichene Auslastung der MAD-Stellen und der Prüfdienste zu sorgen. Als einziges personenbezogenes Datum enthält die Datei eine Personenidentifikationsnummer, die für die Zuordnung zu dem betreffenden Vorgang erforderlich ist. Die Daten in dieser Datei werden spätestens fünf Quartale nach Erledigung des Auftrags bzw. Rückgabe der Akten an das MAD-Amt gelöscht.

Wie bereits bei einer früheren Kontrolle einer MAD-Außenstelle (s. 17. TB Nr. 15.1) habe ich auch bei der Kontrolle der MAD-Stelle Düsseldorf datenschutzrechtliche Mängel oder sonstige Verstöße gegen datenschutzrechtliche Vorschriften nicht festgestellt.

18.4 MAD zieht aufgrund meiner Bedenken Antrag auf Genehmigung einer Datei zurück

Nach § 8 MAD-Gesetz (MADG) i. V. m. § 14 Bundesverfassungsschutzgesetz (BVerfSchG) hat der MAD für jede automatisierte Datei mit personenbezogenen Daten, die sich auf den Aufgabenbereich nach dem MADG bezieht, eine Dateianordnung zu erstellen, die der Zustimmung des BMVg bedarf und zu der ich angehört werde. Auch im Berichtszeitraum hat mir das BMVg einige Dateianordnungen übermittelt, die – bis auf eine Ausnahme – keine grundsätzlichen datenschutzrechtlichen Probleme aufwarfen.

In der Datei, die auf datenschutzrechtliche Bedenken stieß, sollten Daten von bestimmten Personen gespeichert werden, deren Speicherung als Grundlage zur Erstellung einer Bedrohungsanalyse und zur Beurteilung der Sicherheitslage dienen sollte. Hierzu habe ich erhebliche Zweifel geäußert, ob die Führung dieser Datei zur Erfüllung der Aufgaben nach § 1 Abs. 2 MADG zulässig ist, ohne dass Anhaltspunkte dafür vorliegen, ob die dort zu speichernden Personen ihre Bestrebungen oder Tätigkeiten gegen Dienststellen oder Einrichtungen der Bundeswehr oder der verbündeten Streitkräfte richten. Diese Datei hätte nicht die gesetzlichen Speicherkriterien nach dem MADG erfüllt, die an den Geschäftsbereich des BMVg anknüpfen. Vielmehr ist der mit der Datei verfolgte Zweck dem Aufgabenbereich des BfV nach § 3 Abs. 1 BVerfSchG zuzuordnen. Wenn Anhaltspunkte dafür vorliegen, dass sich solche Tätigkeiten gegen die in § 1 Abs. 2 MADG genannten Einrichtungen richten, ist das BfV nach § 10 Abs. 1 MADG zur Übermittlung personenbezogener Daten an den MAD befugt. Erst dann wäre die Zuständigkeit des MAD gegeben. Bei der beabsichtigten Datei hätte es sich somit um eine datenschutzrechtlich unzulässige Vorratsspeicherung außerhalb des Anwendungsbereichs des MADG gehandelt.

Aufgrund meiner Bedenken hat der MAD seinen Antrag auf Genehmigung dieser Datei zurückgezogen.

19 Bundesnachrichtendienst

19.1 Auch der BND erhält durch das Terrorismusbekämpfungsgesetz erweiterte Befugnisse

Im Zuge des Terrorismusbekämpfungsgesetzes (TBG) vom 9. Januar 2002 (s. u. 2.2) ist auch als Artikel 3 das BND-Gesetz geändert worden. Danach erhält der BND, obwohl er Auslandsnachrichtendienst ist, zur Erfüllung seiner Aufgaben, dem § 8 Abs. 5 ff. Bundesverfassungsschutzgesetz folgend, Auskunftsbefugnisse bei Banken, sonstigen Finanzdienstleistern sowie im Bereich der Telekommunikation (vgl. § 2 Abs. 1a BND-Gesetz n. F.). Die dabei zu beachtenden verfahrensrechtlichen Schutzvorkehrungen entsprechen den Regelungen im Bundesverfassungsschutzgesetz (s. im Einzelnen unter Nr. 17.1). Insbesondere gilt auch die Befristung der Regelung auf fünf Jahre und die Evaluationsverpflichtung gemäß Artikel 22 TBG.

19.2 Trotz einiger datenschutzrechtlicher Verbesserungen bleibt das neue Artikel 10-Gesetz hinter einigen Erwartungen zurück

Das Gesetz zur Neuregelung von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G10) ist am 29. Juni 2001 in Kraft getreten (BGBl. I S. 1253). Damit wurde die zeitliche Vorgabe des Bundesverfassungsgerichts in seiner Entscheidung vom 19. Juli 1999 eingehalten. Das Gericht hatte darin einige Bestimmungen des G10 im Bereich der strategischen Fernmeldeaufklärung durch den Bundesnachrichtendienst für verfassungswidrig erklärt (s. 18. TB Nr. 16.1.1). Die Bundesregierung hat das Gesetzgebungsverfahren dazu genutzt, über die Vorgaben des Gerichts hinaus weitere Änderungen im G10-Bereich zu erreichen.

Das G10 enthält neben Änderungen zur strategischen Fernmeldekontrolle auch einige datenschutzrechtlich erfreuliche Verbesserungen, wie die deutliche Stärkung der parlamentarischen Kontrolle der Tätigkeit der Nachrichtendienste, weiter reichende Pflichten zur Löschung von Daten und die Einbeziehung auch der Individualanordnung nach § 3 G10 in die Berichtspflicht des Parlamentarischen Kontrollgremiums an den Deutschen Bundestag (§ 14 Abs. 1 Satz 2 G10).

Allerdings ist die Forderung der Datenschutzbeauftragten des Bundes und der Länder in der Entschließung der 61. Datenschutzkonferenz (s. Anlage 12), die neuen Regelungen zur Erweiterung der Überwachungsbefugnis auf Einzeltäter und lose Gruppierungen (§ 3 Abs. 1 Nr. 6 G10), zu Parteienverbotsverfahren (§ 4 Abs. 3 Nr. 3 G10), zur Verwendung von G10-Erkenntnissen bei Gefahren für Leib oder Leben einer Person im Ausland (§ 8 G10) und zu Spontanübermittlungen an den BND (§ 8 Abs. 2 BND-Gesetz) zu befristen und einer wirksamen und umfassenden Erfolgskontrolle (Evaluation) zu unterziehen, nicht in dieser Weise aufgegriffen worden. Der Gesetzgeber hat gleichwohl die Bundesregierung in einer Protokollnotiz aufgefordert, ihn nach Ablauf von zwei Jahren nach In-Kraft-Treten der Gesetzesänderungen „über die mit der Novellierung gemach-

ten Erfahrungen, insbesondere unter dem Gesichtspunkt des Datenschutzes“, zu unterrichten.

Vor dem Hintergrund, dass der Gesetzgeber nunmehr im Terrorismusbekämpfungsgesetz vom 9. Januar 2002 eine Evaluierungsverpflichtung vor allem bezüglich der neuen Befugnisse der Nachrichtendienste statuiert hat (s. o. Nr. 2.3.1), sehe ich dieser Unterrichtung mit Interesse entgegen.

19.3 Quellenschutz und datenschutzrechtliche Kontrolle – ein Konflikt, der sich lösen lässt

Mit dem BfV habe ich vor Jahren ein Verfahren vereinbart, wie die Interessen des BfV an einer Geheimhaltung nachrichtendienstlicher Verbindungen mit meiner umfassenden Kontrollbefugnis in Einklang gebracht werden können. Danach verwehrt das BfV meinen Mitarbeitern eine Einsichtnahme in quellengeschützte Unterlagen nur dann, wenn aus den Unterlagen direkt auf eine Quelle geschlossen werden kann (s. 18. TB Nr. 14.2).

Die Frage der Einsichtnahme in operative Quellenakten und Quellenschutz habe ich auch mit dem BND im Rahmen eines Kontrollbesuchs im Jahre 2001 erörtert. Der BND hat hierzu unter anderem erklärt, dass der Vertrauensschutz sowohl im Rahmen bereits bestehender nachrichtendienstlicher Verbindungen als auch im Hinblick auf neu aufzubauende Kontakte zu Zielpersonen ein unverzichtbares und prägendes Element jeglicher nachrichtendienstlicher Arbeit mit menschlichen Quellen sei. Zu bedenken sei in diesem Zusammenhang aber auch das Schutzinteresse des BND selbst an den operativen Akten (opAkten).

Ein Vergleich mit den beim BfV geführten Akten sei nicht möglich. Die opAkten des BND seien anders aufgebaut; zudem werde dort auch nicht zwischen Sach- und Personenakten unterschieden. In der überwiegenden Mehrzahl aller opAkten ließe sich aus dem Aktenzusammenhang direkt auf die menschliche Quelle schließen.

Ich verkenne zwar nicht die unterschiedliche Ausgangslage beim BND im Vergleich zum BfV. Es muss aber auch für den BND ein vernünftiger Weg gefunden werden, der den Notwendigkeiten – Kontrolle durch mich und Quellenschutz – Rechnung trägt. Die bisherige Argumentation des BND und dessen Lösungsvorschläge, auf die ich aus Gründen der Geheimhaltung hier nicht näher eingehen kann, haben mich nicht überzeugt. Ich werde dieses Thema im Rahmen künftiger Kontrollbesuche erneut aufgreifen und darauf drängen, dass auch hier ein Kompromiss zwischen den berechtigten Interessen des BND und meinem gesetzlichen Auftrag gefunden wird.

19.4 Datenschutzrechtliche Kontrollen – neben alt bekannten Themen auch neue Probleme

Im Berichtszeitraum habe ich die Verarbeitung personenbezogener Daten in mehreren Fachdateien des BND kontrolliert. Hierzu wurde jeweils nach einem Zufallsprinzip eine Anzahl von Datensätzen ausgewählt. Bei den Kontrollen habe ich hinsichtlich der Speicherung personenbezogener Daten keine nennenswerten datenschutzrechtlichen Verstöße festgestellt.

Probleme haben sich aber in anderen Bereichen gezeigt:

– Nach § 5 Abs. 1 BNDG i. V. m. § 12 Abs. 3 BVerfSchG hat der BND bei jeder Einzelfallbearbeitung und nach festgesetzten Fristen, spätestens nach fünf Jahren zu prüfen, ob gespeicherte personenbezogene Daten zu berichtigen oder zu löschen sind. Hierzu wird in den Dateien zu jedem Datensatz ein Wiedervorlage-Datum gesetzt und der Datensatz zum jeweiligen Wiedervorlage-Termin vorgelegt. Bei der Kontrolle einer Fachdatei habe ich jedoch festgestellt, dass bei der Regelüberprüfung nach fünf Jahren erhebliche Mängel bestehen. Die zu überprüfenden Datensätze werden zum Überprüfungszeitpunkt zwar vorgelegt, eine individuelle Prüfung auf Richtigkeit und Erfordernis der weiteren Speicherung scheint aber in der Regel nicht durchgeführt zu werden. Vielmehr wird nach meinen Feststellungen in vielen Fällen das Wiedervorlage-Datum ohne nähere Prüfung um weitere fünf Jahre verlängert.

  Der BND räumte ein, die Überprüfungen wegen des damit verbundenen hohen Arbeits- und Zeitaufwandes nicht immer tagesaktuell durchführen zu können. Den Vorwurf der fehlenden Einzelfallprüfung wies er allerdings zurück. Dies deckt sich jedoch nicht mit meinem bei dem Kontrollbesuch gewonnenen Eindruck und den Gesprächen, die hierbei mit den verantwortlichen Mitarbeitern des BND geführt wurden.

  Die hohe Arbeitsintensität, die nach Aussage des BND an personelle Kapazitätsgrenzen stößt – am Tage meines Kontrollbesuchs wurden 36 zu überprüfende Datensätze angezeigt –, kann den BND aber nicht von der gesetzlichen Verpflichtung des § 5 BNDG i. V. m. § 12 Abs. 3 BVerfSchG entbinden. Ich habe diesen daher aufgefordert, die Mitarbeiter erneut und mit Nachdruck auf diese gesetzliche Verpflichtung hinzuweisen und anzuhalten, bei jeder Einzelfallbearbeitung und bei den regelmäßigen Wiedervorlage-Terminen zeitnah eine „echte“ Überprüfung vorzunehmen.

  In diesem Zusammenhang warf der BND zum wiederholten Male die Frage auf, ob die fünfjährige Überprüfungsverpflichtung für einen Auslandsnachrichtendienst überhaupt zweckmäßig sei. Der Gesetzgeber hat jedoch in den vorgenannten Vorschriften eine eindeutige Regelung getroffen, deren Beachtung sich der BND aus reinen Zweckmäßigkeitserwägungen nicht entziehen kann.

– Organisatorische Änderungen und neuere Entwicklungen in der DV-Anwendung haben den BND dazu veranlasst, bisherige Dateianwendungen in einigen Bereichen auf neue Systeme umzustellen. Diese Umstellung bedingt u. a., Daten aus bisherigen Dateien in die neuen Systeme zu überführen. Auf die alten Dateien besteht nur noch lesender Zugriff. Bei der Überführung der Daten in die neuen Dateien habe ich einen erheblichen Arbeitsrückstand festgestellt. Laut BND würde das Fehlen erfahrenen Personals und der hohe Zeitaufwand – es dauere bis zu einem Arbeitstag pro Datensatz, z. B. unterschiedliche Schreibweisen von Personen in Übereinstimmung zu bringen, bevor ein entsprechender Datensatz in die neue Datei überspielt werden könne – bedingen, dass diese Altdatenbereinigung noch einige Zeit in Anspruch nehmen würde. Der BND äußerte jedoch die Erwartung, diese Probleme bis Ende 2004 beheben zu können.

Der vom BND seit Jahren immer wieder gegebene Hinweis auf seine personellen Engpässe kann an seiner Verpflichtung, gesetzlich vorgeschriebene Überprüfungs- und Bereinigungsarbeiten zeitnah bzw. in einem vertretbaren und angemessenen Zeitrahmen durchzuführen, nichts ändern. Ich habe daher den BND gebeten, die rückständigen Bereinigungsarbeiten in dem kontrollierten Bereich bis zu dem vorgenannten Zeitpunkt abzuschließen.

– Im Zusammenhang mit der Kontrolle einer Fachdatei hat der BND seine Absicht mitgeteilt, einer Behörde außerhalb des BND personenbezogene Daten im Wege der Online-Übermittlung zur Verfügung zu stellen. Gegen diese Absicht habe ich datenschutzrechtliche Bedenken geäußert. Zwar ist nach § 10 BDSG die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, zulässig. Jedoch ist die Anwendung dieser Vorschrift durch § 11 BNDG ausgeschlossen. Ich halte daher einen Online-Zugriff von Drittstellen auf personenbezogene Daten in BND-Dateien wegen der Nichtanwendbarkeit des § 10 BDSG und des Fehlens einer spezialgesetzlichen Vorschrift im BNDG grundsätzlich für unzulässig. Dies gilt im Übrigen auch für die Datenbestände der anderen Nachrichtendienste.

  Das Bundeskanzleramt und der BND halten dagegen eine Online-Übermittlung in bestimmten Fällen für erforderlich und auch zulässig. § 11 BNDG sei nach seiner Entstehungsgeschichte nicht dahin zu verstehen, dass dem BND die in § 10 BDSG beschriebene Möglichkeit der Datenübermittlung verboten wäre. § 11 BNDG stelle lediglich klar, dass die für den BND geltenden Spezialvorschriften nach dem BNDG den Umgang mit personenbezogenen Daten besonders regeln und die einschlägigen Spezialvorschriften den korrespondierenden Normen des BDSG vorgehen würden.

  Dieser Auffassung konnte ich mich auch in einer gemeinsamen Besprechung mit dem Bundeskanzleramt und dem BND nicht anschließen. Denn bei der Übermittlung personenbezogener Daten im Wege des automatisierten Abrufs handelt es sich um eine besondere Art der Übermittlung, bei der u. a. die nach § 9 BNDG erforderliche Einzelfallprüfung entfällt. Mit § 11 BNDG hat der Gesetzgeber jedoch eindeutig geregelt, dem BND – ebenso wie dem BfV nach dem BVerfSchG und dem MAD nach dem MADG – diese besondere Übermittlungsart ohne Einzelfallprüfung nicht einzuräumen.

  Das Bundeskanzleramt wies hingegen darauf hin, dass ein Vergleich mit dem BfV und dem MAD in dieser Frage irreführend sei, da § 1 Abs. 2 Satz 2 BNDG einen wesentlichen Unterschied zu diesen Behörden verdeutliche. Nach dieser Vorschrift richte sich die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur dann nach dem BNDG, wenn diese im Geltungsbereich dieses Gesetzes erhoben werden. In der hier in Rede stehenden Datei seien aber nahezu ausschließlich Daten erfasst, die im Ausland erhoben worden seien. Es sei unverhältnismäßig, einen automatisierten Abruf wegen des sehr geringen Anteils von im Inland erhobenen Daten generell auszuschließen.

  Diese Betrachtungsweise des Bundeskanzleramtes hätte Auswirkungen auf zahlreiche Dateien des BND mit der Konsequenz, dass personenbezogene Daten dahin gehend zu kennzeichnen wären, ob diese im Inland oder im Ausland erhoben wurden. Nur so ließe sich eindeutig feststellen, ob für den Umgang mit diesen Daten das BNDG oder das BDSG anzuwenden ist. Eine solche Abgrenzung dürfte besonders bei den durch Residenturen erhobenen Daten kaum zu realisieren sein.

  Die Diskussion über diese Rechtsfrage ist noch nicht abgeschlossen. Bemerkenswert ist jedenfalls, dass dieses Problem erstmals nach zwölf Jahren Anwendung des BNDG auftritt. Das Bundeskanzleramt hat mir eine ergänzende Stellungnahme angekündigt. Des Weiteren habe ich das Ressort, dem die Daten durch die Einrichtung eines automatisierten Verfahrens zur Verfügung gestellt werden sollen, gebeten, seinen Bedarf und die Notwendigkeit für diese besondere Übermittlungsart darzulegen.

  Beide Stellungnahmen lagen mir bei Redaktionsschluss noch nicht vor.

– Nach § 4g Abs. 2 BDSG ist dem behördlichen Datenschutzbeauftragten von der verantwortlichen Stelle eine Übersicht über alle Verfahren automatisierter Verarbeitung personenbezogener Daten zur Verfügung zu stellen. Nachdem der BND sich zunächst geweigert hatte, mir zur Ausübung meines umfassenden Kontrollrechts eine Übersicht aller beim BND geführten Dateien mit personenbezogenen Daten zu übermitteln, hat er mir schließlich Gelegenheit gegeben, in das von der behördlichen Datenschutzbeauftragten zusammengestellte Gesamtverzeichnis Einsicht zu nehmen. Hierbei habe ich eine bedenklich hohe Anzahl von Dateien festgestellt, die zwar zum Teil unter den Anwendungsbereich des BNDG fallen, darüber hinaus aber auch so genannnte Verwaltungsdateien außerhalb dieses Anwendungsbereichs, die nicht dem BNDG unterfallen. Viele dieser Dateien sind im Laufe der Zeit von Mitarbeitern des BND gewissermaßen als „Handakten“ angelegt worden und entsprechen in keiner Weise den datenschutzrechtlichen Erfordernissen. Selbst zu den Dateien für den eigentlichen Aufgabenbereich des BND liegen überwiegend keine Dateianordnungen nach § 6 BNDG i. V. m. § 14 BVerfSchG vor. Die so genannnten Verwaltungsdateien, die von den Fachabteilungen geführt werden und die u. a. auch personenbezogene Daten zu Mitarbeitern der jeweiligen Abteilung enthalten, dürften – ohne dass dies von mir bisher näher geprüft werden konnte – den Vorschriften der §§ 90 ff. Bundesbeamtengesetz nicht entsprechen.

  Ich habe den BND dringend aufgefordert, diesen rechtswidrigen Zustand zu beseitigen, den dieser selbst als unhaltbar bezeichnet. Ziel sei es, die nicht genehmigten Dateien in ein geordnetes Genehmigungsverfahren oder die dort enthaltenen Daten in bestehende genehmigte Dateien zu überführen bzw. die unzulässigen Dateien ganz zu löschen. Dies werde jedoch wegen der großen Anzahl der vorgefundenen Dateien eine geraume Zeit in Anspruch nehmen.

  Ich werde die Umsetzung dieser Bereinigungsarbeiten sorgfältig beobachten und nach einer angemessenen Zeit kontrollieren. Von einer förmlichen Beanstandung nach § 25 Abs. 1 BDSG habe ich zunächst abgesehen.

– In dem vorstehend beschriebenen Zusammenhang wurde auch folgende Problemstellung erörtert: In vielen Bereichen des Dienstes ergebe sich für den BND die Notwendigkeit zu Datenhaltungen und -sammlungen, die sich entweder wegen ihres noch vagen Analyseaspekts als noch nicht speicherfähig in gefestigten Dateistrukturen erwiesen hätten, oder die ad-hoc zur schnellen Krisenreaktion erforderlich würden. Die aktuell erforderliche und im Rahmen der Berichtspflicht nach § 12 BNDG geprägte Ad-hoc-Auftragserledigung ließe sich vielfach mit den regulären Fachdateien nicht realisieren. Es seien daher so genannnte Arbeitsdateien erforderlich, die aber die Kriterien für ein geordnetes Genehmigungsverfahren nach § 6 BNDG noch nicht voll erfüllen würden. Nachdem ich mich anhand der Präsentation von zwei vorgesehenen Ad-hoc-Arbeitsdateien von deren Zweckmäßigkeit und Notwendigkeit überzeugen konnte, wurde mit dem BND folgendes Verfahren festgelegt:

  – Für die so genannnten Ad-hoc-Arbeitsdateien wird mir der BND, soweit möglich, in einer Dateimeldung die in § 14 Abs. 1 BV erfSchG genannten notwendigen Angaben übermitteln. Hierbei ist vor allem der Zweck der Datei themenartig zu beschreiben.
  – Solche Arbeitsdateien unterliegen einer Höchstspeicherdauer von sechs Monaten. Nach Ablauf dieser Frist hat
    – bei Beendigung des Auftrags eine Überführung der Daten in bestehende, genehmigte Fachdateien zu erfolgen; ansonsten sind die Daten zu löschen

    oder

    – bei Verstetigung des Auftrages die Erstellung einer Dateianordnung zu erfolgen.

  Nach dieser Verfahrensfestlegung hat mir der BND für die beiden Dateien, die er mir zuvor zur Begründung der Notwendigkeit präsentiert hatte, entsprechende Dateimeldungen zugeleitet, die die vorgenannten Kriterien im Wesentlichen erfüllen und die nach Form und Inhalt eine gangbare Lösung darstellen. Dies könnte auch auf andere künftig erforderliche Ad-hoc-Arbeitsdateien übertragen werden.

20 Sicherheitsüberprüfung

20.1 Sicherheitsüberprüfungen nun auch bei Tätigkeiten in lebens- und verteidigungswichtigen Einrichtungen

Im Rahmen des Terrorismusbekämpfungsgesetzes vom 9. Januar 2002 (vgl. Nr. 2) als Folge der Ereignisse des 11. September 2001 wurde auch das Sicherheitsüberprüfungsgesetz (SÜG) um den so genannten vorbeugenden personellen Sabotageschutz erweitert. Bislang galt das SÜG nur für den personellen Geheimschutz, also den Umgang mit Verschlusssachen, die mit VS-vertraulich oder höher eingestuft sind. Nunmehr übt nach § 1 Abs. 4 SÜG eine sicherheitsempfindliche Tätigkeit auch aus, wer an einer sicherheitsempfindlichen Stelle innerhalb einer lebens - oder verteidigungswichtigen Einrichtung oder wer innerhalb einer besonders sicherheitsempfindlichen Stelle des Geschäftsbereichs des BMVg („Militärischer Sicherheitsbereich“) beschäftigt ist oder werden soll. Ziel dieser Gesetzesänderung ist es, sicherheitsempfindliche Stellen in lebens- und verteidigungswichtigen Einrichtungen sowohl im öffentlichen als auch im nicht öffentlichen Bereich vor so genannten Innentätern zu schützen. Der Zugang zu VS-Unterlagen ist in diesen Fällen nicht mehr Voraussetzung für eine Sicherheitsüberprüfung. Ähnliche Überprüfungen gibt es bereits nach dem Atomgesetz und dem Luftverkehrsgesetz.

Um einer uferlosen Überprüfungspraxis vorzubeugen, habe ich im Zuge des Gesetzgebungsverfahrens gefordert, den Begriff der sicherheitsempfindlichen Stelle innerhalb einer lebens- und verteidigungswichtigen Einrichtung im Gesetz klar zu definieren. Dieser Forderung ist der Gesetzgeber nachgekommen und hat mit den Definitionen in § 1 Abs. 5 SÜG eine ausreichende Klarstellung vorgenommen. Ferner habe ich gefordert, die lebens- und verteidigungswichtigen Einrichtungen in einer Verordnung enumerativ aufzuzählen. Das BMI hat inzwischen aufgrund der ebenfalls erweiterten Ermächtigung in § 34 SÜG den Referentenentwurf einer „Verordnung zur Feststellung der Behörden des Bundes mit Aufgaben von vergleichbarer Sicherheitsempfindlichkeit wie die der Nachrichtendienste des Bundes und zur Feststellung der öffentlichen Stellen des Bundes und der nicht öffentlichen Stellen mit lebens- oder verteidigungswichtigen Einrichtungen (Sicherheitsüberprüfungsfeststellungsverordnung)“ vorgelegt. In diesem Verordnungsentwurf werden die lebens- und verteidigungswichtigen Einrichtungen abschließend festgelegt. Zu einer von mir zunächst befürchteten uferlosen Überprüfungspraxis wird es nach dem vorgelegten Verordnungsentwurf nicht kommen. Der Eingriff in das Persönlichkeitsrecht wird durch die überschaubare Anzahl der in dem Verordnungsentwurf festgeschriebenen Einrichtungen und die im Gesetz festgelegte Beschränkung auf eine einfache Sicherheitsüberprüfung, bei der z. B. die Einbeziehung des Ehegatten oder Lebenspartners nicht vorgesehen ist, in einem vertretbaren Rahmen gehalten. Zudem sind solche Überprüfungen stets nur mit der Zustimmung des Betroffenen möglich.

Bei Redaktionsschluss war die Verordnung noch im Stadium des Referentenentwurfs.

20.2 Luftverkehrsgesetz und Luftverkehrs-Zuverlässigkeitsüberprüfungsverordnung der neuen Gefährdungssituation angepasst

Mit dem ersten Sicherheitspaket (s. Nr. 2.2.1) wurde – als umgehende Reaktion auf die Ereignisse vom 11. September 2001 – nach jahrelanger Vorbereitung (vgl. 16. TB Nr. 17.2) die Luftverkehrs-Zuverlässigkeitsüberprüfungsverordnung (LuftVZÜV) vom 8. Oktober 2001 (BGBl. I S. 2625) erlassen. Dabei handelt es sich im Wesentlichen um den Entwurf, der bereits im Mai 2000 dem Bundesministerium für Verkehr, Bau- und Wohnungswesen vorlag.

Erst in einem zweiten Schritt wurde mit dem Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (s. Nr. 2.2.3) die auch von mir kritisierte Ermächtigungsnorm des § 29d Luftverkehrsgesetz (LuftVG) in eine normenklare Rechtsgrundlage umgewandelt. Diese Vorschrift und dazu die §§ 19b, 20a und 32 Abs. 2b LuftVG enthalten nunmehr – der Wesentlichkeitstheorie des Volkszählungsurteils entsprechend – die Regelungen, die durch den Gesetzgeber selbst zu erfolgen haben. Dies sind alle Tatbestände, die wesentliche Rechte des Betroffenen bei der Verarbeitung seiner Daten berühren. An

der Vorbereitung des nunmehr geltenden Textes war ich im August 2001 auf Arbeitsebene intensiv beteiligt. § 29d LuftVG regelt vor allem, dass zum Schutz vor Angriffen auf die Sicherheit des Luftverkehrs die Zuverlässigkeit verschiedener Personengruppen, die in Ausübung ihrer beruflichen Tätigkeit nicht nur gelegentlich Zugang zu Flugsicherheitsbereichen haben, zu überprüfen ist. Die Zuverlässigkeitsüberprüfung entfällt, wenn der Betroffene im Inland innerhalb der letzten zwölf Monate einer zumindest gleichwertigen Überprüfung unterzogen worden ist und keine Anhaltspunkte für seine Unzuverlässigkeit vorliegen oder der Betroffene der Sicherheitsüberprüfung nach § 9 Sicherheitsüberprüfungsgesetz (SÜG) oder nach § 10 SÜG unterliegt. Im Rahmen der Überprüfung darf die zuständige Luftfahrtbehörde nach § 29d Abs. 2 LuftVG

- die Identität des Betroffenen prüfen;
- Anfragen bei den Polizei- und Verfassungsschutzbehörden der Länder stellen;
- beim Bundeskriminalamt, dem Bundesamt für Verfassungsschutz, dem Bundesnachrichtendienst, dem Militärischen Abschirmdienst und dem Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR Informationen einholen;
- eine unbeschränkte Auskunft aus dem Bundeszentralregister erhalten;
- soweit im Einzelfall erforderlich, Anfragen bei den Flugplatz-, Luftfahrt- und Flugsicherungsunternehmen stellen;
- den gegenwärtigen Arbeitgeber des Betroffenen nach dort vorhandenen, für die Beurteilung der Zuverlässigkeit bedeutsamen Informationen fragen. Darüber hinaus darf sie bei Zweifeln an der Zuverlässigkeit des Betroffenen zur Behebung dieser Zweifel erforderliche Auskünfte von Strafverfolgungsbehörden einholen.

Die Überprüfung bedarf der Zustimmung des Betroffenen. Über sein Verweigerungsrecht nach § 29 Abs. 4 Satz 4 LuftVG ist er vorher zu belehren. Nicht zu verkennen ist jedoch, dass die Zustimmung kaum verweigert werden kann, sollen berufliche Nachteile vermieden werden. Jedenfalls ist dem Betroffenen vor der Entscheidung der Luftfahrtbehörde Gelegenheit zu geben, sich zu den eingeholten Auskünften zu äußern, soweit diese Zweifel an seiner Zuverlässigkeit begründen und Geheimhaltungspflichten nicht entgegenstehen. Dabei ist der Betroffene nach § 29d Abs. 4 Satz 3 LuftVG verpflichtet, wahrheitsgemäße Angaben zu machen und ihm nachträglich bekannt werdende, für die Überprüfung bedeutsame Tatsachen unverzüglich anzuzeigen. In § 29d Abs. 5 LuftVG ist die Zweckbestimmung der Verarbeitung und Nutzung geregelt.

Aufgrund der neuen Regelungen im LuftVG wurden – in erster Linie klarstellende – Änderungen der LuftVZÜV erforderlich. Darüber hinaus geht es u. a. um die Erweiterung des zu überprüfenden Personenkreises. Hier kam es im Rahmen der Länderbeteiligung und der Beteiligung der Verbände der Luftfahrt zu Diskussionen. So wurden z. B. die Einbindung der Luftfahrtunternehmen als Arbeitgeber in die Durchführung der Zuverlässigkeitsüberprüfung als hoheitliche Maßnahme kritisiert und darin auch datenschutzrechtliche Probleme gesehen. Weiter wurde die neue Regelung, wonach die Zuverlässigkeit auch dann versagt werden kann, wenn der Betroffene seiner Mitwirkungspflicht nicht oder nicht ausreichend nachkommt und daher die entsprechenden Grundlagen für die Überprüfung fehlen, als rechtswidrig bezeichnet. Diese Regelung sei von der Ermächtigungsgrundlage des § 29d LuftVG nicht umfasst; die Mitwirkungspflicht gehe zu weit.

Eine Reaktion der Bundesregierung lag bis Redaktionsschluss noch nicht vor.

20.3 Durchführung von datenschutzrechtlichen Kontrollen – erfreulich hoher datenschutzrechtlicher Standard

Nach dem Sicherheitsüberprüfungsgesetz (SÜG) ist eine Person, die mit einer sicherheitsempfindlichen Tätigkeit betraut werden soll, zuvor einer Sicherheitsüberprüfung (SÜ) zu unterziehen. Zuständig für die SÜ ist grundsätzlich die Behörde, die einer Person eine sicherheitsempfindliche Tätigkeit zuweisen, übertragen oder sie dazu ermächtigen will. Mitwirkende Behörde, d. h. die Behörde, die die SÜ durchführt, ist das BfV bzw. im Geschäftsbereich des BMVg der MAD. Der BND, das BfV und der MAD sind für ihre eigenen Bediensteten zugleich zuständige und mitwirkende Behörde.

Im Berichtszeitraum habe ich das Verfahren nach dem SÜG beim BND (Nachkontrolle), MAD, BfV (als mitwirkende Behörde), AA und bei zwei Unternehmen kontrolliert.

20.3.1 BND (Nachkontrolle)

Bei einer Kontrolle im Jahre 2000 hatte ich bemängelt, dass auch mehr als fünf Jahre nach In-Kraft-Treten des SÜG Abschlussberichte der SÜ noch vollständig als recherchefähiger Text in der „SÜ-Datei“ des BND gespeichert waren (s. 18. TB Nr. 17.2). Der BND hat hierzu mitgeteilt, dass die seit dem 1. April 1994 eingestellten Langfassungen der Abschlussberichte zum 31. Mai 2001 gelöscht und durch entsprechende Kurzfassungen ersetzt worden seien. Hiervon konnte ich mich bei einer Nachkontrolle im Jahre 2002 überzeugen. Dagegen war eine solche Bereinigung bei den Abschlussberichten, die vor In-Kraft-Treten des SÜG gespeichert worden waren, weitestgehend noch nicht erfolgt; sie sollte nach Aussage des BND im Einzelfall bei der laufenden Bearbeitung erfolgen. Zur beschleunigten Aufarbeitung dieser Berichte sollten nach Angaben des BND personalverstärkende Maßnahmen ergriffen werden. Hierzu ist es jedoch – nicht zuletzt vor dem Hintergrund der Ereignisse des 11. September 2001 – bislang nicht gekommen. Ich habe gegenüber dem BND erklärt, dass ich für die personellen Probleme, gerade nach den Terroranschlägen im Jahre 2001, zwar Verständnis habe, dennoch bedürfe es nach wie vor organisatorischer und personeller Überlegungen, wie die Akten- und Datenbereinigung erfolgen soll. Die Abschlussberichte aus den Jahren vor 1994 nur im Einzelfall gelegentlich einer Sachbearbeitung zu kürzen, halte ich nach den gesetzlichen Regelungen für eine nicht ausreichende Maßnahme. Der BND hofft, eine Lösung des Problems durch eine effektive Nachbesetzung von vakanten Dienstposten – im Jahre 2002 waren in diesem Organisationsbereich nach Angaben des BND zehn von 68 Dienstposten nicht besetzt – zu erreichen.

Auch die Bereinigung von Altakten wird sich weiter verzögern. Der BND hat zwar inzwischen eine Arbeitsanweisung erlassen, die eine Liste von Unterlagen enthält, die

- bei der Aktualisierung,
- beim Abschluss einer Wiederholungsprüfung,
- bei Akteneinsicht durch berechtigte Stellen oder
- bei Abgabe an das Bereichsarchiv wegen Ausscheidens eines Mitarbeiters

zu entnehmen und zu vernichten sind. Bis auf die detaillierte Arbeitsanweisung, deren Erstellung und Inkraftsetzung ich begrüße, hat sich der Sachstand vor allem im Bereichsarchiv jedoch nicht wesentlich verändert. Nach wie vor ist nahezu der gesamte Altaktenbestand im Bereich der SÜ noch nicht bereinigt. Der BND begründet dies ebenfalls mit der angespannten Personalsituation nach dem 11. September 2001. Für diese Bereinigungsarbeiten stehe kein zusätzliches Personal zur Verfügung. Die vorhandenen Mitarbeiter seien zwar angewiesen, neben ihren eigentlichen Aufgaben im Bereich der aktuell durchzuführenden SÜ auch Altakten des Bereichsarchiv zu bereinigen. Ohne gezielte Personalverstärkung werde jedoch auch dieses Verfahren noch einen erheblichen Zeitraum beanspruchen.

Ich werde die Bemühungen des BND bei der Bereinigung seiner Altdaten- und Altaktenbestände im Auge behalten und mich nach angemessener Zeit vom Fortgang der Bereinigungsarbeiten überzeugen. Auch bei Würdigung der bestehenden personellen Engpässe sollte der BND verstärkte Anstrengungen vornehmen, diesen datenschutzrechtlich unhaltbaren Zustand so schnell wie möglich zu beseitigen.

20.3.2 MAD

Bei der Kontrolle einer MAD-Stelle (s. Nr. 18.3) habe ich auch die dort vorliegenden Aufträge im Bereich der SÜ überprüft.

Für die Einleitung der SÜ ist der jeweilige Sicherheitsbeauftragte der Dienststelle des Betroffenen zuständig. Dieser sendet die Sicherheitserklärung an die jeweils zuständige MAD-Stelle, von der sie auf Bearbeitungsreife vor geprüft wird. Eine inhaltliche Prüfung der Angaben des Betroffenen findet hier nicht statt. Die bearbeitungsreifen Sicherheitserklärungen werden anschließend dem MAD-Amt zugeleitet. Dort erfolgen die inhaltliche Prüfung sowie die routinemäßigen Anfragen nach § 12 Abs. 1 u. 2 SÜG. Die weitere Bearbeitung – z. B. Befragung des Betroffenen und von Referenz- und Auskunftspersonen – erfolgt im Auftrag des MAD-Amtes durch die MAD-Stelle, je nachdem welchem Bereich die zu befragende Person örtlich zuzuordnen ist. Bei den MAD-Stellen besteht somit kein kompletter Überblick über die Person eines Betroffenen. Es erfolgt jeweils nur eine punktuelle Bearbeitung. Zur Bearbeitung der Aufträge des MAD-Amtes werden Teile der beim MAD-Amt geführten Sicherheitsüberprüfungsakte – ggf. in Ablichtung – übersandt. Die Übersendung von Akten beschränkt sich hierbei auf die Teile, die für die Erledigung des Auftrags erforderlich sind. Nach Erledigung des Auftrags wird der Vorgang ggf. mit einer Bewertung der gewonnenen Erkenntnisse an das MAD-Amt zurückgesandt. Sämtliche Arbeitsergebnisse fließen beim MAD-Amt zusammen, das auch die abschließende Bewertung vornimmt; dort werden auch die nach dem SÜG zulässigen Daten gespeichert und die Akten aufbewahrt.

Bei der Kontrolle eines Teils der vorliegenden Aufträge habe ich keine datenschutzrechtlich bedeutsamen Verstöße festgestellt. Kleinere Mängel konnten nach Gesprächen mit den zuständigen Bearbeitern bzw. nach entsprechenden Hinweisen in meinem Prüfbericht bereinigt werden.

20.3.3 Bundesamt für Verfassungsschutz

Anlässlich einer früheren Kontrolle beim BfV im Jahre 1986 – also lange vor In-Kraft-Treten des SÜG im Jahre 1994 – hatte ich zahlreiche Verstöße gegen die damals geltenden Vorschriften festgestellt und nach dem damaligen § 20 BDSG förmlich beanstandet. Die jetzige Kontrolle hat gezeigt, dass durch das SÜG, das die SÜ erstmalig auf eine normenklare gesetzliche Grundlage gestellt hat, Rechtsklarheit und Rechtssicherheit eingetreten sind. Verstöße gegen das SÜG habe ich nur noch in wenigen Fällen festgestellt. Diese Mängel wurden nach meiner Kontrolle ausnahmslos bereinigt bzw. sollen, soweit ein gewisser Verwaltungsaufwand erforderlich ist, in einem angemessenen Zeitrahmen bereinigt werden.

Eine Auswertung der statistischen Unterlagen zeigt folgende Entwicklung:

Das BfV hat in den Jahren

1995	rd. 28 000
1998	rd. 19 000
1999	rd. 22 000 und
2000	rd. 22 000

SÜ als mitwirkende Behörde durchgeführt. Diese Übersicht zeigt, dass sich die Anzahl der SÜ nach In-Kraft-Treten des SÜG deutlich verringert hat. Seit 1999 liegt sie auf gleichem Niveau. Eine deutliche Zunahme ist allerdings nach Einführung des personellen Sabotageschutzes (s. o. Nr. 20.1) zu erwarten.

Ein wesentliches Ergebnis der Kontrolle war die Feststellung, dass die zuständigen Behörden ihrer Mitteilungspflicht über die Nichtaufnahme einer sicherheitsempfindlichen Tätigkeit oder deren Beendigung nach einem negativen Votum des BfV nicht nachgekommen sind. Diese Feststellung beruht auf der Prüfung der Fälle, in denen das BfV zu dem Ergebnis gekommen war, es liege ein Sicherheitsrisiko vor, und der zuständigen Behörde gegenüber nach § 14 Abs. 2 SÜG ein negatives Votum abgegeben hatte. Eine Nachprüfung durch das BfV, ob die zuständige Behörde dem Votum gefolgt ist oder eine abweichende Auffassung vertreten hat, fand in keinem Fall statt.

Ich habe hierzu die Auffassung vertreten, dass ein negatives Votum des BfV in jedem Fall eine Rückkoppelung des Geheimschutzbeauftragten der zuständigen Behörde mit dem BfV zur Folge haben muss. Nach § 22 Abs. 2 Nr. 2c SÜG hat das BfV die in Dateien gespeicherten sicherheitserheblichen Erkenntnisse und Erkenntnisse, die ein Sicherheitsrisiko begründen (gem. § 20 Abs. 2 Nr. 3 SÜG), unverzüglich zu löschen, sobald feststeht, dass der Betroffene die sicherheitsempfindliche Tätigkeit nicht aufnimmt oder sie nicht mehr ausübt. Dieser Verpflichtung kann das BfV aber nur nachkommen, wenn der Geheimschutzbeauftragte aus der zuständigen Behörde dem BfV eine entsprechende Mitteilung macht.

Das BMI hat meiner Auffassung zugestimmt und diese Problematik bei der Dritten Novellierung der Ausführungsvorschriften zum SÜG aufgegriffen. In den Ausführungen zu

§ 18 Abs. 5 SÜG ist nunmehr eindeutig geregelt, dass das BfV unverzüglich über das Ausscheiden oder die Nichtaufnahme der sicherheitsempfindlichen Tätigkeit zu unterrichten ist, wenn sicherheitserhebliche Erkenntnisse oder Erkenntnisse, die ein Sicherheitsrisiko begründen, vorliegen.

Neben dieser in die Zukunft gerichteten verfahrensmäßigen Verbesserung habe ich jedoch auch eine datenmäßige Bereinigung für die Vergangenheit gefordert. Das BMI hat zugesagt, eine Überprüfung all dieser Fälle durch das BfV vornehmen zu lassen. Diese Arbeiten sollten, da sie mit einem gewissen Verwaltungsaufwand verbunden sind, bis Ende des Jahres 2002 abgeschlossen sein. Ob dies der Fall ist, stand bei Redaktionsschluss nicht fest.

Die in wenigen Einzelfällen von mir festgestellten Mängel wurden nach meinen entsprechenden Hinweisen beseitigt. Hier handelte es sich im Wesentlichen um unterbliebene Löschungen einzelner Daten in Dateien, die inzwischen nachgeholt wurden.

Insgesamt wurde bei dieser Kontrolle deutlich, dass der Umgang mit personenbezogenen Daten bei den SÜ ein erfreulich hohes datenschutzrechtliches Niveau erreicht hat, das nicht zuletzt auf die klaren Regelungen des 1994 in Kraft getretenen SÜG zurückzuführen ist.

20.3.4 Auswärtiges Amt

Das AA hält eine SÜ bezüglich aller Bediensteter für erforderlich, die der so genannnten Rotation unterliegen. Dies ergebe sich aus der besonderen Aufgabenstellung des AA nach dem Gesetz über den Auswärtigen Dienst, wonach die Mitarbeiter des AA zu jeder Zeit an allen Dienstorten einsatzfähig sein müssten. An den Auslandsvertretungen seien von den entsandten Dienstkräften Querschnittsfunktionen für die gesamte Bundesregierung wahrzunehmen, die auch einen Zugang zu Verschlusssachen beinhalteten.

Da die SÜ einen erheblichen Eingriff in das Persönlichkeitsrecht darstellt, muss hier eine sorgfältige Interessenabwägung zwischen dem Geheimhaltungsinteresse des Staates und dem Persönlichkeitsrecht der Bediensteten vorgenommen werden. Ich habe mich nach ausführlichen Diskussionen der Argumentation des AA nicht verschließen können und gegen diese Praxis, die eine im Vergleich zu anderen Geschäftsbereichen außerordentlich hohe Anzahl von SÜ mit sich bringt, letztlich keine Bedenken erhoben.

Zu begrüßen ist in diesem Zusammenhang, dass das AA die Sicherheitsbereiche seiner Zentrale neu geordnet hat. Durch diese Neuordnung, die auch mit einer Rationalisierung des Verfahrens der SÜ einherging, wird künftig die Zahl der SÜ für das Personal, das nicht der Rotation unterliegt, reduziert. Dies ist ein datenschutzrechtlich erfreulicher Fortschritt.

Bei meiner Kontrolle habe ich schwerwiegende datenschutzrechtliche Verstöße nicht festgestellt. Gegen einige Handlungsweisen des AA habe ich jedoch datenschutzrechtliche Bedenken erhoben:

– In einem Einzelfall hatte sich ein abgelehnter Bewerber darüber beklagt, dass er zu der Ablehnung nicht gehört worden sei. Wie sich herausstellte, war der Bewerber jedoch tatsächlich über die Gründe, die zu der Ablehnung geführt hatten, unterrichtet worden.

  Ob allerdings in der Vergangenheit in Fällen abgelehnter Bewerber immer eine Anhörung nach § 6 Abs. 1 SÜG durchgeführt worden war, konnte zwar bei der Kontrolle nicht festgestellt werden. Das AA konnte aber auch nicht mit Sicherheit bestätigen, dass in allen Fällen die Anhörung tatsächlich durchgeführt worden ist.

  Ich habe deutlich gemacht, dass die Anhörungspflicht nach § 6 SÜG in jedem Einzelfall auch bei abgelehnten Bewerbern zu beachten ist. Für einen aufgrund eines negativen Votums abgelehnten Bewerber hat die Entscheidung des Geheimschutzbeauftragten besonders einschneidende Folgen. Ihm muss daher Gelegenheit gegeben werden, sich zu den Gründen, die zur Ablehnung geführt haben, zu äußern und diese ggf. zu entkräften.

  Das AA hat zugesagt, die Anhörung nach § 6 SÜG künftig in jedem Falle sicherzustellen.

– Bei der regelmäßig alle fünf Jahre vorzunehmenden Aktualisierung nach § 17 Abs. 1 SÜG holt das AA jeweils eine Auskunft aus dem Bundeszentralregister (BZR) ein. Die Einholung einer BZR-Auskunft gehört jedoch zu den Maßnahmen, die die mitwirkende Behörde nach § 12 SÜG trifft; sie steht dem Geheimschutzbeauftragten nicht zu.

  Das AA hat bestätigt, dass das bisherige Verfahren nicht der Rechtslage entspricht und hat diese Praxis inzwischen eingestellt.

– Die Sicherheitsakten enthielten z. T. Unterlagen, die nicht die SÜ betrafen bzw. für die sicherheitsmäßige Bewertung nicht erheblich waren. Zu diesen Unterlagen gehörten z. B.:

  – Personalbögen im Zusammenhang mit der Bewerbung;
  – Übersichten über Bewerber für ein Auswahlverfahren;
  – Vermerk über den Antrag zur Anerkennung als Kriegsdienstverweigerer;
  – Vermerke über Erkrankungen und einen Krankenhausaufenthalt;
  – Auszüge/Ablichtungen aus Beurteilungen;
  – Altersteilzeitvereinbarung;
  – Disziplinarurteil, das nach der Bundesdisziplinarordnung bereits nicht mehr Bestandteil der Personalakte sein durfte.

Das AA hatte bereits vor meiner Kontrolle damit begonnen, alle Sicherheitsakten zu überprüfen und alle Unterlagen ohne sicherheitserhebliche Relevanz aus den Akten zu entfernen. Der hierzu vom AA aufgestellte Maßnahmenkatalog wurde im Hinblick auf die festgestellten Mängel ergänzt; die bereits überprüften Akten werden anlässlich einer gelegentlichen Bearbeitung einer erneuten Überprüfung unterzogen.

20.3.5 Privatwirtschaft

In früheren Tätigkeitsberichten (s. 16. TB Nr. 17.4; 17. TB Nr. 17 und 18. TB Nr. 17.1) habe ich festgestellt, dass es bei den SÜ in Unternehmen der Privatwirtschaft keine größeren

datenschutzrechtlichen Mängel gegeben hat. Dieser datenschutzrechtlich beachtliche Standard hat sich auch bei meinen Kontrollen im Berichtszeitraum bestätigt. Kontrolliert habe ich ein größeres Unternehmen in der Schifffahrtsindustrie, bei dem eine relativ hohe Anzahl sicherheitsüberprüfter Mitarbeiter beschäftigt ist, und ein kleines mittelständisches Unternehmen im Dienstleistungsbereich. Insgesamt haben diese Prüfungen ergeben, dass die Verarbeitung personenbezogener Daten auch bei diesen Unternehmen einen erfreulichen Sicherheitsstandard aufwies. Kleinere Mängel konnten an Ort und Stelle nach entsprechenden Beratungen und Hinweisen bereinigt werden.

Erfreulich war auch festzustellen, dass die Geheimschutzbevollmächtigten, die in den Unternehmen die Aufgaben nach dem SÜG wahrnehmen, dem Datenschutz gegenüber sehr aufgeschlossen sind und offenkundig strikt auf die Einhaltung der Vorschriften des SÜG und anderer datenschutzrechtlicher Bestimmungen achten.

20.4 Ehegatten und Lebenspartner dürfen der Speicherung ihrer Daten in Dateien widersprechen

Nach § 20 Abs. 2 des Sicherheitsüberprüfungsgesetzes (SÜG) darf die mitwirkende Behörde auch Daten des in die Sicherheitsüberprüfung einbezogenen Ehegatten oder Lebenspartners in Dateien speichern. Das Bundesverwaltungsgericht hat hierzu in seinem Beschluss vom 2. April 1996 – BVerwG 1 WB 71.95 – festgestellt, dass die nach § 20 SÜG zulässige Speicherung von Daten der in die Sicherheitsüberprüfung einbezogenen Ehefrau weder gesetzlich zwingend vorgeschrieben noch unerlässlich ist. Das Gericht hat das BMVg zur Fortsetzung der Sicherheitsüberprüfung des Soldaten verurteilt, die zuvor wegen der Weigerung seiner Ehefrau, ihre Daten in Dateien des MAD speichern zu lassen, abgebrochen worden war. Über diesen Fall habe ich in meinem 16. TB (Nr. 17.1) berichtet.

Das BMI hat daraufhin die Allgemeine Verwaltungsvorschrift (AVV) zu § 5 Abs. 1 SÜG dahin gehend ergänzt, dass eine Sicherheitsüberprüfung wegen fehlender Überprüfbarkeit dann nicht durchgeführt werden kann, wenn der Ehegatte oder Lebenspartner zwar der Einbeziehung in die Sicherheitsüberprüfung zustimmt, aber einer Speicherung von Daten zu seiner Person in Dateien widerspricht. Das BMI hat damit den vor genannten Beschluss des Bundesverwaltungsgerichts in sein Gegenteil verkehrt. Im Rahmen der Anhörung zur Änderung der AVV habe ich zwar auf diesen Widerspruch hingewiesen; die AVV wurde dennoch in Kraft gesetzt.

Im Jahre 2001 wandte sich eine Petentin an mich. Sie hatte zwar zunächst unter Hinweis auf den Beschluss des Bundesverwaltungsgerichts der Speicherung ihrer Daten in Dateien widersprochen. Nachdem ihr von der zuständigen Stelle jedoch mitgeteilt worden war, dass die Sicherheitsüberprüfung ihres Ehemannes ohne ihre Einwilligung in die elektronische Speicherung ihrer Daten nicht durchgeführt werden könne, habe sie – gezwungenermaßen – der elektronischen Speicherung ihrer Daten in Dateien zugestimmt, um die Beschäftigung ihres Ehemannes nicht zu gefährden. In ihrer Eingabe hat sie um Klärung der Angelegenheit gebeten.

Das BfV, das ich als die mitwirkende Behörde um Stellungnahme gebeten hatte, vertrat die Auffassung, es könne die bereits eingeleitete Sicherheitsüberprüfung des Ehemannes unter Berufung auf die AVV des BMI zu § 5 Abs. 1 SÜG nicht weiterführen, wenn die Petentin ihre Zustimmung zur Speicherung ihrer Daten in Dateien des BfV widerrufen würde.

Daraufhin habe ich gegenüber dem BMI die Auffassung vertreten, dass sowohl die der Maßnahme zugrunde liegende Regelung in der AVV des BMI als auch der Abbruch der o. g. Sicherheitsüberprüfung des Ehemanns der Petentin mit dem Beschluss des Bundesverwaltungsgerichts nicht vereinbar seien. Das BMI hat schließlich meiner Auffassung zugestimmt und die AVV erneut geändert. Die Änderung stellt nunmehr klar, dass eine Sicherheitsüberprüfung bei einem bloßen Widerspruch des Ehegatten oder Lebenspartners gegen eine Speicherung von Daten zu seiner Person in Dateien durchgeführt werden muss. Damit ist das BMI letztlich dem Beschluss des Gerichts gefolgt.

Die bereits gespeicherten Daten der Petentin in Dateien des BfV wurden inzwischen gelöscht.

21 Mitarbeiterdatenschutz

21.1 Arbeitnehmerdatenschutzgesetz dringender denn je!

Wiederholt habe ich in meinen Tätigkeitsberichten darauf hingewiesen, dass die Schaffung eines bereichsspezifischen Arbeitnehmerdatenschutzgesetzes dringlicher denn je ist (zuletzt in meinem 18. TB Nr. 18.1).

Mehrfach hat die Bundesregierung angekündigt, dass sie unter Einbeziehung von Wissenschaft und Praxis einen Gesetzentwurf zu einem Arbeitnehmerdatenschutzgesetz vorlegen will. Ich begrüße deshalb, dass der Deutsche Bundestag von der Bundesregierung erwartet, den Gesetzentwurf so rechtzeitig in das parlamentarische Verfahren einzubringen, dass er bis zur Mitte der 15. Legislaturperiode beraten und beschlossen werden kann. Zu begrüßen ist auch, dass in der Koalitionsvereinbarung verabredet ist, „den Schutz der Daten der Arbeitnehmerinnen und Arbeitnehmer erstmals in einem eigenen Gesetz zu verankern“.

Nach meiner Auffassung sollten in diesem Gesetz folgende Grundsätze berücksichtigt werden, die sich im Datenschutzrecht bereits bewährt haben:

- Nach dem Prinzip der Datensparsamkeit dürfen personenbezogene Daten des Arbeitnehmers nur erhoben, verarbeitet und genutzt werden, wenn dies zur Begründung, Durchführung, Beendigung oder Abwicklung eines Arbeitsverhältnisses erforderlich oder sonst gesetzlich vorgeschrieben ist.
- Die Datenerhebung sollte grundsätzlich beim Arbeitnehmer selbst erfolgen; Ausnahmen sind gesetzlich zu regeln.
- Regelungen über die Einwilligung eines Arbeitnehmers oder eines Bewerbers in eine Datenerhebung müssen Klarheit darüber schaffen, dass diese nur dann als Grundlage einer Datenerhebung, -verarbeitung oder -nutzung infrage kommen können, wenn ihre Freiwilligkeit sichergestellt ist. Die Einwilligung muss demgemäß ohne Furcht vor Nachteilen auch verweigert werden können. Desgleichen dürfen allein aufgrund einer Einwilligung beispielsweise keine Gesundheitszeugnisse, Ergebnisse

von Genomanalysen oder ähnl iche Unterlagen verlangt werden, wenn sie den Rahmen des Befragungsrechts des Arbeitgebers überschreiten.

– Die strikte Zweckbindung der erhobenen Daten muss gesetzlich verankert werden. Personenbezogene Arbeitnehmerdaten dürfen nur für den Zweck, für den sie erhoben worden sind, verwendet werden. Daten, die für diesen Zweck nicht mehr erforderlich sind, sind zu löschen.

– Die Schaffung von Persönlichkeitsprofilen der Arbeitnehmer muss grundsätzlich verboten sein.

– Aus Gründen der Transparenz sind Arbeitnehmer umfassend darüber zu informieren, welche Daten zu welcher Zeit, auf welche Weise und zu welchem Zweck über sie erhoben sowie in welcher Art und W eise ausgewertet werden. Dies muss umfassende Auskunfts- und Einsichtsrechte des Arbeitnehmers einschließen.

– Die Mitbestimmungsrechte von Betriebs- und Personalräten bei der Einführung, Anwendung und bei wesentlichen Änderungen automatisierter Dateien mit personenbezogenen Daten für Zwecke der Personalverwaltung müssen gestärkt werden.

Das Gesetz muss auch Regelungen zur Nutzung von E-Mail und Internetdiensten am Ar beitsplatz enthalten (s. o. Nr. 11.16).

21.2 Personalakten: Es besteht immer noch Handlungsbedarf

21.2.1 Personalaktenführung, Personalaktenrichtlinien

Durch das Neunte Gesetz zur Änderung dienstrechtlicher Vorschriften vom 11. Juni 1992 sind mit W irkung vom 1. Januar 1993 Regelungen für die Personalakten geschaf fen worden. Bei Kontrollen und Beratungsbesuchen musste ich jedoch immer wieder feststellen, dass bei vielen Behörden den Regelungen der §§ 90 f f. Bundesbeamtengesetz nicht im vollem Umfange Rechnung getragen wird. Zur Personalaktenführung habe ich mich in meinen Tätigkeitsberichten mehrfach geäußert (s. 18. TB Nr. 18.3). Mit Schreiben vom 23. November 2001 habe ich daher das Bundesministerium des Innern (BMI) hierauf hingewiesen und gebeten, zur Verbesserung der Personalaktenführung eine „Muster - Personalaktenrichtlinie“ für die Bundesverwaltung zu erarbeiten.

Das BMI hat dazu mit Schreiben vom 30. Januar 2002 mitgeteilt, dass es angesichts der detaillierten und erschöpfenden Regelungen des Personalaktenrechts im Bundesbeamtengesetz meiner Forderung nicht entsprechen kann.

Dies bedauere ich. Allerdings begrüße ich es, dass das BMI mit Rundschreiben vom 30. Januar 2002 (s. Anlage 27) die Obersten Bundesbehörden auf die in meinen letzten Tätigkeitsberichten angeführten Vollzugsdefizite im Bereich des Personalaktenrechts hingewiesen hat. Das BMI hat in diesem Rundschreiben mehrere wiederholt verletzte Regeln der Personalaktenführung sowie insbesondere auch die Bereinigung von Personalakten und die unterschiedlichen Aufbewahrungsfristen angesprochen.

Bei künftigen Beratungs- und Kontrollbesuchen werde ich mein besonderes Augenmerk auf die Führung der Personalakten, insbesondere auch auf die Behandlung der so genannten „Vorakten“, legen.

21.2.2 Dürfen behördliche Datenschutzbeauftragte und Gleichstellungsbeauftragte Personalakten einsehen?

Im Berichtszeitraum bin ich mehrfach darauf angesprochen worden, ob behördliche Datenschutzbeauftragte und Gleichstellungsbeauftragte ein Recht auf Einsicht in Personalakten haben.

Nach In-Kraft-Treten des Änderungsgesetzes zum BDSG am 23. Mai 2001 sind durch § 4f BDSG behördliche Datenschutzbeauftragte bei Bundesbehörden nunmehr zwingend vorgeschrieben (s. o. Nr. 3.2.5). Nach § 4g BDSG hat der behördliche Datenschutzbeauftragte auf die Einhaltung des BDSG und anderer Vorschriften über den Datenschutz hinzuwirken; zu diesen Vorschriften gehören auch die §§ 90 bis 90g Bundesbeamtengesetz, in denen der Umgang mit Personalakten geregelt ist. Aufgrund der neuen Rechtslage hat der behördliche Datenschutzbeauftragte nunmehr ein Recht auf Einsicht in Personalakten; dies erstreckt sich auch auf die Einsichtnahme in Personaldatei en, in denen Personalaktendaten gespeichert sind.

Um den Interessen der Beschäftigten gerecht zu werden, sollte der behördliche Datenschutzbeauftragte von der Einsichtnahme absehen, wenn der Beschäftigte ihm gegenüber der Einsichtnahme widersprochen hat; dies entspricht meiner Praxis bei der Kontrolle von Personalakten.

Die Gleichstellungsbeauftragte gehört nach § 18 Abs. 1 des Gleichstellungsgesetzes der Personalverwaltung an. Im Rahmen dieser Aufgabe hat die Gleichstellungsbeauftragte ein Recht auf Einsicht in die Personalakten, soweit dies zur Wahrnehmung ihrer Aufgaben erforderlich ist; auf die Begründung zu dem Entwurf des Gleichstellungsgesetzes (Bundestagsdrucksache 14/5679) wird hingewiesen.

21.2.3 Feststellungen aus Datenschutzkontrollen

21.2.3.1 Diagnosedaten zur Vorbereitung von Mitarbeitergesprächen bei der Deutschen Post AG

Durch mehrere Eingaben bin ich darauf aufmerksam geworden, dass die Deutsche Post AG über erkrankte Mitarbeiter Diagnosedaten zur Vorbereitung von Personalmaßnahmen erhebt, verarbeitet und nutzt. Bei der datenschutzrechtlichen Kontrolle einer Niederlassung habe ich in diesem Zusammenhang folgendes feststellen müssen:

Bei der Niederlassung wurden „fürsor gliche Mitarbeitergespräche“ mit erkrankten Mitarbeitern (hauptsächlich Postzustellern) durch Fachvor gesetzte geführt. Zur V orbereitung dieser Gespräche wurden erkrankte Mitarbeiter von der Fachabteilung der Niederlassung teilweise zu Hause angerufen und zu ihrer Erkrankung befragt. Manche Mitarbeiter wurden auch bedrängt, die sie behandelnden Ärzte von der ärztlichen Schweigepflicht zu entbinden, um „sich unmittelbar mit dem Arzt über die gesundheitlichen Probleme zu unterhalten“. Die so zusammengetragenen Diagnosedaten wurden schriftlich festgehalten. In den vor gefundenen Unterlagen fanden sich u. a. folgende V ermerke, die Aussagen zur gesundheitlichen Situation enthielten: „Krankenhaus:

u. a. Nierensteine, Rückenprob leme“, „Atemnot, Aller gie, Arzt anrufen“, „Rehaklinik Schwarzwald, T elefonnummer ...., Operation vor fünf Wochen“, „Kalkablagerungen, sieben Schleimbeutel, Entzündung Schultergelenk“, „hat Herzklappenfehler“, „gerüchteweise: strebt Dienstunfähigkeit an“.

Anhand der Aufzeichnungen wu rde entschieden, welcher Mitarbeiter zu einem Mitarbei tergespräch eingeladen werden sollte. Zur weiteren V orbereitung eines solchen Mitarbeitergespräches hat die Fachabte ilung dann die entsprechenden Personalakten hinzugezogen und auszugsweise für das zu führende Gespräch fotokopiert. In den Unterlagen der Fachabteilung fanden sich u. a. Kopien eines vollständigen ärztlichen Gutachtens des zuständigen Betriebsarztes mit medizinischen Befunden und Diagnosedaten sowie die Meldung eines Arbeits- oder Dienstunfalles an die Unfallkasse Post und Telekom mit sensiblen personenbezogenen Daten, wie z. B. die Art der Verletzung eines Mitarbeiters. Darüber hinaus fanden sich im Büro der Fachabteilung auch Ordner mit entsprechenden Unterlagen aus Vorjahren.

Nach einem auf der beschriebenen Basis durchgeführten Mitarbeitergespräch wurde dessen Inhalt in einem V ermerk festgehalten und zur Personalakte verfügt. Die V ermerke wurden als Zweitschrift auch in der Fachabteilung der Niederlassung verwahrt und enthielten ebenfalls Angaben über Erkrankungen, (z. B. „Nervenentzündung“, „Knorpelschaden an den Knien“, „Thrombose linkes Bein“). T eilweise wurden sie auch per E-Mail über ei nen großen Verteiler (wie z. B. an weitere Fachabteilungen bis zur dortigen Sachbearbeiterebene, an Fachvorgesetzte in den Zustellstützpunkten der Postzusteller sowie an den Betriebsrat) versandt und von den jeweiligen Empfängern eb enfalls wieder per E-Mail an weitere Personen verschickt, sodass – unabhängig von der rechtlichen Zulässigkeit – im Nachhinein nicht mehr nachzuvollziehen war, wer über die Vermerke mit solch sensiblen Personalaktendaten verfügt bzw. davon Kenntnis erhalten hat.

Diese Erhebung von Krankheitsdaten habe ich hinsichtlich der Beamten als unzulässig gemäß § 90 Abs. 3 und 4 Bundesbeamtengesetz (BBG) bewertet; hinsichtlich der anderen Arbeitnehmer verstößt sie gegen den Grundsatz von T reu und Glauben (§ 12 Abs. 4, § 28 Abs. 1 Satz 1 Nr . 1 und Satz 2 BDSG). Die Abfrage von Krankheitsdaten beim Betroffenen selbst steht mit de m Fragerecht des Arbeitgebers nicht in Einklang. Dies muss erst recht für die Datenerhebung bei Dritten (Ärzten, Klin iken etc.) gelten. Zur Erhebung von Diagnosedaten durch Arbeitgeber habe ich mich bereits in meinem 15. TB (Nr. 9.3.2) geäußert.

Der Zugang zu den Personalakten durch die Vorgesetzten einer Fachabteilung stellt auch einen Verstoß gegen § 90 Abs. 3 BBG dar, der den Zugang zur Personalakte nur für Beschäftigte zulässt, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist. Die von den Mitarbeitern erbetene Schweigepflichtentbindungserklärung für die sie behandelnden Ärzte verstößt gegen die Vorgaben des § 90 Abs. 4 i. V . m. §§ 46a, 42 Abs. 1 Satz 3 BBG hinsichtlich der Beamten und gegen die §§ 13 Abs. 1, 12 Abs. 4 i. V. m. § 28 Abs. 1 Satz 2 BDSG hinsichtlich der weiteren Arbeitnehmer. Die Versendung der Vermerke über die geführten Mitarbeiter gespräche per E-Mail an Unbefugte habe ich als eine V erletzung des Personalaktengeheimnisses (§ 90 Abs. 1 Satz 3, Abs. 3 BBG) bewertet und die zahlreichen Verstöße insgesamt gemäß § 25 Abs. 1 BDSG beanstandet.

Nach einem anschließenden Schriftwechsel sowie zahlreichen, ergänzenden mündlichen Erörterungen hat die Deutsche Post AG nunmehr mitget eilt, dass die vor genannten Mängel abgestellt worden sind und die Befugnisse von Fachabteilungsleitern hinsichtlich der W ahrnehmung von Aufgaben der Personalverwaltung klar geregelt werden. Ein erfreulicher Abschluss nach langen Mühen.

21.2.3.2 Wehrbereichsverwaltung: Gesetzliche Vorgaben zur Personalaktenführung ignoriert

Meine Kontrollen im vorherigen Berichtszeitraum haben mich veranlasst, bei weiteren großen Behörden der Bundesverwaltung die Führung von Personalakten zu überprüfen. Das BMVg hat die mit dem Neunten Gesetz zur Änderung dienstrechtlicher Vorschriften zum 1. Januar 1993 in Kraft getretenen umfassenden Neuregelungen zur Form und zum Inhalt von Personalakten für seinen Zuständigkeitsbereich bereits im Dezember 1993 in eine Personalaktenrichtlinie umgesetzt.

Das Beispiel einer von mir kontrollierten W ehrbereichsverwaltung zeigt, dass auch hier die Umsetzung der gesetzlichen Regelungen des Bundesbeamtengesetzes (§§ 90 f f. BBG) offenbar große Schwierigke iten bereitet (vgl. auch Nr. 21.2.1). Bemerkenswert war allerdings, dass die Umstellung der Personalakten der Arbeitnehmer und Angestellten in der Wehrbereichsverwaltung durch die jeweiligen Personalsachbearbeiter bereits erfolgt war. Für die Personalaktenführung der Tarifkräfte hat das BMVg in der o. a. Personalaktenrichtlinie die §§ 90 f f. BBG für entsprechend anwendbar erklärt. Im Einzelne n festgestellte Mängel, wie z. B. in der Personalakte abgelegte z. T. sehr alte Auskünfte aus dem Bundeszentralregister, wurden noch vor Ort aus der Personalakte entfernt und deren Beseitigung auch aus anderen Personalakten zugesagt.

Die Führung der Personalakten der Beamten entsprach dagegen in keinem der geprüften Fälle den gesetzlichen V orgaben bzw. der Personalaktenrichtlinie des BMVg. Meine Feststellungen gleichen weitgehend den ausführlichen Darstellungen in meinem letzten Tätigkeitsbericht (s. 18. TB Nr. 18.3). Zum Beispiel:

- Unvollständige Inhaltsverzeichnisse (§ 90 Abs. 2 Satz 4 BBG),
- Personalaktendaten mehrerer Mitarbeiter in einer Personalakte (§ 90 Abs. 1 Satz 1, 2. Halbsatz BBG),
- Ablage von allgemeinem Schriftverkehr (§ 90 Abs. 1 Satz 2, 2. Halbsatz BBG).

Auch die Führung der eingesehenen T eilakten hatte erhebliche Mängel. So wurden als so genannte „Vorakten“ Personalakten aus früheren V erwendungen bei anderen Dienststellen des BMVg geführt und die eingesehenen T eilakten „Abwesenheit“ enthielten Unterlagen, wie z. B. Arbeitsunfähigkeitsbescheinigungen, Urlaubsbewilligungen und weitere Unterlagen, die lückenlos alle Abwesenheiten von Beginn des Beschäftigungsverhältnisses bis zum Kontrollzeitpunkt belegten.

So genannte „Restakten“ oder auch „Ruhestandsakten“ über einzelne Beamte enthielten umfangreiche Personalaktendaten, wie z. B. arbeitsmedizinische Bescheinigungen, Abwesenheitsunterlagen, Schriftverkehr über Reaktivierungswünsche, Schriftwechsel mit dem Petitionsausschuss des Deutschen Bundestages sowie weitere Kopien aus der Personalgrundakte. Nach den Vorgaben des BMVg werden die Personalakten von Ruhestandsbeamten mit der Versetzung in den Ruhestand an die für die Versorgung zuständige Wehrbereichsverwaltung abgegeben. Ich halte es für grundsätzlich ausreichend, wenn die Dienststelle, bei der die Personalakte zuletzt geführt wurde, lediglich noch das Schreiben behält, das die Abgabe der Personalakte dokumentiert. Eine Aufbewahrung weiterer Unterlagen ist für die Aufgabenerfüllung der ehemaligen Dienststelle nicht mehr erforderlich und damit unzulässig.

Die zahlreichen Verstöße gegen die gesetzlichen Vorgaben der §§ 90 ff. BBG habe ich gemäß § 25 Abs. 1 BDSG beanstandet. Das BMVg hat mir eine Beseitigung der festgestellten Mängel versichert und eine Prüfung der Personalaktenrichtlinie auf missverständliche Regelungen zugesagt. Ich werde zu gegebener Zeit das Ergebnis der Umsetzung erneut überprüfen.

21.2.3.3 Personalaktenführung in der Bundesanstalt für Arbeit soll jetzt den gesetzlichen Vorgaben angepasst werden

In meinem letzten Tätigkeitsbericht (Nr. 18.3) habe ich über zahlreiche schwerwiegende Verstöße bei der Personalaktenführung in der Hauptstelle der Bundesanstalt für Arbeit (BA) berichtet. Nachdem sich die BA in der zurückliegenden Zeit nur langsam bereit erklärt hatte, meinen Anregungen und Forderungen zu folgen, wurde in mehreren Beratungsgesprächen, an denen zuletzt auch das Bundesministerium für Wirtschaft und Arbeit als Rechtsaufsicht beteiligt war, nunmehr vereinbart, meine Forderungen in vollem Umfang umzusetzen. Meinen Mitarbeitern wurde auch zugesagt, die bisher aufgrund der umfangreichen organisatorischen Veränderungen nicht erfolgte Stellungnahme zu meiner damaligen Beanstandung nunmehr kurzfristig nachzureichen.

Die BA wird ein Personalentwicklungskonzept erstellen. Die damit zusammenhängenden Personalmaßnahmen werden es erforderlich machen, alle Personalakten in einem Zeitraum von fünf Jahren „zu bewegen“, was eine günstige Gelegenheit für die geforderte Umstellung darstellt. Dabei soll auch ein System entwickelt werden, das einen Überblick über die jeweilige Zahl der umgestellten Personalakten ermöglicht. Für die Umstellung aller ca. 100 000 Personalakten wird nach Darstellung der BA ein Zeitraum von etwa fünf Jahren benötigt.

Ich werde die Umstellung der Personalakten auf dieser Grundlage weiter im Auge behalten und mich anhand der dargelegten Konzepte über den weiteren Fortgang unterrichten lassen.

21.3 Automatisierte Personaldatenverarbeitung

21.3.1 Moderne Technik erobert Personalstellen

Die Tätigkeit in den Personalabteilungen der Bundesbehörden wird zunehmend durch den Einsatz von immer leistungsfähigerer Informations- und Kommunikationstechnologie geprägt, mit deren Unterstützung Mitarbeiterdaten für Zwecke der Personalverwaltung/-wirtschaft automatisiert verarbeitet werden. Der Trend, völlig neue Systeme zu entwickeln oder Alt-Systeme neuer Technik anzupassen oder durch neue Programme zu ersetzen, hat sich im Berichtszeitraum fortgesetzt.

Neben Kontrollen der automatisierten Personaldatenverarbeitung (vgl. hierzu Nr. 21.3.4) habe ich Ministerien und Bundesbehörden verstärkt umfassend zu den hierbei zu beachtenden gesetzlichen Vorgaben beraten. Durch die mit den Bundesbehörden konstruktiv geführten Gespräche ist es mir möglich, schon frühzeitig die besonderen datenschutzrechtlichen Anforderungen an solche Systeme in der Entwicklungs- bzw. Einführungsphase einzubringen. Meine Hinweise und Empfehlungen richten sich u. a. auf die Umsetzung der gesetzlichen Vorgaben der §§ 90 ff. Bundesbeamtengesetz (BBG), insbesondere § 90g BBG in der Praxis, auf Datenumfang, Zugriffsrechte, Protokollierungen, Auswertungsmöglichkeiten, Löschungsregelungen, Ausschluss einer Verhaltens- und Leistungskontrolle, technisch-organisatorische Maßnahmen und den Inhalt von Dienstvereinbarungen oder -anweisungen hierzu.

Neben der Beratung zu sonstigen Verfahren automatisierter Verarbeitungen, etwa zur Durchführung der gleitenden Arbeitszeit (vgl. hierzu Nr. 21.3.3) oder zur Beihilfebearbeitung, liegt der Schwerpunkt bei den sehr komplexen Personalinformations-/Personalverwaltungssystemen. Insbesondere vor dem Hintergrund, dass in der Bundesverwaltung kein einheitliches System existiert oder entwickelt wird, ist die aus datenschutzrechtlicher Sicht zu begrüßende Beratung sehr zeitintensiv und erstreckt sich oftmals über mehrere Jahre. Beispiele für solche sich in der Entwicklung befindenden Systeme sind das Personalverwaltungssystem für die Bundesverwaltung für Verkehr, Bau- und Wohnungswesen sowie das IT-unterstützte Personalmanagementsystem der BfA. Die Beratungen zu beiden Systemen, die auf der Basis der Standardsoftware SAP R/3HR arbeiten (s. hierzu 18. TB Nr. 8.6.4), dauert an.

Zahlreiche Fragestellungen, die an mich herangetragen werden, betreffen darüber hinaus auch die Verarbeitung von Mitarbeiterdaten im Zusammenhang mit dem Einsatz sonstiger moderner Informationstechnologien wie Internet, Intranet, E-Mail, Telearbeit, Kosten- und Leistungsrechnung oder Telefondatenverarbeitung. Hierbei ist insbesondere der Ausschluss einer unzulässigen Verhaltens- und/oder Leistungskontrolle der Mitarbeiter von Bedeutung.

21.3.2 Travel-Management-System verbessert Dienstreisewesen

Im Berichtszeitraum hat das BMI zur Optimierung des Dienstreisewesens ein Travel-Management-System (TMS) eingeführt, mit dem der Prozess der Reiseabwicklung weitgehend elektronisch unterstützt wird. Hierbei werden personenbezogene Daten der Beschäftigten, die bei der Vorbereitung, Genehmigung, Durchführung und Abrechnung von Dienstreisen im TMS entstehen, nicht nur vom BMI und den Behörden des Geschäftsbereiches, sondern auch von den beteiligten Wirtschaftsunternehmen (etwa Reisebüro, Kreditkartenunternehmen, Fluggesellschaften) als ausge-

wählten Vertragspartnern des Auftraggebers BMI erhoben, verarbeitet oder genutzt.

Ich habe es begrüßt, dass mich das BMI im Vorfeld des Abschlusses einer entsprechenden Dienstvereinbarung mit dem Hauptpersonalrat zu den datenschutzrechtlichen Fragen um beratende Unterstützung gebeten hat. So habe ich zu dem Entwurf der Dienstvereinbarung über die elektronische Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten im Rahmen des TMS umfangreiche datenschutzrechtliche Änderungsvorschläge unterbreiten und Empfehlungen und Hinweise geben können, die berücksichtigt worden sind.

Aus datenschutzrechtlicher Sicht galt hierbei ein besonderes Augenmerk den Regelungen zur Auftragsdatenverarbeitung (§ 11 BDSG), den Zugriffsberechtigungen, zulässigen Auswertungsmöglichkeiten, vorgesehenen Datenübermittlungen, den Löschungsregelungen, der umfassenden Unterrichtung der Beschäftigten und deren Rechten, dem Ausschluss einer Verhaltens- und Leistungskontrolle der Dienstreisenden, aber auch den technisch-organisatorischen Maßnahmen (§ 9 sowie Anlage zu § 9 Satz 1 BDSG).

Das BMI hat meine Anregungen aufgegriffen und zugesagt, die Beschäftigten über alle Module des Systems im Einzelnen vor der Einführung jeweils detailliert zu unterrichten.

Es bestand Einvernehmen, dass es neben den getroffenen Regelungen der Dienstvereinbarung für eine abschließende datenschutzrechtliche Bewertung des TMS später auf die Umsetzung der dort vereinbarten datenschutzrechtlichen Bestimmungen, insbesondere der technisch-organisatorischen Maßnahmen, in der Praxis ankommen wird. Eine solche Prüfung habe ich mir vorgemerkt.

21.3.3 Automatisierte Gleitzeitverarbeitung will gut organisiert sein

Auch in diesem Berichtszeitraum haben mich zahlreiche Bundesbehörden, Personalvertretungen und die Fraktion der SPD im Deutschen Bundestag gebeten, sie bei der Einführung oder Umsetzung der gleitenden Arbeitszeit mittels elektronischer Zeiterfassungssysteme, die gem. § 75 Abs. 3 Nr. 17 Bundespersonalvertretungsgesetz der Mitbestimmung unterliegen, beratend zu unterstützen.

Die Rechtmäßigkeit der Datenerhebung, -verarbeitung und -nutzung von Mitarbeiterdaten im Rahmen eines automatisierten Zeiterfassungssystems bestimmt sich bei den Bundesbehörden nach den Vorschriften des § 12 Abs. 4 sowie § 28 Abs. 1 Nr. 1 BDSG. Ferner sind von ihnen die „Rahmengrundsätze für die gleitende Arbeitszeit in der Bundesverwaltung“ des BMI zu beachten. Die wichtigsten datenschutzrechtlichen Anforderungen lassen sich wie folgt zusammenfassen:

- Mittels automatisierter Zeiterfassungssysteme dürfen nur die Daten aufgezeichnet werden, die für die Abrechnung der Gleitzeit erforderlich sind.
- Die erfassten Daten dürfen nur den mit der Abrechnung und Kontrolle dieser Aufzeichnungen beauftragten Stellen zugänglich sein. Diese dürfen die Daten zu keinem anderen als zum Zweck der Gleitzeitberechnung und -kontrolle verarbeiten, bekannt geben oder sonst nutzen.
- Die aufgezeichneten Daten sind zu löschen, wenn ihre Kenntnis für die zulässigen Kontrollzwecke der Dienststelle nicht mehr erforderlich ist und schutzwürdige Belange des betroffenen Beschäftigten durch die Löschung nicht beeinträchtigt werden.
- Durch geeignete technische und organisatorische Maßnahmen ist eine unbefugte Kenntnisnahme der Zeitdaten durch Dritte zu verhindern.
- Die Mitarbeiter sind umfassend über das Verfahren der automatisierten Gleitzeitverarbeitung zu unterrichten, der Abschluss einer Dienstvereinbarung ist empfehlenswert.

Ein wichtiger Beratungsgegenstand war auch die Frage der Organisation von Gleitzeitstellen, insbesondere die zwischenzeitlich von mehreren Bundesbehörden und auch von meiner Dienststelle praktizierte bzw. angestrebte Ausgliederung der Gleitzeitstelle. Aus datenschutzrechtlicher Sicht halte ich eine solche Aufgabenverlagerung der Gleitzeitverarbeitung von der Beschäftigungsbehörde hin zu einer anderen Bundesbehörde (etwa dem Bundesverwaltungsamt) für eine gute Lösung.

Maßgeblich ist hierbei jedoch immer die datenschutzgerechte Organisation und Gestaltung des automatisierten Verfahrens und der Gleitzeitstelle und eine klare Abgrenzung und Festlegung, wer bei der Verarbeitung von Mitarbeiterdaten welche konkreten Aufgaben wahrnimmt und somit die Befugnisse hat, die hierfür erforderlichen Personaldaten zu verarbeiten. Dies sollte detailliert zwischen der verantwortlichen Stelle und der beauftragten Behörde (z. B. im Rahmen einer Dienstleistungsvereinbarung) geregelt werden, sich in einer Dienstvereinbarung widerspiegeln und den Mitarbeitern transparent dargestellt werden.

Ich werde auch in Zukunft der Thematik Gleitzeitverarbeitung eine besondere Aufmerksamkeit widmen.

21.3.4 Kontrollen weisen große Mängel auf – Kraftfahrt-Bundesamt mehrfach beanstandet

Im Berichtszeitraum habe ich zweimal das Kraftfahrt-Bundesamt (KBA), die Zentrale des Auswärtigen Amtes (AA) sowie ein Bundesgrenzschutzamt beraten und kontrolliert, insbesondere im Hinblick auf die automatisierte Personaldatenverarbeitung.

Zu den Kontrollen im KBA:

Bereits im Jahre 1994 hatte ich im KBA eine Kontrolle im Bereich der automatisierten Personaldatenverarbeitung durchgeführt und hierüber auch in meinem 15. TB (Nr. 9.7.3) berichtet.

Eine erste Prüfung im Berichtszeitraum (2001) hat gezeigt, dass das KBA entgegen den im 15. TB und auch in der Stellungnahme der Bundesregierung hierzu dargestellten Zusagen, die bereits 1994 festgestellten Mängel zu beseitigen, dies in drei Bereichen nicht umgesetzt hatte: Kein Abschluss einer Dienstvereinbarung zur Personaldatei (Personalinformationssystem), weiterhin umfangreiche, ausgefüllte Bemerkungs- und Freitextfelder und immer noch eine große Anzahl unzulässiger Dateien mit Personalaktendaten in Fachabteilungen des KBA.

Daneben habe ich zahlreiche weitere unzulässige automatisierte, aber auch manuelle Verarbeitungen von Personal-/Personalaktendaten festgestellt. So hat das KBA z. B. über Jahre hinaus alle Personalakten von Beamten, die zu einer anderen Behörde oder in den Ruhestand versetzt wurden, vor der Abgabe der (Original-)Personalakte vollständig kopiert (bis zu 200 Seiten) und dauerhaft ohne Wissen der Betroffenen im KBA aufbewahrt. Das KBA konnte mir weder eine Begründung hierfür geben noch darlegen, aufgrund welcher oder wessen Anweisung dies aufwendige Verfahren so praktiziert worden ist. Die zahlreichen (teils seit 1994 vorhandenen) Mängel des KBA im Umgang mit Personalaktendaten habe ich gemäß § 25 Abs. 1 BDSG gegenüber dem Bundesministerium für Verkehr, Bau- und Wohnungswesen (BMVBW) als einen Verstoß gegen die Regelungen der §§ 90 ff. BBG beanstandet und dringenden Handlungsbedarf aufgezeigt.

Die Umsetzung der mir vom BMVBW gegebenen Zusagen bzw. dargestellten Maßnahmen habe ich nach über einem Jahr (2002) nochmals im KBA kontrolliert. Hierbei war es mir erstmalig möglich, auch außerhalb des Personalinformationssystems im Personalreferat geführte weitere automatisierte Dateien mit Personal-/Personalaktendaten auf ihre Rechtmäßigkeit hin zu überprüfen. Diese waren mir leider auch auf meine Nachfragen hin bei der Kontrolle im Jahre 2001 nicht gezeigt worden und ihre Existenz wurde mir erst bestätigt, nachdem mir hierfür Anhaltspunkte vorlagen. Ich habe gegenüber dem BMVBW deutlich gemacht, dass ein solches Verhalten des KBA nicht im Einklang mit § 24 Abs. 4 BDSG steht. Danach sind die öffentlichen Stellen des Bundes verpflichtet, mich bei der Erfüllung meiner Aufgaben zu unterstützen. Ich habe feststellen müssen, dass diese beim Sachgebietsleiter geführten Dateien gegen zahlreiche Vorschriften des BBG und des BDSG verstoßen. Sie verletzen insbesondere die Persönlichkeitsrechte der Betroffenen, weil dort Vermerke mit auf Mitarbeiter bezogenen, subjektiven, negativen und diskriminierenden Inhalten und mit besonderen Arten personenbezogener Daten gemäß § 3 Abs. 9 BDSG (Angaben über die Gesundheit) gespeichert sind.

Neben diesen und weiteren umfangreichen neuen Datenschutzverletzungen ergab die Nachkontrolle wiederum teilweise deckungsgleiche schwere Mängel und Verstöße des KBA im Umgang mit diesen besonders sensiblen und schützenswerten Personal-/Personalaktendaten. Bestätigungen bzw. Zusagen mir gegenüber hinsichtlich einer datenschutzgerechten Verfahrensweise trafen größtenteils immer noch nicht zu bzw. waren nicht umgesetzt, was angesichts der 2001 ausgesprochenen Beanstandung völlig unverständlich ist.

Ich habe deshalb die wiederum zahlreichen festgestellten Mängel im Umgang des KBA mit Personalaktendaten gemäß § 25 Abs. 1 BDSG gegenüber dem BMVBW als einen Verstoß gegen die Regelungen der §§ 90 ff. BBG beanstandet. Darüber hinaus musste ich aufgrund der vorgefundenen erheblichen technisch-organisatorischen Mängel bei der Verarbeitung dieser Mitarbeiterdaten, insbesondere solcher mit Angaben über die Gesundheit, gem. § 25 Abs. 1 BDSG einen Verstoß gegen § 9 BDSG nebst Anlage beanstanden.

Vor dem Hintergrund der wiederholten, teilweise jahrelangen unzulässigen Datenverarbeitungen des KBA habe ich das BMVBW aufgefordert, dringend dafür Sorge zu tragen, dass die Verarbeitung von Personal-/Personalaktendaten dort zukünftig gesetzmäßig erfolgt. Hierauf werde ich ein besonderes Augenmerk legen.

Zur Kontrolle in der Zentrale des AA:

In den Personalreferaten der Zentrale des AA wird das selbstentwickelte zentrale Personalinformations-/-verwaltungssystem PEPSY eingesetzt. Daneben habe ich bei einem Kontroll- und Beratungsbesuch dort noch zahlreiche sonstige automatisierte Personaldateien mit oftmals identischem Inhalt vorgefunden, in denen Daten zu solchen Zwecken verarbeitet wurden, für die das AA PEPSY entwickelt hat.

Damit war eine einheitliche „Pflege“ der Personal-/Personalaktendaten nicht gewährleistet, mit der Gefahr, dass die Mitarbeiterdaten nicht deckungsgleich und damit teilweise unrichtig waren. Ich habe in diesem Zusammenhang auch auf das hierdurch verursachte Problem aufmerksam gemacht, die Wahrnehmung der Einsichts- und Auskunftsrechte der Beschäftigten gemäß § 90c BBG bzw. 34 BDSG sicherzustellen, und auf die erschwerte Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme durch den behördlichen Datenschutzbeauftragen gemäß § 4g Abs. 1 Nr. 1 BDSG hingewiesen.

Da es weder zu PEPSY noch zu den sonstigen automatisierten Verarbeitungen von Mitarbeiterdaten schriftliche Datenschutzregelungen/Dienstanweisungen gab, habe ich entsprechenden Handlungsbedarf aufgezeigt. Das AA hat umgehend eine solche Anweisung für die Beschäftigten in den Personalreferaten erlassen, eine sofortige Bestandsaufnahme aller Dateien mit Mitarbeiterdaten durchgeführt, deren Erforderlichkeit für die Aufgabenerfüllung der Personalreferate außerhalb von PEPSY geprüft und weitere notwendige Maßnahmen (z. B. Löschung der Daten oder Übernahme in PEPSY) durchgeführt. Zu weiteren Kontrollfeststellungen hat das AA schnellstmöglich meine datenschutzrechtlichen Empfehlungen umgesetzt und in den kurze Zeit später in Kraft gesetzten Datenschutzgrundsatz-Runderlass auch Regelungen zur Verarbeitung von Mitarbeiterdaten aufgenommen. Unter Berücksichtigung dieser Tatsachen war es mir nach § 25 Abs. 2 BDSG möglich, von einer förmlichen Beanstandung dieser Verstöße abzusehen.

Zur Kontrolle eines Bundesgrenzschutzamtes:

Im Sachgebiet Personal des geprüften Bundesgrenzschutzamtes werden zahlreiche selbstentwickelte elektronische Dateien mit Personal-/Personalaktendaten geführt. Neben den dort festgestellten und aus datenschutzrechtlicher Sicht problematischen Bemerkungsfeldern zum freien Eintrag von Texten fanden sich auch für die Aufgabenerfüllung der Personalstelle nicht (mehr) erforderliche Dokumente, aber auch komplette Dateien, die bereits erledigte bzw. abgeschlossene Vorgänge betrafen und damit unzulässig waren.

Auch in einer zu diesem Bundesgrenzschutzamt gehörenden Grenzschutzinspektion waren beim Leiter zwei Dateien mit sehr sensiblen Personalaktendaten (u. a. Beurteilungsnoten) gespeichert, deren dauerhafte elektronische Speicherung weder vorgesehen noch erforderlich war und die hätten gelöscht sein müssen. Als gravierenden Verstoß gegen die gesetzlichen Vorgaben der §§ 90 ff. BBG und gegen § 9 sowie Anlage zu § 9 Satz 1 BDSG habe ich bewertet, dass sich der Dienststellenleiter diese Dateien unter der

Bezeichnung „Heimarbeit“ vom Systemadministrator auf Diskette hatte speichern lassen, um sie anschließend auf seinem privaten PC zu Hause zu verarbeiten. Die Prüfung im Bereich der konventionellen Personaldatenverarbeitung ergab ebenfalls umfassende Gesetzesverstöße (etwa bei der Führung der Personalnebenakten in der Grenzschutzinspektion).

Die Mängel im Umgang mit besonders sensiblen und schützenswerten Personal-/Personalaktendaten habe ich gemäß § 25 Abs. 1 BDSG gegenüber dem BMI als Verstoß gegen die Regelungen der §§ 90 ff. BBG beanstandet. Das BMI hat umgehend im geprüften Bundesgrenzschutzamt, aber auch im gesamten Bereich des Bundesgrenzschutzes die notwendigen Maßnahmen zur Einhaltung der gesetzlichen Regelungen der § 90 ff. BBG getroffen.

21.4 Beihilfedaten – noch immer für die Personalverwaltung interessant?

In der Vergangenheit habe ich mich mehrfach zur Bearbeitung von Beihilfen sowie zur Abschottung der Beihilfebearbeitung von der übrigen Personalverwaltung geäußert (s. 15. TB Nr. 9.5.21; 16. TB Nr. 23.4.3; 17 TB Nr. 18.5; 18. TB Nr. 18.5.1).

Bei der Behandlung von Einzeleingaben habe ich festgestellt, dass Probleme bei der Abschottung der Beihilfebearbeitung dadurch entstehen können, dass in einer Organisationseinheit sowohl Beihilfen als auch die übrigen Personalausgaben bearbeitet werden.

In § 90a Bundesbeamtengesetz (BBG) ist u. a. festgelegt, dass die Beihilfeakte in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden soll.

Eine Einengung des Begriffs „übrige Personalverwaltung“, wie sie in der Begründung zu § 90a BBG enthalten ist (Personalverwaltung im engeren Sinn, d. h. Erledigung der Personalangelegenheiten ohne die Bearbeitung von Personalausgaben), kann im Hinblick auf die neueren Regelungen zum Umgang mit besonderen Kategorien personenbezogener Daten nicht vorgenommen werden; sowohl Artikel 8 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr als auch § 3 Abs. 9 BDSG in der seit 23. Mai 2001 geltenden Fassung erklären Gesundheitsdaten zu besonderen personenbezogenen Daten, die damit in besonderem Maße zu schützen sind.

Aus den vorgenannten Gründen halte ich eine strikte Abschottung der Beihilfebearbeitung von der gesamten übrigen Personalverwaltung – also auch von der Bearbeitung der sonstigen Personalausgaben – für dringend erforderlich.

Folgende organisatorische Lösungen könnten dabei getroffen werden:

1. Die Beihilfebearbeitung wird von einer Stelle außerhalb der Personalverwaltung der Behörde wahrgenommen.
2. Die Beihilfebearbeitung für die Beschäftigten wird einer anderen Behörde übertragen.

Beide Lösungen halte ich für datenschutzgerecht.

Über diese Auffassung habe ich die obersten Bundesbehörden mit Rundschreiben vom 17. September 2002 (s. Anlage 28) unterrichtet.

Durch eine Einzeleingabe bin ich auf Mängel im Umgang mit Beihilfeakten bei der Grenzschutzdirektion hingewiesen worden.

Nach § 90a Satz 3 BBG darf die Beihilfeakte für andere als für Beihilfezwecke nur verwendet oder weitergegeben werden, wenn der Beihilfeberechtigte im Einzelfall einwilligt. In einem Einzelfall hat die Grenzschutzdirektion Auszüge aus der Beihilfeakte eines Beamten in einem Verwaltungsstreitverfahren über die Zahlung von Bezügen dem Verwaltungsgericht übermittelt. Diese Übermittlung ist erfolgt, ohne dass der Beamte in die Übermittlung eingewilligt hat. Hierin habe ich einen schwerwiegenden Verstoß gegen die Vorschriften des § 90a BBG gesehen, den ich nach § 25 Abs. 1 BDSG beanstandet habe.

22 Sozialdatenschutz – Allgemeines –

22.1 Nutzung von Sozialdaten zu anderen, insbesondere privaten Zwecken

Im Rahmen der Beratungen eines Gesetzes für eine bessere Absicherung der Vorleistungen von Bauhandwerkern (Vorleistungssicherungsgesetz) war im Frühjahr 2002 vom Bundesrat vorgeschlagen worden, in das Sozialgesetzbuch X einen neuen § 68a einzufügen, durch den den Sozialleistungsträgern die Befugnis übertragen werden sollte, Anschriften von Betroffenen für die Vollstreckung privatrechtlicher Titel an Private zu übermitteln. Hiergegen sind von mir, aber auch von den Bundesministerien für Gesundheit sowie für Arbeit und Sozialordnung erhebliche Bedenken vorgetragen worden. Mit dem vorgesehenen § 68a SGB X wäre es ermöglicht worden, Sozialdaten durch Sozialleistungsträger an Private zur Durchsetzung privatrechtlicher Ansprüche zu übermitteln.

Bei den Sozialdaten handelt es sich um personenbezogene Daten, die einem besonderen Amtsgeheimnis unterliegen (§ 35 SGB I). Diese Daten sind besonders schutzbedürftig. Die Vorschriften des SGB über den Datenschutz stellen diesen besonderen Schutz in hohem Maße sicher. Die Übermittlung von Sozialdaten ist nur zulässig, soweit dies im SGB X oder in anderen Büchern des Sozialgesetzbuches erlaubt wird. Zweck dieser Ausnahmevorschriften ist die Versorgung bestimmter öffentlicher Stellen, z. B. Polizeibehörden, Staatsanwaltschaften oder Gerichte, mit bestimmten Grundinformationen, die diese zur Erfüllung ihrer öffentlichen Aufgaben benötigen.

Hiermit sind die in dem Gesetzentwurf beabsichtigten Übermittlungstatbestände nicht zu vergleichen. Hier geht es um private Interessen, die von jedermann geltend gemacht werden können. Diesen Interessen gegenüber ist das Sozialgeheimnis höher zu bewerten, zumal es sich hierbei um ein Recht handelt, dem nach der Verfassung ein besonderer Schutz zukommt. Anderenfalls würden die Sozialleistungsträger zu Ersatzmeldebehörden. Eine solche Funktion wäre mit ihrer Aufgabenerfüllung als Sozialleistungsträger nicht vereinbar.

Ich werde auch künftig gegen eine Ausweitung der Übermittlungsbefugnisse im Rahmen des Sozialgesetzbuches in dem vorgenannten Sinne eintreten.

23 Arbeitsverwaltung

23.1 Organisation des Datenschutzes in der Bundesanstalt für Arbeit

Die Organisation des Datenschutzes in der Bundesanstalt für Arbeit (BA) ist seit langem Gegenstand meiner Tätigkeitsberichte (2. TB S. 30 f.; 3. TB S. 43; 5. TB S. 56 f.). Seit den frühen Achtzigerjahren wurde der Datenschutz in der Hauptstelle der BA

- fachintegriert von den Abteilungen durch Fachreferate mit Ausnahme der IT;
- abteilungsübergreifend bei gemeinsamen Angelegenheiten von einem Fachreferat Datenschutz, das gleichzeitig Ansprechpartner für mich bei der BA war;
- abteilungsübergreifend im Zusammenhang mit der IT von einem IT-Fachreferat und
- als Kontrolltätigkeit vom Beauftragten für den Datenschutz der BA (BfD/BA – diese Tätigkeit war seit Anfang der Achtzigerjahre verbunden mit der Funktion des Direktors des Vorprüfungsamtes)

wahrgenommen. Hinzu kamen die nach dem Dienstblatt-Runderlass 46/97 vorgesehenen Ansprechpartner für den Datenschutz in den einzelnen Arbeitsämtern.

Insbesondere nach der Novellierung des Datenschutzrechts im Jahr 2001 entsprach diese Organisation – auch nach Auffassung der BA – nicht mehr den gesetzlichen Vorgaben und den fachlichen Anforderungen an einen zeitgemäßen Datenschutz. Maßgeblich für die Organisation des Datenschutzes und die Bestellung des behördlichen Datenschutzbeauftragten in der BA sind § 18 BDSG sowie § 81 Abs. 4 SGB X i. V. m. §§ 4f, 4g BDSG. Danach ist der behördliche Datenschutzbeauftragte dem Leiter des Sozialleistungsträgers unmittelbar zu unterstellen, wobei er bei der Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei ist (§ 81 Abs. 4 SGB X i. V. m. § 4f Abs. 3 Sätze 1 und 2 BDSG). Dies war bei der bisherigen Organisationsform nicht der Fall. Hinzu kamen auch Probleme in der täglichen Praxis mit der bisherigen Datenschutzorganisation bei der BA.

Die erforderliche Neuorganisation des Datenschutzes der BA habe ich beratend begleitet. So habe ich darauf hingewirkt, dass angesichts der Größe der BA mit ihren ca. 96 000 Mitarbeitern und jährlich ca. sechs bis sieben Millionen Kunden die Arbeitskapazität des BfD/BA für seine Aufgaben nach § 81 Abs. 4 SGB X i. V. m. § 4g Abs. 1 BDSG freigehalten und ihm die erforderlichen Sach- und Personalmittel zur Verfügung gestellt werden. Erfreulicherweise ist die BA dieser Anregung gefolgt. Die Funktion des BfD/BA wird nunmehr als „full-time-job“ wahrgenommen. Auch ist er nunmehr organisatorisch unmittelbar dem Vorstand der BA unterstellt, was sich auch im Organigramm der Hauptstelle wiederfindet.

Nicht geändert hat sich jedoch, dass neben dem BfD/BA ein Fachreferat Datenschutz (Ref. IT/DS) eingerichtet ist, das insbesondere in Petitionsangelegenheiten mein Ansprechpartner bei der BA ist. Überlegungen der BA – die von mir nachhaltig unterstützt wurden – diese beiden Stellen zusammenzuführen, sind bedauerlicherweise nicht verwirklicht worden. In der Praxis zeigen sich hier häufig vermeidbare Reibungsverluste. Auch habe ich angesichts der Größe der Bundesanstalt Überlegungen unterstützt, den BfD/BA mit einer ausreichenden Anzahl Mitarbeiter auszustatten, wie dies in § 81 Abs. 4 Satz 1 SGB X i. V. m. § 4f Abs. 5 Satz 1 BDSG vorgesehen ist. Bedauerlicherweise wurden auch hier die positiven Überlegungen innerhalb der BA nicht realisiert. Hinsichtlich der Sicherstellung des Datenschutzes in den Arbeitsämtern sollten auch unter Nutzung vorhandener Fachkunde in den Landesarbeitsämtern und bei den Ansprechpartnern für den Datenschutz in den Arbeitsämtern praxisnahe Lösungen gefunden werden. Zu meinem Bedauern wurden auch hier bei der Umsetzung der Überlegungen in die Praxis erhebliche Abstriche gemacht.

Wenn auch noch Nachbesserungen bezüglich der Organisation des Datenschutzes in der BA dringend erforderlich sind, verkenne ich nicht, dass die BA bei der Neuorganisation des Datenschutzes in ihrem Bereich einen erheblichen Schritt in die richtige Richtung gemacht hat.

23.2 Modernisierung der Arbeitsverwaltung

23.2.1 Zusammenarbeit zwischen Arbeits- und Sozialämtern – Das Projekt MoZArT

Besondere Probleme bei der Vermittlung in Arbeit haben die Arbeitsämter bei den Arbeitslosen, die sowohl Arbeitslosen- als auch Sozialhilfe beziehen. Zwischen der Arbeitslosen- und der Sozialhilfe bestehen neben vielfältigen Unterschieden sich teilweise überschneidende Zielsetzungen. So ist es nicht verwunderlich, dass die Verbesserung der Zusammenarbeit der hierfür jeweils zuständigen Behörden bis hin zur Zusammenlegung dieser beiden staatlichen Fürsorgesysteme schon längere Zeit diskutiert wird.

Eine engere Zusammenarbeit zwischen Arbeits- und Sozialämtern war allerdings nicht erst im Berichtszeitraum ein wichtiges Thema. Bereits seit Mitte der Achtzigerjahre gibt es Kooperationsvereinbarungen zwischen einzelnen Arbeits- und Sozialämtern. Die Regierungskoalition nahm in ihrer Koalitionsvereinbarung vom 20. Oktober 1998 für die 14. Legislaturperiode ausdrücklich die Verbesserung der Zusammenarbeit zwischen Arbeits- und Sozialämtern auf, um die Vermittlung in Arbeit zu erleichtern und um überflüssige Bürokratie abzubauen. Auch die Opposition hat sowohl über den Bundesrat (identische Gesetzesinitiativen in Bundesratsdrucksache 52/02, 443/02 und 812/02) als auch über die CDU/CSU-Fraktion des Deutschen Bundestages (Bundestagsdrucksache 14/8365 und 15/24 – identisch mit den Bundesratsinitiativen) mit dem Entwurf eines Gesetzes zum optimalen Fördern und Fordern in Vermittlungsagenturen (OFFENSIV-Gesetz = **O**ptimal **F**ördern und **F**ordern – **En**gagierter **S**ervice **i**n **V**ermittlungsagenturen) sowie dem Entwurf eines Gesetzes zum Fördern und Fordern in der Sozialhilfe und Arbeitslosenhilfe (Fördern-und-Fordern-Gesetz – Bundestagsdrucksache 15/46) die Zusammenführung von Arbeitslosen- und Sozialhilfe in das Gesetzgebungsverfahren eingeführt. Dies verdeutlicht, dass hier in der Politik – bei unterschiedlicher Auffassung hinsichtlich der konkreten Umsetzung – ein grundsätzlicher Konsens besteht.

In der Mitte der Legislaturperiode legte die Bundesregierung einen Gesetzentwurf vor, der als „Gesetz zur Verbesserung der Zusammenarbeit zwischen Arbeitsämtern und Trägern der Sozialhilfe“ vom 20. November 2000 (BGBl. I S. 1590 – Zusammenarbeitsgesetz) verabschiedet wurde. Danach fördert das Bundesministerium für Arbeit und Sozialordnung – BMA (jetzt: Bundesministerium für Wirtschaft

und Arbeit) aufgrund von Koope rationsverträgen zwischen Arbeits- und Sozialämtern durchgeführte Modellprojekte zur Verbesserung der Zusammenarbeit zwischen diesen Behörden, um insbesondere die V ermittlungssituation von arbeitslosen Empfängern von Sozial hilfe deutlich zu verbessern (§§ 371a und 421d SGB III, §§ 18 Abs. 2a und 18a Bundessozialhilfegesetz – BSHG). Im Berichtszeitraum wurde unter dem Projektnamen MoZArT (**Mo**dellprojekte zur Verbesserung der **Z**usammenarbeit zwischen **Ar**beitsämtern und **T**rägern der Sozialhilfe) begonnen, ca. 30 Projekte (z. B. Job-Center [s. u. Nr. 23.2.2]), Kombi-Lohnkostenzuschüsse etc.) mithilfe eines privaten Projektträgers zu fördern. Die Förderung endet spätes tens zum 31. Dezember 2004 (§ 421d Abs. 1 Satz 6 SGB III). Eine Liste mit einer stichwortartigen Beschreibung der Mo dellprojekte findet sich im Internet unter der Adresse http://www.bma-mozart.de.

Folgende Grundtypen von Modellvorhaben werden gefördert:

Schwerpunktmäßige Betreuung der Bezieher von Arbeitslosen- und/oder von Sozialhilfe (Beratung, Vermittlung, Erarbeitung von Eingliederungsplänen, Vorbereitung und Organisation von Eingliederungsmaßnahmen, Auszahlung von Leistungen)

- durch das Arbeitsamt oder
- durch den Träger der Sozialhilfe oder
- durch eine vom Arbeitsamt und den T rägern der Sozialhilfe gemeinsam gebildete oder beauftragte Stelle.

Andere Arbeitslose, z. B. Bezieher von Arbeitslosengeld, können in die Modellvorhaben einbezogen werden, wenn dies aufgrund von deren Ausgestaltung zweckmäßig ist. Die Modellprojekte beinhalten

- gemeinsame Aktivitäten, insbesondere Datenaustausch;
- gemeinsame Einbeziehung (privater) Dritter bei der Vermittlung, Beratung und Betreuung;
- gemeinsame Planung und Durchführung von Eingliederungsprojekten (u. a. Errichtung einer gemeinsamen Anlaufstelle);
- gemeinsame Projekte zur Schaffung von Arbeitsplätzen;
- gemeinsam finanzierte Qualifizierungs- und/oder Beschäftigungsmaßnahmen.

Das mit dem Zusammenarbeitsgesetz verfolgte Ziel, Synergieeffekte anzustreben und doppelten Aufwand bei bzw . Reibungsverluste zwischen Arbeits- und Sozialamt zu vermeiden, habe ich ausdrücklich unterstützt. Zu meinem Bedauern wurden im Gesetzgebungsverfahren datenschutzrechtliche Fragen jedoch nicht ausreichend berücksichtigt. Dies führte bei der Umsetzung des Gesetzes im Berichtszeitraum zu nicht unerheblichen Problemen:

- Die in § 371a SGB III vorgesehenen Kooperationsverträge zwischen Arbeits- und Sozialämtern sollen – wie sich aus der amtlichen Begründung zu dieser V orschrift ergibt (Bundestagsdrucksache 14/3765 S. 5) – auch dafür sorgen, dass die Möglichkeiten moderner Informations- und Kommunikationstechnik umfassend bei und zwischen Arbeits- und Sozialamt genutzt werden. Ein solcher Kooperationsvertrag ist von seiner Rechts qualität her jedoch nicht geeignet, Grundrechte wie das Recht auf informationelle Selbstbestimmung einzuschränken. Mangels anderweitiger Regelung in § 371a SGB III und § 18 Abs. 2 BSHG gelten für den „Datenaustausc h“ zwischen Arbeits- und Sozialamt daher weiterhin die §§ 67 f f. SGB X und 35 SGB I, in deren Rahmen si ch auch die Kooperationsverträge zwischen Arbeits- und Sozialamt bewegen müssen. Eine in Nr. B.3 des Vorblatts des Regierungsentwurfs zum Zusammenarbeitsgesetz suggerierte Abweichung von bisherigen datenschutzr echtlichen Regelungen besteht daher nicht. In der Praxis habe ich jedoch immer wieder feststellen müssen, dass dieser Hinweis als „Freibrief“ für einen ungehinderten und umfassenden Datenaustausch zwischen den beteiligten Behörden sowie beteiligten privaten Dritten angesehen wurde.

  Um den Gesetzeszweck, Modelle für eine künftige Zusammenarbeit zwischen Arbeits- und Sozialämtern auszuprobieren, nicht zu gefährden, habe ich meine nicht unerheblichen Bedenken gegen die Übermittlung von Daten Arbeitsuchender an Sozialämter oder die gemeinsam gebildeten oder beauftragten Stellen nach § 421d Abs. 2 Nr. 3 SGB III zurückgestellt, soweit es sich um Daten von Personen handelt, für die das Modellprojekt geschaffen wurde. Einen Zugriff von Sozialämtern oder der gemeinsam gebildeten oder beauftragten Stelle auf alle Daten des Arbeitsamtes darf es jedoch nicht geben. In diesen Fällen läge eine V erletzung des Sozialgeheimnisses vor. Ich habe große Zweifel, ob bei der derzeitigen technischen Ausstattung der Arbeitsämter die erforderliche Einschränkung der Zugrif fsberechtigung zu Daten von Arbeitsuchenden in den Computersystemen der Bundesanstalt für Arbeit (BA) realisierbar ist. Unter dem Stichwort „Datenschutz durch T echnik“ gilt es hier , die technische Ausstattung bei der BA auf den Stand der heutigen Technik zu bringen.

- Das Zusammenarbeitsgesetz berücksichtigt ferner nicht, dass es sich bei den Arbeitsämtern um Bundesbehörden, bei den Trägern der Sozialhilfe dagegen um Kommunen handelt. Die genannten Stellen unterliegen daher einer unterschiedlichen Dienst-, Fach und Datenschutzaufsicht. Das Gesetz lässt Fragen zur rechtlichen V erantwortlichkeit sowie der rechtlichen und parlamentarischen Kontrolle, insbesondere der durch §§ 421d Abs. 2 Nr. 3 SGB III und § 18a Abs. 2 Nr . 1 BSHG vorgesehenen „gemeinsam gebildete(n) oder beauftragte(n) Stelle“ völlig offen. Soweit es sich bei diesen Stellen um private Dritte handelt, darf nicht aus dem Auge verloren werden, dass diese Stellen nicht Sozialleistungsträger sind und für sie daher der Sozialdatenschutz nicht gilt.

  Mit den für die Kommunen und damit für die Sozialämter zuständigen Landesbeauftragten für den Datenschutz habe ich mich dahingehend ge einigt, dass für die Modellprojekte insoweit gemeinsame datenschutzrechtliche Kontrollen durchgeführt werden sollen. Eine solche Kontrolle mit einem Landesbeauftragten für den Datenschutz hat im Berichtszeitsraum stattgefunden.

- Besondere Probleme bereitete die in § 421 Abs. 3 SGB III und § 18a Abs. 4 BSHG vor gesehene Evaluierung der Modellprojekte. Gemeinsam mit den Landesbeauftragten für den Datenschutz habe ich bezweifelt,
  - ob diese Regelungen die Übermittlung nicht anonymisierter personenbezogener Daten an das beauftragte private Forschungsinstitut rechtfertigen, insbesondere

auch soweit es sich um Daten von Arbeitsuchenden bzw. Sozialhilfeempfängern handelt, die nicht von den Modellprojekten erfasst werden,

- ob diese Regelungen eine personenbezogene Übermittlung der Daten Arbeitsuchender und Sozialhilfeempfänger ohne deren Einwilligung erlauben,
- ob die Übermittlung der Sozialversicherungsnummer an das private Forschungsinstitut mit dem Verbot des § 18f Abs. 5 SGB IV vereinbar ist, diese als Ordnungsnummer zu nutzen,
- ob die Übermittlung der Daten an das private Forschungsinstitut ohne die nach § 75 SGB X erforderliche Genehmigung durch die zuständige oberste Bundes- oder Landesbehörde erfolgen durfte.

Mit dem BMA und dem beauftragten Forschungsinstitut wurden dabei von den Landesbeauftragten und mir intensive Gespräche geführt, die dazu führten, dass das Forschungsinstitut mittlerweile die erforderlichen Genehmigungen nach § 75 SGB X beantragt und erhalten hat. Auf die Übermittlung der Sozialversicherungsnummer hat es inzwischen verzichtet und bildet aus dem Aktenzeichen des Sozialamtes und weiteren Daten eine „virtuelle Kundennummer". Es hat den Landesbeauftragten und mir nachvollziehbar dar gelegt, aus welchen Gründen die Einwilligung der betroffenen Arbeitsuchenden und Sozialhilfeempfänger nicht eingeholt werden kann. Außerdem wurde den Landesbeauftragten und mir erläutert, dass die Daten von Arbeitsuchenden bzw. Sozialhilfeempfängern aus nicht an Modellprojekten beteiligten Arbeits- und Sozialämtern zu Vergleichszwecken benötigt würden, um den Erfolg bzw. Misserfolg des Modellprojektes aufzeigen zu können. Um die Modellprojekte evaluieren zu können, werden von den Arbeits- und Sozialämtern dem Forschungsinstitut personenbezogene Daten von

- Personen, die von Modellämtern zur Teilnahme am Modellprojekt ausgesucht wurden;
- Personen, die von Modellämtern nicht zur Teilnahme am Modellprojekt ausgesucht wurden;

und

- Personen, die von Vergleichsämtern benannt werden;

übermittelt, die zusätzlich persönlich befragt werden sollen.

Das Ziel der Kooperation von Arbeits- und Sozialämtern, die betroffenen arbeitssuchenden Sozialhilfeempfänger von bürokratischen Zwängen, Laufereien usw. zu befreien und den beteiligten Stellen Mehrfacharbeit etwa durch doppelte Erhebung des gleichen Lebenssachverhalts zu ersparen, wird von mir nachhaltig unterstützt. Dabei darf allerdings der Grundrechtsschutz des Betroffenen nicht aus den Augen verloren werden. Das Unglück, seine Arbeitsstelle zu verlieren oder Sozialhilfeberechtigter zu werden, darf nicht zum Schaden für das Grundrecht auf informationelle Selbstbestimmung des Betroffenen führen. Unter Berücksichtigung der grundlegenden Unterschiede zwischen Arbeitslosen- und Sozialhilfe halte ich eine engere, auch technikunterstützte und datenschutzgerechte Kooperation von Arbeits- und Sozialämtern für realisierbar. Dem Datenschutzrecht kommt hierbei keine verhindernde, sondern eine gestaltende Rolle zu.

23.2.2 Die Vorschläge der Hartz-Kommission auf dem datenschutzrechtlichen Prüfstand

Im Februar 2002 beauftragte die Bundesregierung eine aus 15 Mitgliedern bestehende Kommission „Moderne Dienstleistungen am Arbeitsmarkt" unter Leitung von Dr. Peter Hartz, Mitglied des Vorstandes der Volkswagen AG (nach ihrem Vorsitzenden auch „Hartz-Kommission" genannt), Vorschläge zur Reform der BA zu erarbeiten. Am 16. August 2002 legte die Kommission einen umfangreichen Bericht vor, der noch im Berichtszeitraum gesetzgeberisch umgesetzt wurde (Erstes und Zweites Gesetz für moderne Dienstleistungen am Arbeitsmarkt, jeweils vom 23. Dezember 2002, BGBl. 2002 I, S. 4607 bzw. S. 4621).

Die Vorschläge der Hartz-Kommission haben zum Teil erhebliche Auswirkungen auf rechtliche Regelungen zum Sozialdatenschutz:

- Das von der Hartz-Kommission vorgeschlagene Modell Job-Center zur Zusammenarbeit von Arbeits- und Sozialämtern ist eines der aufgrund des Gesetzes zur Verbessung der Zusammenarbeit zwischen Arbeitsämtern und Trägern der Sozialhilfe vom 20. November 2000 (BGBl. I S. 1590 – Zusammenarbeitsgesetz, s. o. Nr. 23.2.1) geförderten Modellprojekte. Der aufgrund dieses Vorschlags durch das Zweite Gesetz für moderne Dienstleistungen am Arbeitsmarkt geänderte § 402 SGB III hat den Betrieb von Job-Centern durch das Arbeitsamt in den Katalog der Aufgaben der BA aufgenommen und die Erhebung, Verarbeitung und Nutzung der erforderlichen Sozialdaten für zulässig erklärt. Damit wird dem Arbeitsamt die Möglichkeit eröffnet, von dem örtlichen Sozialamt Daten zu erhalten sowie für dessen Aufgaben Daten zu erheben und an dieses zu übermitteln. § 18 Abs. 2a BSHG beinhaltet eine korrespondierende Vorschrift für die Sozialämter.

  Bei einem Arbeitsamt, das ein Job-Center betreibt, werde ich in den nächsten Monaten gemeinsam mit dem für das örtliche Sozialamt zuständigen Landesbeauftragten für den Datenschutz einen datenschutzrechtlichen Kontroll-, Beratungs- und Informationsbesuch machen und auf dieser Grundlage eine gemeinsame datenschutzrechtliche Beurteilung der Job-Center abgeben.

- Die stärkste Entlastung auf dem Arbeitsmarkt erhofft sich die Hartz-Kommission durch eine Ausweitung der Zeitarbeit. Zu diesem Zweck wurde § 37c mit der Verpflichtung in das SGB III eingeführt, dass jedes Arbeitsamt mindestens eine Personal-Service-Agentur (PSA) in seinem Bezirk einrichtet. Zu diesem Zweck sollen die Arbeitsämter Verträge mit privaten Zeitarbeitsunternehmen abschließen und nur ausnahmsweise PSA in Eigenregie betreiben. Die Arbeitslosen sollen von der PSA angestellt und nach Tariflohn bezahlt werden. Unternehmen können die Leiharbeiter kostenlos auf Probe oder gegen Entgelt einstellen, sie aber auch jederzeit entlassen, wenn es die Auftragslage notwendig machen sollte. Die Zeitarbeit soll insbesondere schwer vermittelbaren Langzeitarbeitslosen zu einer Stelle verhelfen. Wer die Beschäftigung in einer PSA ablehnt, dem wird das Arbeitslosengeld gekürzt.

  Die PSA werfen datenschutzrechtlich eine Reihe von noch nicht geklärten Fragen auf. Dazu gehört auch das Verhältnis von Job-Center im Arbeitsamt zu den privat-

rechtlich betriebenen PSA und hier vorkommenden Übermittlungen von Daten Arbeitsuchender. Das Gesetz ist zwar erst zum 1. Januar 2003 in Kraft getreten; mir liegen allerdings bereits Eingaben zu diesem Bereich vor, denen ich nachgehen werde.

– Im Bericht der Hartz-Kommission wird unter dem Stichwort „Vernetzung mit Kooperationspartnern" u. a. der „gesonderte Datenzugang" für Zeitarbeitsfirmen und private Vermittler angeregt, wobei dort ausdrücklich darauf hingewiesen wird, Fragen des Datenschutzes zu berücksichtigen.

  Hier liegt eines der größten datenschutzrechtlichen Probleme bei den Vorschlägen der Hartz-Kommission: die Eröffnung der Möglichkeit für Dritte, Zugang zu den Computersystemen der Arbeitsämter zu erhalten. Dabei ist dieser Vorschlag keinesfalls neu. Entsprechende Anliegen, mein Einverständnis hierzu zu erteilen, wurden bereits in den letzten Jahren mehrfach an mich herangetragen. Das größte Problem ist die veraltete Technik der BA. Diese erlaubt derzeit lediglich, den Zugang Dritter auf die Datenbanken und Computersysteme der BA insgesamt zuzulassen oder gar nicht. Ein Mittelweg, wie etwa die Eröffnung des Zugangs nur zu bestimmten Teilen des Systems, ist derzeit nicht möglich. Ein ungehinderter Zugriff privater Dritter auf die Computersysteme der BA (nicht nur der Vermittlungs-, sondern auch der Leistungsdaten) würde einer Abschaffung des Sozialdatenschutzes für Arbeitslose gleichkommen. Dem Bericht der Hartz-Kommission habe ich aber auch entnommen, dass die Informationstechnik der BA künftig neu ausgerichtet werden soll. Ich werde diesen Prozess datenschutzrechtlich begleiten.

– Auch der im Bericht der Hartz-Kommission beschriebene Aufbau eines Forschungsdatenzentrums bei der BA wirft eine Reihe datenschutzrechtlicher Fragen auf, wie der Zugang externer Wissenschaftler zu personenbezogenen Daten aus den Datenbeständen der BA ausgestaltet werden soll. Die Schaffung eines in diesem Zusammenhang genannten „Scientific/Public Use File" und eines speziellen Forschungsdatengeheimnisses war im Berichtszeitraum bereits Gegenstand intensiver Gespräche mit Vertretern der Ressorts, der BA, dem Statistischen Bundesamt und vor allem der Wissenschaft. Es wurde vereinbart, eine Arbeitsgruppe aus Vertretern von Bundesministerien, BA, Statistischem Bundesamt, Wissenschaft und Datenschutzbeauftragten zu bilden, die die mit der Erstellung eines „Scientific Use File" verbundenen Probleme aufbereiten und Lösungsvorschläge erarbeiten soll. Zur Mitarbeit hieran habe ich mich bereit erklärt.

– Die im Bericht der Hartz-Kommission erwähnte Entwicklung einer digitalen Signaturkarte für den Abruf von Verdienst- und Arbeitsbescheinigungen (JobCard) wird datenschutzrechtlich von mir bereits seit einiger Zeit begleitet. Sie soll zu erheblichen Einsparungen bei den Unternehmen führen, die sich durch die Ausstellung von entsprechenden Bescheinigungen für ihre Arbeitnehmer bzw. ehemaligen Arbeitnehmer erheblich finanziell belastet fühlen. Die Unternehmen sollen künftig die Bescheinigungen in verschlüsselter Form bei einem Dritten (Datenpool) hinterlegen. Der Bürger soll im Bedarfsfall die öffentliche Stelle, die die Daten benötigt, mithilfe der Signaturkarte berechtigen, die im Datenpool vorhandenen erforderlichen Daten abzurufen. An dem derzeit laufenden Pilotprojekt, mit dem die Praxistauglichkeit der Signaturkarte für Daten aus Arbeitsbescheinigungen nach § 312 SGB III getestet werden soll, bin ich beteiligt. Dabei zeigt sich, dass im Detail eine Reihe von datenschutzrechtlichen Fragen auftaucht, die noch einer Lösung zugeführt werden müssen:

  – Es entsteht eine Datenspeicherung auf Vorrat, deren Vereinbarkeit mit den vom Bundesverfassungsgericht im Volkszählungsurteil aufgestellten verfassungsrechtlichen Grundsätzen noch geprüft werden muss. So sind nach § 312 SGB III die Arbeitgeber verpflichtet, bei Beendigung des Arbeitsverhältnisses alle Tatsachen zu bescheinigen, die für die Entscheidung über den Anspruch auf Arbeitslosengeld, Arbeitslosenhilfe, Unterhaltsgeld oder Übergangsgeld erheblich sein können (Arbeitsbescheinigung). Diese Arbeitsbescheinigung wird daher bei jeder Beendigung eines Arbeitsverhältnisses ausgestellt. Aber nur ein geringer Teil der ehemaligen Arbeitnehmer muss bei einem entsprechenden Antrag die Arbeitsbescheinigung beim Arbeitsamt tatsächlich vorlegen. Ein großer Teil der in den Datenpool einfließenden Daten wird daher nie benötigt werden.

  – Der Bericht der Hartz-Kommission sieht in diesem Zusammenhang die Einführung einer einheitlichen Versicherungsnummer aller Sozialversicherungsträger als sinnvoll an. Im Zusammenhang mit der Schaffung der digitalen Signaturkarte für Arbeitgeberbescheinigungen ist eine solche Nummer als Ordnungsnummer erforderlich, um Daten einem bestimmten Arbeitnehmer eindeutig zuweisen zu können. Dabei ist zu beachten, dass die Restriktionen bei der Nutzung der Sozialversicherungsnummer (§§ 18 f und g SGB IV) und der Krankenversichertennummer auf der Krankenversichertenkarte (§§ 290 und 291 SGB V) vom Gesetzgeber aus gutem Grund geschaffen wurden. Insbesondere für die Sozialversicherungsnummer hat der Gesetzgeber ausdrücklich angeordnet, dass diese nicht als Ordnungsmerkmal dienen soll (§ 18f Abs. 5 SGB IV). Mit den am Pilotprojekt beteiligten Stellen bin ich im Gespräch, um eine datenschutzgerechte Lösung für das Problem zu erreichen.

23.3 Teilnahmebescheinigungen sind keine Beurteilungen

In meinem 18. TB (Nr. 20.4) habe ich darüber berichtet, dass für die Beurteilungen von Leistungen und dem Verhalten Arbeitsloser bei der Durchführung von Maßnahmen, die das Arbeitsamt angeordnet hat, keine Rechtsgrundlage besteht und dass die gefundene Einwilligungsregelung nur als Übergangslösung betrachtet werden kann. Durch das Gesetz zur Reform der arbeitsmarktpolitischen Instrumente vom 10. Dezember 2001 (Job-AQTIV-Gesetz, BGBl. I S. 3443) hat der Gesetzgeber meine Hinweise zum Teil aufgegriffen und für Teilnehmer an einer beruflichen Weiterbildung geregelt, dass diese verpflichtet sind, „eine Beurteilung ihrer Leistung und ihres Verhaltens durch den Träger zuzulassen" (§ 318 Abs. 2 Satz 1 Nr. 2 SGB III). Gleichzeitig wurden die

Maßnahmeträger verpflichtet, ihre Beurteilungen des Teilnehmers unverzüglich dem Arbeitsamt zu übermitteln. Obwohl mir die Bundesanstalt für Arbeit (BA) erst wenige Monate vor dem Erlass des Job-AQTIV-Gesetzes mitgeteilt hatte, dass im Rahmen von Arbeitsbeschaffungsmaßnahmen (ABM) „von den Arbeitgebern keine Zeugnisse/Beurteilungen abgegeben“ werden, da „bei ABM ... dies nicht erforderlich (sei), weil es sich um ein Arbeitsverhältnis handelt“, hat der Gesetzgeber die Träger oder durchführenden Unternehmen von Arbeitsbeschaffungsmaßnahmen nach den §§ 260 ff. SGB III und von Strukturanpassungsmaßnahmen nach §§ 272 ff. SGB III verpflichtet, für die geförderten Arbeitnehmer eine Teilnahmebeurteilung für das Arbeitsamt auszustellen (§ 261 Abs. 5, § 278 SGB III). Die hier vorgesehenen Regelungen sind allerdings deshalb unzureichend, weil sie lediglich den Maßnahmeträger verpflichten, eine Beurteilung des Teilnehmers an der Maßnahme durchzuführen. Eine Verpflichtung des Teilnehmers, seine Leistung und sein Verhalten beurteilen zu lassen, besteht hier nicht.

Nicht geregelt wurde jedoch die Beurteilung von Teilnehmern an Trainingsmaßnahmen nach den §§ 48 ff. SGB III und von berufsvorbereitenden Bildungsmaßnahmen nach den §§ 61 ff. SGB III. Auch für die Beurteilung von Teilnehmern an Maßnahmen im Rahmen der Förderung behinderter Menschen am Arbeitsleben nach §§ 97 ff. SGB III fehlt es an einer entsprechenden Regelung.

Insbesondere von Teilnehmern an Trainingsmaßnahmen nach §§ 48 ff. SGB III erreichen mich weiterhin eine Reihe von Eingaben, in denen sich Arbeitsuchende darüber beklagen, dass ohne ihre Einwilligung ihre Leistung und ihr Verhalten von Maßnahmeträgern beurteilt und diese Beurteilung dem Arbeitsamt übermittelt wurde. Mangels einer gesetzlichen Regelung halte ich dies weiterhin für unzulässig, soweit nicht der Betroffene in das Verfahren ausdrücklich eingewilligt hat. Die allgemeine Datenerhebungs- und -verarbeitungsklausel in § 402 SGB III, die das Bundesministerium für Arbeit und Sozialordnung (jetzt: Bundesministerium für Wirtschaft und Arbeit – BMWA) in seiner Stellungnahme als Ermächtigungsgrundlage heranziehen will, reicht wegen des weit reichenden Eingriffs in das Persönlichkeitsrecht der Arbeits- bzw. Ausbildungsplatzsuchenden nicht aus.

Ich hoffe daher, dass das BMWA einen Gesetzentwurf vorlegt, um dieses dringliche Problem zu lösen. Meine Bereitschaft, an einer praktikablen Lösung mitzuwirken, habe ich mehrfach erklärt.

23.4 Arbeitsvermittlung im Internet

23.4.1 Veröffentlichung von medizinischen Daten im Internet

Aufgrund von Eingaben bin ich darauf aufmerksam geworden, dass die Bundesanstalt für Arbeit (BA) in Einzelfällen Auszüge aus ärztlichen Gutachten in ihren u. a. im Internet abrufbaren Bewerberangeboten, dem so genannnten Arbeitgeber-Informations-Service (AIS), veröffentlicht hat. Die Angaben über Schwerbehinderungen oder Alkoholgefährdung der Betroffenen fanden sich hierbei im Feld „Kenntnisse“.

Um passgenaue Arbeitsplätze vermitteln zu können, sollen in diesem Feld des Bewerberangebots eigentlich Angaben über die beruflichen Kenntnisse und Fertigkeiten des Bewerbers eingetragen werden. Da bei der Erstellung eines Bewerberprofils oder der Veröffentlichung von Bewerberdaten im AIS programmtechnisch, d. h. automatisch auf die im Bewerberangebot gespeicherten Angaben zurückgegriffen wird, wurden die wohl versehentlich unter „Kenntnisse“ gespeicherten medizinischen Daten in den vorliegenden Fällen im Internet veröffentlicht. Auch wenn in das AIS nur anonymisierte Daten aufgenommen werden und dort insofern in aller Regel ein Personenbezug nicht herstellbar ist, können den Betroffenen dennoch erhebliche Nachteile entstehen, wenn die Eintragung von medizinischen Daten dazu führt, dass ihnen dadurch eine geringere Anzahl von Stellenangeboten unterbreitet wird. Außerdem wird der Personenbezug vom Arbeitsamt immer dann hergestellt, wenn ein Arbeitgeber Interesse an dem Bewerberangebot bekundet und Kontakt zu dem Bewerber aufnehmen möchte. In einem der an mich herangetragenen Fälle wurde das Bewerberprofil mit den fraglichen Daten zudem an einen Bildungsträger übermittelt und den Teilnehmern des dortigen Bewerbertrainings vorgelesen.

Die geschilderte unzulässige Offenbarung medizinischer Daten stellt einen gravierenden Verstoß gegen das Sozialgeheimnis dar. Die Eintragungen in den Bewerberangeboten hätten – wie auch jede korrekte Eintragung – vor einer Weitergabe oder Veröffentlichung auf ihre Aktualität und Richtigkeit hin geprüft und mit dem Betroffenen abgestimmt werden müssen. Bei einer solchen Prüfung, die in den bekannt gewordenen Fällen offensichtlich unterblieben ist, wären die unzulässig gespeicherten Daten vermutlich aufgefallen und hätten korrigiert oder gelöscht werden können. Die BA hat mir jedoch versichert, dass sie die Mängel sofort nach deren Bekanntwerden behoben hat, indem die infrage stehenden Daten gelöscht wurden. Um zu gewährleisten, dass solche Fehler in Zukunft möglichst ausgeschlossen werden, wurden darüber hinaus Qualitätszirkel eingerichtet, die die Bewerberdaten überprüfen und bei Bedarf überarbeiten. Ziel dieser Zirkel ist es, die Qualität der Daten zu optimieren, unzulässige, fehlerhafte oder gegen datenschutzrechtliche Bestimmungen verstoßende Eintragungen festzustellen und diese vor einer möglichen Datenübermittlung zu beheben. Darüber hinaus wurde eine Arbeitshilfe Qualitätsstandards des Vermittlungsprozesses erstellt, mit der die korrekte Erfassung der in die IT-Systeme einzugebenden Daten ebenfalls nachhaltig verbessert werden soll. Die Landesarbeitsämter haben hierzu bereits vielfältige Maßnahmen mit unterschiedlichen Aktivitäten und Verbesserungsansätzen – z. B. im Rahmen von Schulungen oder durch Analysen in den Ämtern – umgesetzt.

Ich halte die von der Arbeitsverwaltung getroffenen Maßnahmen für geeignet, die zugrunde liegende Problematik in den Griff zu bekommen. Auf eine förmliche Beanstandung habe ich deshalb verzichtet, nicht zuletzt auch, weil die aufgezeigten Mängel unverzüglich abgestellt wurden.

23.4.2 Weiterhin Probleme bei der Anonymisierung!

In meinem 18. TB (Nr. 20.7.1) habe ich berichtet, dass die von den Arbeitsämtern im AIS vorgenommene Anonymisierung der eingestellten Bewerberangebote nicht immer einwandfrei funktioniert. Dies liegt, wie ich bereits damals erläutert habe, daran, dass es systembedingt nicht

möglich ist, in kritischen Einzelfällen auf die Veröffentlichung des Teils des Bewerberdatensatzes zu verzichten, der die Identifizierung unter bestimmten Umständen ermöglicht. Die Hauptstelle der BA hatte mir daher eine Regelung angekündigt, mit der sichergestellt werden sollte, dass Bewerberangebote auch dann datenschutzgerecht in den AIS eingestellt werden können, wenn allein durch Weglassen des Namens die Anonymisierung nicht gewährleistet ist. Eine solche Regelung wird es nach Auskunft der Hauptstelle nunmehr doch nicht geben. Mir wurde lediglich zugesichert, dass in den Fällen, in denen die Anonymisierung der Daten nicht gewährleistet ist, auf Wunsch des Betroffenen auch künftig von der Einstellung des Bewerberdatensatzes in den AIS abgesehen wird. Diese Entwicklung der Angelegenheit halte ich aus datenschutzrechtlicher Sicht nicht für befriedigend. Auch unter dem Gesichtspunkt einer effektiven Arbeitsvermittlung kann es nicht erstrebenswert sein, bestimmte Arbeitslose von den Vermittlungsmöglichkeiten, die die BA im Internet bietet, abzukoppeln, nur weil es systembedingt nicht möglich ist, alle Bewerberangebote datenschutzgerecht zu anonymisieren. Ich hoffe deswegen, dass die BA die bekannten Unzulänglichkeiten im Rahmen der Weiterentwicklung oder bei Neuentwicklungen der Informationstechnik berücksichtigen wird, und werde die Angelegenheit spätestens dann wieder ins Gespräch bringen.

23.5 Einzelfälle

23.5.1 Unzulässige Datenerhebung bei einem früheren Arbeitgeber

Ein Petent hatte bei einem Arbeitsamt einen Antrag auf Unterhaltsgeld gestellt. Da dieses nicht in der ihm seiner Meinung nach zustehenden Höhe bewilligt wurde, reichte er Widerspruch und anschließend Klage vor dem Sozialgericht ein. Anlässlich des Gerichtsverfahrens holte das Arbeitsamt beim ehemaligen Arbeitgeber des Petenten Auskünfte zu dessen Gehalt ein und übermittelte diese an das Sozialgericht. Diese Angaben zum Gehalt wurden nach Darstellung des Arbeitsamtes benötigt, da das Unterhaltsgeld im vorliegenden Fall anhand eines fiktiven Bemessungsentgelts festzulegen war, dessen Höhe überprüft werden musste. Die Datenerhebung beim ehemaligen Arbeitgeber und die Übermittlung der unzulässig erhobenen Daten an das Sozialgericht habe ich wegen Verstoßes gegen § 67a Abs. 2 und § 69 Abs. 1 Nr. 2 SGB X beanstandet. Das Arbeitsamt hätte die Daten – wenn überhaupt – beim Betroffenen selbst erheben müssen. Die Voraussetzungen für eine Datenerhebung ohne Mitwirkung des Betroffenen waren allesamt nicht gegeben. Darüber hinaus hätte das Arbeitsamt zur Festlegung des fiktiven Bemessungsentgelts das in diesem Fall ortsübliche Arbeitsentgelt zugrunde legen können. Um dieses zu ermitteln, wäre es ausreichend gewesen, verschiedene ortsansässige Firmen, die vergleichbare Tätigkeiten anbieten, ohne konkreten Personenbezug zu befragen. Die Erhebung des tatsächlich ehemals an den Petenten gezahlten Gehalts war zur Aufgabenerfüllung des Arbeitsamtes im vorliegenden Fall nicht erforderlich. Die Arbeitsverwaltung hat mir zugesagt, die unzulässig erhobenen Daten zu löschen und das Sozialgericht entsprechend zu benachrichtigen. Der Direktor des betroffenen Arbeitsamtes hat sich bei dem Petenten entschuldigt.

23.5.2 Umfangreiche Datenübermittlung an eine Krankenkasse

Ein Ehepaar hat sich an mich gewandt, weil das Arbeitsamt, bei dem die Ehefrau Arbeitslosenhilfe beantragt hatte, Daten mit der Krankenkasse des Ehemanns ausgetauscht hat. Die meisten der aufgezeigten Datenübermittlungen waren zur Aufgabenerfüllung eines der beiden Sozialleistungsträger erforderlich und damit zulässig (§ 69 Abs. 1 Nr. 1 SGB X). So hat das Arbeitsamt der Krankenkasse auf deren Anfrage unter anderem mitgeteilt, dass der Ehemann anlässlich der Prüfung der Bedürftigkeit seiner Frau dem Arbeitsamt gegenüber angegeben habe, aus seiner selbstständigen Tätigkeit keinen Gewinn zu erzielen. Diese Information war nach Darstellung der Krankenkasse zur Beurteilung der Krankengeldansprüche des Ehemanns erforderlich. Das Arbeitsamt hat seinem Antwortschreiben allerdings zusätzliche Unterlagen beigefügt, die die Krankenkasse zur Prüfung von Ansprüchen nicht benötigte und auch nicht erbeten hatte. Seitens der Arbeitsverwaltung wurde schließlich eingeräumt, dass eine Datenübermittlung in dieser Breite tatsächlich nicht erforderlich gewesen wäre, die Unterlagen jedoch „der Einfachheit halber“ beigefügt worden waren. Diese Begründung zeigt, wie unbedacht und leichtfertig hier mit Sozialdaten umgegangen wurde. Nicht zuletzt weil ich in dem hier geschilderten Fall zum wiederholten Mal feststellen musste, dass ein Arbeitsamt über die Erforderlichkeit hinaus Unterlagen an eine Krankenkasse übermittelt hat, habe ich diese Übermittlung wegen Verstoßes gegen § 69 Abs. 1 Nr. 1 SGB X beanstandet.

23.5.3 Erhebung und Nutzung von Daten zu privaten Zwecken

Ein Mitarbeiter eines Landesarbeitsamtes nutzte seine berufliche Position, um bei einer Krankenkasse personenbezogene Daten über seine geschiedene Ehefrau einzuholen. Anschließend verwendete er die auf diese Weise unzulässig erhobenen Daten für seine privaten Zwecke, indem er den von der Krankenkasse erhaltenen Datenausdruck im Rahmen einer Unterhaltsstreitsache an ein Gericht übermittelte. Der Mitarbeiter, der aufgrund seiner Tätigkeit über den besonderen Schutz und die Sensibilität von Sozialdaten belehrt worden war, hat sich durch sein Verhalten bewusst über die ihm bekannten datenschutzrechtlichen Bestimmungen hinweggesetzt. Diesen gravierenden Verstoß gegen das Sozialgeheimnis habe ich beanstandet. Das Landesarbeitsamt hat den betroffenen Mitarbeiter aufgrund seines Fehlverhaltens in eine andere Funktion zu einer anderen Dienststelle umgesetzt und entsprechende Disziplinarmaßnahmen eingeleitet.

23.5.4 Arbeitsamt übermittelt Sozialdaten an eine Detektei

Ein anderer Petent hat sich an mich gewandt, nachdem er erfahren hatte, dass der Rechtsanwalt seines Vermieters in einer Streitsache in einem Schreiben an ein Gericht Daten von ihm angegeben hatte, die nur der BfA und dem Arbeitsamt hätten bekannt sein können. Der Rechtsanwalt hatte in dem Schreiben weiter ausgeführt, dass die Daten von einem Dritten, einer Detektei, bestätigt werden könnten. Der Petent vermutete daher, dass einer der beiden genannten Sozialleistungsträger dieser Detektei unbefugt Auskünfte erteilt habe.

Nachdem sowohl die Bundesanstalt für Arbeit (BA) als auch die BfA von mir um Stellungnahme zu der Angelegenheit gebeten worden waren, stellte sich heraus, dass die in dem Schreiben des Rechtsanwalts aufgeführten Leistungszeiträume mit den im Arbeitsamt über den Petenten gespeicherten Sozialdaten identisch waren. Eine Befragung der Mitarbeiter des Arbeitsamtes, die Zugriff auf die gespeicherten Daten hatten, ergab erwartungsgemäß keine weiteren Aufschlüsse. Dennoch ging auch die BA bei Betrachtung der Gesamtzusammenhänge davon aus, dass die Sozialdaten von einem Mitarbeiter des Arbeitsamtes offenbart worden waren. Obwohl datenschutzrechtliche Weisungen der BA ausdrücklich vorsehen, dass vor der telefonischen Übermittlung schutzwürdiger Daten die Identität des Anrufers zu prüfen ist, wurde dies im vorliegenden Fall offensichtlich nicht beachtet. Auch diesen Verstoß gegen das Sozialgeheimnis habe ich daher beanstandet. In ihrer Stellungnahme hat die BA erklärt, dass es gerade in letzter Zeit häufiger vorkomme, dass sich Beauftragte von Inkassounternehmen oder Auskunfteien telefonisch als Mitarbeiter anderer Behörden ausgeben und versuchen, auf diesem Weg unberechtigt Auskünfte über Kunden des Arbeitsamtes zu erhalten. Die BA hat mir daher zugesagt, den geschilderten Fall zum Anlass zu nehmen, die Mitarbeiter aller Dienststellen nochmals für die Problematik unberechtigter Auskunftsersuchen zu sensibilisieren.

Im Rahmen dieser Eingabe wurde ich auch darauf aufmerksam, dass lesende Zugriffe auf gespeicherte Daten in der Arbeitsverwaltung nicht protokolliert werden. Dies halte ich aus datenschutzrechtlicher Sicht für unbefriedigend. Jeder lesende Zugriff bietet grundsätzlich die Möglichkeit und birgt damit – wie der vorliegende Fall zeigt – auch die Gefahr, dass sensible Sozialdaten unzulässig offenbart werden. Auch ein lesender Zugriff auf IT-Systeme ist immer nur dann zulässig, wenn dies im jeweiligen Einzelfall zur Aufgabenerfüllung erforderlich ist. Ich habe der BA daher dringend empfohlen, auch die lesenden Zugriffe auf die IT-Systeme zu protokollieren. Nicht zuletzt die Kenntnis der Mitarbeiter über eine solche Protokollierung würde die Sensibilität im Umgang mit den gespeicherten Sozialdaten sicherlich erhöhen. Die BA teilt zwar meine Auffassung, dass die Protokollierung lesender Zugriffe aus datenschutzrechtlicher Sicht ein nicht zu vernachlässigendes Instrument ist, will aber dennoch weiterhin darauf verzichten, weil der hierfür erforderliche Aufwand ihrer Meinung nach in keinem vertretbaren Verhältnis zu dem möglichen Sicherheitsgewinn steht. Die Ablehnung dieser zusätzlichen Sicherheitsmaßnahme wird insbesondere damit begründet, dass die in den Arbeitsämtern eingesetzten IT-Systeme, deren Lebenszyklus zu Ende gehe, nur begrenzte Speicherkapazität aufweisen und eine Protokollierung daher nicht leisten könnten. Erst bei künftigen Neuentwicklungen ist man seitens der Arbeitsverwaltung bereit, meine Forderung erneut zu prüfen. Ich habe die BA daher gebeten, mir mitzuteilen, in welchem Zeitrahmen mit der Einführung der Protokollierung zu rechnen ist. Unabhängig davon erwarte ich auch eine Stellungnahme zu der Frage, warum nicht bereits jetzt im Rahmen der vorhandenen Möglichkeiten statt einer Gesamt- zumindest schon eine Blockprotokollierung eingeführt wird. Diese dürfte auch angesichts begrenzter Speicherkapazitäten durchführbar sein.

23.5.5 Unzulässige Datenübermittlung

Eine Petentin hatte bei einem Landesarbeitsamt einen Antrag auf Erlaubnis zur gewerbsmäßigen Arbeitnehmerüberlassung gestellt.

Die Arbeitsverwaltung informierte daraufhin die Stadtverwaltung (Ordnungsamt), bei der die Petentin damals als Mitarbeiterin tätig war, über diesen Antrag. Dies war für die Aufgabenerfüllung des Arbeitsamtes nicht erforderlich. Auch für eine Überlassung dieser Information an die Stadtverwaltung als Arbeitgeberin der Petentin fehlte jede Rechtsgrundlage.

Außerdem wurden dem Ehemann der Petentin im Rahmen einer Einsicht in seine bei der Arbeitsverwaltung geführten Akten unzulässigerweise darin aufgenommene Angaben zum Antrag der Petentin auf Erlaubnis zur gewerbsmäßigen Arbeitnehmerüberlassung zur Kenntnis gegeben.

Diese Verstöße gegen das Sozialgeheimnis habe ich wegen Verstoßes gegen § 35 SGB I i. V. m. § 67d SGB X beanstandet.

24 Krankenversicherung, Pflegeversicherung

24.1 Krankenversicherung

24.1.1 Gesundheitsreform: Der Datenschutz bleibt am Ball!

In der 14. Legislaturperiode habe ich mich in besonderem Maße mit Gesetzgebungsvorhaben im Bereich der Gesundheitsreform befasst. Leider enthält das am 1. Januar 2000 in Kraft getretene GKV-Gesundheitsreformgesetz 2000 (BGBl. I 1999 S. 2626) die im Laufe des Gesetzgebungsverfahrens auf Initiative der Datenschutzbeauftragten des Bundes und der Länder aufgenommenen datenschutzrechtlichen Verbesserungen im Abrechnungssystem der Krankenkassen nicht mehr. Der vom Deutschen Bundestag ursprünglich beschlossene Gesetzentwurf hatte vorgesehen, dass die Krankenkassen künftig zwar über die vollständigen Abrechnungsdaten aller Leistungserbringer, also auch der Ärzte und Zahnärzte, für alle Versicherten verfügen können; andererseits war aber festgelegt, dass die Leistungsabrechnungsdaten den Krankenkassen nur noch pseudonymisiert übermittelt werden sollten (vgl. 18. TB Nr. 21.1).

Nachfolgend, und zwar im Laufe des Jahres 2001 hat das Bundesministerium für Gesundheit Vorstellungen für ein Gesetz zur Verbesserung der Datentransparenz entwickelt. Die Datenschutzbeauftragten des Bundes und der Länder haben sich im März 2001 hierzu umfassend geäußert (s. Anlage 13). Sie begrüßten ausdrücklich, dass mit dem Arbeitsentwurf ihre Forderung wieder aufgegriffen werden sollte, durch Pseudonymisierung des Abrechnungsverfahrens die Belange des Patientengeheimnisses und des Datenschutzes zu wahren. Der Entwurf fiel allerdings gegenüber dem Entwurf des Jahres 1999 zurück; nunmehr sollte nämlich die Pseudonymisierung der Abrechnungsdaten erst nach Durchführung der Abrechnung aller nichtvertragsärztlichen Leistungen durchgeführt werden. Das Bundesministerium für Gesundheit hat den Arbeitsentwurf letztlich nicht weiterverfolgt.

Anfang des Jahres 2002 wurde das Bundesministerium für Gesundheit nochmals aktiv. Es präsentierte als Minimal-

lösung gegenüber den ursprünglichen Vorhaben seine Überlegungen zur Schaffung eines Datenpools für Steuerungsaufgaben der gesetzlichen Krankenversicherung. Nunmehr soll die derzeitige Rechtslage zur Leistungsabrechnung in der gesetzlichen Krankenversicherung beibehalten – damit wird die aus datenschutzrechtlicher Sicht zu begrüßende Pseudonymisierung des Abrechnungsverfahrens nicht mehr weiter verfolgt – und zusätzlich ein Datenpool geschaffen werden, um Auswertungen für die Gesundheitspolitik und für weitere, noch zu definierende Zwecke zu ermöglichen. Hierfür sollen Daten der Versicherten und der Leistungserbringer in pseudonymisierter Form zusammengeführt und ausgewertet werden können. Die Datenschutzbeauftragten des Bundes und der Länder haben zu diesem Vorhaben ausführlich und grundsätzlich Stellung genommen und die datenschutzrechtlichen Anforderungen an einen solchen Datenpool dargelegt. So muss insbesondere eine Reidentifizierung der Versicherten- und Leistungserbringerdaten ausgeschlossen sein. Dies setzt voraus, dass ein sicheres Pseudonymisierungsverfahren eingesetzt, der Umfang der Datenübermittlung begrenzt und das Reidentifizierungsrisiko minimiert wird, indem u. a. nur aggregierte Auswertungen zugelassen werden. Ein Zugriff auf einzelne Datensätze ist ebenfalls auszuschließen. Auch müssen die Zwecke der Datenaufbereitung ebenso wie die Frage, welche Daten in welchem Umfang erhoben und übermittelt werden und wer Zugriff auf die Daten bekommt, abschließend gesetzlich festgelegt sein.

Ich werde den Fortgang der Überlegungen zu diesem Datenpool kritisch begleiten und mich konstruktiv in die weiteren Vorbereitungen einschalten, um die Berücksichtigung der datenschutzrechtlichen Belange der Versicherten und der Leistungserbringer sicher zu stellen.

24.1.2 Disease-Management-Programme (DMP): Wer kontrolliert die chronisch Kranken?

Der seit dem 1. Januar 1994 bestehende Risikostrukturausgleich soll unterschiedlichen historisch gewachsenen Risikostrukturen Rechnung tragen, die sich insbesondere durch die unterschiedliche Verteilung der Versicherten nach Alter, Geschlecht, Berufs- und Erwerbsfähigkeits-Status sowie durch die Unterschiede in der Zahl der beitragsfrei mitversicherten Familienangehörigen ergeben. Hierbei wurde bisher die besonders kostenaufwendige Versorgung einzelner Versicherter, insbesondere chronisch Kranker, nicht berücksichtigt, sodass sich dies geradezu wettbewerbsnachteilig für die Krankenkassen auswirkte.

Um die finanzielle Belastung der Krankenkassen durch solche Versicherte, für die Aufwendungen erheblich über dem Durchschnitt der Standardausgaben im Risikostrukturausgleich entstehen, zumindest teilweise solidarisch zu finanzieren, wird ein Risikopool aufgebaut. Hierbei sollen die Aufwendungen pro Versicherten für die stationäre Versorgung, die Arzneimittelversorgung, die nichtärztlichen Kosten der ambulanten Dialyse und das Kranken- und Sterbegeld, die über einem bestimmten Schwellenwert im Jahr liegen, teilweise ausgeglichen werden. Diese Aufwendungen können ermittelt werden, ohne dass personenbezogene Daten erhoben werden müssen; die Daten sind bei den beteiligten Stellen bereits vorhanden. Im Risikopool selbst sind die Daten nicht versichertenbezogen. Insofern ist dieser Aspekt des Risikostrukturausgleichs datenschutzrechtlich unbedenklich.

Darüber hinaus sind jetzt allerdings erstmals Disease-Management-Programme (DMP) zur Behandlung chronisch Kranker für bestimmte durch einen Koordinierungsausschuss festgelegte chronische Krankheiten entwickelt worden. Mit dem In-Kraft-Treten der §§ 137f und g SGB V am 1. Januar 2002 (BGBl. I 2001 S. 3465) hat der Gesetzgeber die Einführung dieser DMP dem Grunde nach festgelegt und dabei bereits die wesentliche Grundsatzentscheidung getroffen, wonach den Krankenkassen für diese DMP versichertenbezogene Daten zu übermitteln sind. In diesem Zusammenhang habe ich gemeinsam mit den Datenschutzbeauftragten der Länder großen Wert darauf gelegt, dass die versichertenbezogene Datenübermittlung an die Krankenkassen nur in den Fällen zulässig ist, in denen ein Versicherter freiwillig an einem solchen Programm teilnimmt, also ausdrücklich nach umfassender Information einwilligt, dass seine Daten – zweckgebunden versteht sich – weitergegeben werden dürfen.

Die Einzelheiten der Erhebung, Verarbeitung und Nutzung dieser Daten hat das Bundesministerium für Gesundheit in einer Rechtsverordnung gem. § 266 Abs. 7 SGB V (BGBl. I 2002 S. 2286) festgelegt. Im Rahmen dieser Rechtsverordnung hat ein Koordinierungsausschuss aus Vertretern der Leistungsträger und Leistungserbringer vier geeignete chronische Krankheiten festgelegt (Brustkrebs, Coronare Herzkrankheit, Diabetes, chronisch-obstruktive Atmungserkrankungen), für die teilweise inzwischen strukturierte Behandlungsprogramme aus medizinischer Sicht entwickelt worden sind.

Bei der datenschutzrechtlichen Bewertung dieser ärztlicherseits festgelegten Programme musste zwar von der Regelung des SGB V ausgegangen werden, wonach es dem Grunde nach zulässig ist, dass die Krankenkassen versichertenbezogene Daten erheben und speichern, und zwar auch über ärztliche Leistungen für die festgelegten Zwecke der DMP, andererseits ist es mir unter Mitwirkung der Landesbeauftragten für den Datenschutz gelungen, das Bundesministerium für Gesundheit davon zu überzeugen, den Umfang der Daten zu begrenzen, und eine weitgehende Pseudonymisierung des Versichertenbezuges durch die Einschaltung der Kassenärztlichen Vereinigungen im Rahmen einer Arbeitsgemeinschaft vorzusehen. Für den Fall, dass die strukturierten Behandlungsprogramme ohne Beteiligung der Kassenärztlichen Vereinigung durchgeführt werden und die Krankenkasse somit alle Daten unmittelbar erhält, ist es gelungen, die Selbstbestimmung des Patienten zu stärken, indem dieser in jede einzelne Übermittlung seiner Gesundheitsdaten gesondert schriftlich einwilligen muss, wenn sie vom Leistungserbringer an die Krankenkasse unmittelbar erfolgt. Dadurch wird sichergestellt, dass neben der Freiwilligkeit der Teilnahme an dem strukturierten Behandlungsprogramm insgesamt der Betroffene zusätzlich durch seinen Arzt über die Weitergabe seiner sensiblen Patientendaten jeweils unmittelbar zuvor informiert wird und somit erneut die Gelegenheit hat, dieser Weitergabe im Einzelfall zu widersprechen.

Die Risikostrukturausgleichsverordnung ist zum 1. Juli 2002 in Kraft getreten. Durch den Abschluss von Verträgen zwischen den Kassenärztlichen Vereinigungen und den

Krankenkassen ist es jedoch bisher nicht zu einer unmittelbaren Weitergabe von Daten an eine Krankenkasse im Rahmen dieses DMP gekommen, sodass voraussichtlich dadurch in der Praxis die datenschutzfreundlichere Fallgestaltung zur Anwendung gelangen wird.

Auch bei der Freiwilligkeit der Teilnahme an den Behandlungsprogrammen und der informierten Einwilligung der Patienten in die Weitergabe ihrer sensiblen Daten bleibt aus datenschutzrechtlicher Sicht ein gewisses Unbehagen. Diese vom Gesetzgeber (auch im SGB X) genannte Freiwilligkeit steht in einem gewissen Spannungsverhältnis zu den übrigen gesetzlichen Regelungen, die – insbesondere in der Gesetzlichen Krankenversicherung als Pflichtversicherung – auf den Schutz des Betroffenen abzielen; es stellt sich daher die Frage, ob die Einwilligung generell geeignet ist, den gesetzlichen Schutzzweck „auszuhebeln", da der Patient nur die „Wahl" hat, „mitzumachen" oder „auszusteigen". Es ist somit notwendig, die Durchführung der DMP durch die Krankenkassen sorgfältig zu beobachten und ggf. vor Ort zu kontrollieren.

24.1.3 Neue Modellvorhaben – aber nur datenschutzkonform

Am 21. August 2002 hat der Bundestag mit Zustimmung des Bundesrates das Gesetz zur Änderung des Apothekengesetzes (BGBl. I 2002 S. 3352) beschlossen. Durch Artikel 3 dieses Gesetzes wurde in § 63 SGB V eine Rechtsgrundlage für Modellvorhaben geschaffen, mit denen der Einsatz moderner Informationstechnologien im Gesundheitswesen (Telematik) erprobt werden kann. Diese Modellprojekte, mit denen z. B. die Erprobung einer elektronischen Gesundheitskarte (vgl. Nr. 28.3) oder des elektronischen Rezepts (vgl. Nr. 28.2) möglich wird, sollen zugleich auch die Qualität der medizinischen Versorgung verbessern und einen Beitrag zur Erhöhung der Wirtschaftlichkeit leisten.

Die Durchführung derartiger Modellprojekte erfordert – abhängig von der jeweiligen funktionalen und inhaltlichen Ausgestaltung und Zwecksetzung des Projekts – eine inhaltlich erweiterte Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Dazu muss von mehreren datenschutzrechtlichen Regelungen des Zehnten Kapitels des SGB V abgewichen werden, beispielsweise für die Erprobung einer Patientenchipkarte auf Basis der bisherigen Versichertenkarte von § 291 SGB V.

Bei der Vorbereitung des Gesetzentwurfs habe ich nach Abstimmung mit den Landesbeauftragten für den Datenschutz dem Bundesministerium für Gesundheit (BMG) Hinweise zum Datenschutz gegeben und die weitere Entwicklung des Vorhabens intensiv begleitet. Auf diese Weise konnte mit dem BMG eine Regelung abgestimmt werden, die im Wesentlichen den datenschutzrechtlichen Anforderungen genügt und dem Grundgedanken der freiwilligen, informierten und schriftlichen Einwilligung mit Widerrufsvorbehalt Rechnung trägt.

Dabei konnte ich insbesondere erreichen, dass die folgenden Kernpunkte aufgenommen wurden:

- Erfordernis einer schriftlichen, widerrufbaren Einwilligung der Versicherten, die auf den für das jeweilige Modellvorhaben erforderlichen Umfang der Abweichung von den datenschutzrechtlichen Vorgaben des Zehnten Kapitels des SGB V zu begrenzen ist;
- vorherige schriftliche Unterrichtung der Versicherten, in welchem Umfang von den datenschutzrechtlichen Vorgaben des Zehnten Kapitels des SGB V abgewichen wird und aus welchen Gründen dies erforderlich ist;
- die Einwilligung ist auf Zweck, Inhalt, Art, Umfang und Dauer der Erhebung, Verarbeitung und Nutzung der Daten des Betroffenen sowie der daran Beteiligten zu erstrecken;
- Erweiterungen der Krankenversichertenkarte, mit denen von den datenschutzrechtlichen Vorgaben in § 291 SGB V abgewichen wird, sind nur zulässig, wenn die zusätzlichen Daten informationstechnisch von den in § 291 Abs. 2 SGB V genannten Daten getrennt werden;
- entsprechende Geltung des § 6c BDSG beim Einsatz mobiler Speichermedien, wonach umfassende Unterrichtungspflichten gegenüber dem Betroffenen vorgeschrieben sind;
- unverzügliche Löschung der personenbezogenen Daten, die in Abweichung von den datenschutzrechtlichen Vorschriften des Zehnten Kapitels des SGB V erhoben, verarbeitet und genutzt worden sind, nach Abschluss des Modellversuchs;
- rechtzeitige Benachrichtigung des Bundesbeauftragten für den Datenschutz oder der Landesbeauftragten für den Datenschutz – soweit zuständig – vor Beginn des Modellvorhabens.

Bedauerlicherweise wurden meine Vorschläge für eine Regelung, die es dem Versicherten ermöglicht hätte, über die Verwendung seiner Daten im Einzelfall zu entscheiden, nicht aufgegriffen. Allerdings wurde meinem Vorschlag entsprochen, dass im Rahmen der Modellprojekte zur Erprobung einer elektronischen Gesundheitskarte auch solche Modellvorhaben erprobt werden, in denen der Versicherte über die Verwendung seiner Daten im Einzelfall entscheiden kann oder in denen ihm die Möglichkeit gegeben wird, einzelne ärztliche Fachbereiche (z. B. Psychiatrie, Gynäkologie, Haut- und Geschlechtskrankheiten) vom allgemeinen Zugriff auszuschließen. Des Weiteren wird nach der Gesetzesbegründung (Bundestagsdrucksache 14/8930) mit dieser neu geschaffenen Regelung noch keine Vorentscheidung hinsichtlich einer „flächendeckenden" Einführung einer elektronischen Gesundheitskarte getroffen. Die Regelungen für Modellvorhaben greifen damit einer möglichen späteren Einführung einer elektronischen Gesundheitskarte nicht vor. Bei dieser ist dann sicherzustellen, dass die freie und unbeeinflusste Entscheidung der Versicherten über Einsatz und Verwendung der Karte gewährleistet wird. Hierfür werde ich mich intensiv einsetzen.

24.1.4 Anforderung von Krankenhausentlassungsberichten durch Krankenkassen – geht ein Dauerstreit zu Ende?

In meinem 18. TB (Nr. 21.3) habe ich ausführlich meine Auffassung zur Befugnis der Krankenkassen, von Krankenhäusern Krankenhausentlassungsberichte anzufordern, dargelegt. Diese Auffassung wurde nun durch das Urteil des Bundessozialgerichts vom 23. Juli 2002 – B 3 KR 64/01 R – bestätigt. In diesem legt das Gericht dar, dass die Krankenkassen nicht

aus eigenem Recht Einsicht in Behandlungsunterlagen verlangen können, sondern insoweit auf ein Tätigwerden des Medizinischen Dienstes der Krankenkassen (MDK) angewiesen sind. In § 301 SGB V sei aus datenschutzrechtlichen Gründen abschließend aufgezählt, welche Angaben den Krankenkassen bei einer Krankenhausbehandlung ihrer Versicherten zu übermitteln sind. Behandlungsdaten der Versicherten gehörten nicht hierzu. Für die Krankenkassen sei es zur Erfüllung ihrer Aufgaben auch nicht erforderlich, in die Behandlungsunterlagen der Versicherten Einsicht zu nehmen. Bei Zweifeln an der sachlich-rechnerischen Richtigkeit einer Krankenhausabrechnung habe die Krankenkasse nach § 275 Abs. 1 Satz 1 SGB V eine gutachterliche Stellungnahme des MDK einzuholen. Der MDK sei im Falle einer Abrechnungsprüfung ermächtigt, die erforderlichen Sozialdaten bei den Krankenhäusern anzufordern. Gleichzeitig sei der MDK verpflichtet, der Krankenkasse das Ergebnis der Begutachtung sowie die erforderlichen Angaben über den Befund mitzuteilen.

Damit stellt das Bundessozialgericht klar, dass es allein Aufgabe des MDK ist, medizinische Unterlagen für die sachlich-rechnerische Prüfung der Abrechnung eines Krankenhauses zu beurteilen, und nur der MDK in Behandlungsunterlagen von Versicherten Einsicht nehmen darf. Das Einholen einer Einwilligungserklärung des Versicherten zur Übermittlung von Behandlungsunterlagen – wie von einigen Krankenkassen praktiziert – stellt eine Umgehung der abschließenden Regelung des § 301 SGB V sowie der gesetzlichen Regelung dar, dass allein der MDK für die Prüfung medizinischer Sachverhalte zuständig ist. Forderungen der Krankenkassen an Krankenhäuser und Ärzte, bei Vorliegen einer Einwilligungserklärung des Versicherten die Behandlungsunterlagen an die Krankenkasse zu übermitteln, halte ich aus diesem Grund für rechtlich nicht gedeckt und damit für unzulässig.

Ich werde bei Beratungen und Kontrollen von Krankenkassen weiterhin meine im 18. TB (Nr. 21.3) dargelegte Rechtsauffassung vertreten. Hierauf habe ich auch die Spitzenverbände der Krankenkassen hingewiesen und gebeten, ihre Mitgliedskassen entsprechend zu unterrichten.

24.1.5 Wozu braucht ein Untersuchungslabor personenbezogene Daten?

Sind im Rahmen einer ärztlichen Behandlung labormedizinische Untersuchungen (z. B. von Blut, Urin und anderem Körpermaterial) erforderlich, schaltet der behandelnde Arzt hierfür regelmäßig ein medizinisches Labor ein. Zusammen mit dem Untersuchungsauftrag an das Labor werden auch die genaue Diagnose oder Verdachtsdiagnose und/oder wichtige Befunde angegeben. Nach erfolgter Untersuchung werden diese Daten mit den Untersuchungsergebnissen zusammengeführt und gespeichert. In Großlaboren, die sich aufgrund des zunehmenden Konzentrationsprozesses in diesem Bereich gebildet haben, erfolgen diese Untersuchungen mit computergestützten Analyseautomaten innerhalb kürzester Zeit. Laboratorien mit über 400 000 Fällen pro Jahr sind keine Seltenheit mehr und die größten Labors rechnen jährlich zwei bis vier Millionen Fälle ab. Bei einer solchen Menge von Patientendaten in privaten Datenbanken handelt es sich um eine aus datenschutzrechtlicher Sicht problematische Entwicklung für das Recht auf informationelle Selbstbestimmung der Betroffenen.

Vor diesem Hintergrund habe ich die Kassenärztliche Bundesvereinigung (KBV) und die Bundesärztekammer (BÄK) um Prüfung eines besseren Datenschutzes der Versicherten bei laborärztlichen Untersuchungen gebeten, damit eine Offenlegung der Identität der jeweiligen Versicherten vermieden wird. Hierzu habe ich in Absprache mit den Landesbeauftragten für den Datenschutz vorgeschlagen, auf die Angabe der Stammdaten der Versicherten zu verzichten und Laborüberweisungen nur noch mithilfe von Nummerncodes vorzunehmen. Für Laboruntersuchungen, bei denen die Proben vom behandelnden Arzt eingesandt werden und die Untersuchungsergebnisse an diesen zurückgehen, sind m.E. die Namen der jeweiligen Versicherten nicht erforderlich. Das Labor, soweit es selbst die Laborleistungen mit der Krankenkasse abrechnet, benötigt hierfür lediglich die Krankenversichertennummer und die Krankenkasse des Versicherten. Allerdings dürfte es aus medizinischen Gründen erforderlich sein, dem Laborarzt auch das Geschlecht und das Alter des Patienten mitzuteilen. Eine Umstellung auf ein solches Verfahren wäre m. E. ohne größeren Aufwand möglich, zumal die vertraglich festgelegten Abrechnungswege bestehen bleiben könnten. Auch gibt es bereits Erfahrungen mit entsprechenden Verfahren. So beauftragen einige staatliche Gesundheitsämter private Labore mit der Untersuchung codierter bzw. pseudonymisierter Proben. Auch gibt es Laborgemeinschaften, denen die zu untersuchenden Proben codiert übersandt werden. Die Sicherheit vor einer Verwechslung codierter Proben hängt dabei von der technischen Ausgestaltung und der Zuverlässigkeit des Codierungsverfahrens ab.

Die Gespräche mit der KBV und der BÄK dauern noch an.

24.2 Pflegeversicherung

24.2.1 Gemeinsame Verarbeitung und Nutzung personenbezogener Daten durch Krankenkassen 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, habe ich mich bereits mehrfach befasst (vgl. 16. TB Nr. 24.1, 17. TB Nr. 24.1, 18. TB Nr. 24.1.2).

Da eine Präzisierung der von den Krankenkassen und Pflegekassen gemeinsam zu verarbeitenden und zu nutzenden Daten nicht gelungen ist, 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. Diese Regelung ist auf meinen Vorschlag hin in den Entwurf eines Gesetzes zur Qualitätssicherung und zur Stärkung des Verbraucherschutzes in der Pflege aufgenommen worden. Das Gesetz ist am 1. Januar 2002 (BGBl. I 2001 S. 2320) in Kraft getreten.

Mit dieser Gesetzesänderung ist ein praktikabler und auch datenschutzgerechter Gesetzesvollzug in diesem Bereich erreicht worden.

24.2.2 Pflegedokumentation: Müssen Pflegebedürftige ihrer Krankenkasse besonders intime Daten offen legen?

Mehrere Anfragen von Pflegediensten waren für mich Anlass, zu der Problematik der Einsichtsrechte in die Pflegedokumentation von Pflegebedürftigen Stellung zu nehmen.

Vor dem Hintergrund meiner Ausführungen zum Thema „Anforderung von Krankenhausentlassungsberichten durch Krankenkassen“ (vgl. 18. TB Nr. 21.3), die zwischenzeitlich vom Bundessozialgericht in seinem Urteil vom 23. Juli 2002 – Az.: B3 KR 64/01 R – umfassend bestätigt wurden (vgl. dazu Nr. 24.1.4), ist aus datenschutzrechtlicher Sicht auch bei den Einsichtsrechten der Pflegekassen in die Pflegedokumentation von Pflegebedürftigen eine entsprechende Anwendung der hierzu entwickelten Grundsätze angezeigt.

Zweck und Aufgabe der Pflegedokumentation ist es, die ordnungsgemäße Durchführung der Pflege zu gewährleisten. Die Pflegedokumentation enthält alle pflegerelevanten Daten über den Pflegebedürftigen, wie z. B. Anamnese- und Diagnosedaten oder Angaben zur Pflegeplanung (Ziele, Verlauf und Ergebnisse der Pflege). In der häuslichen Pflege werden Eintragungen vom Pflegebedürftigen selbst sowie von allen an der Pflege Beteiligten (Angehörigen, Pflegekräften, aber auch von Haus- und Notärzten) vorgenommen. Sie ist Eigentum des Pflegedienstes und verbleibt während der Pflege grundsätzlich beim Pflegebedürftigen. Nach Beendigung der Pflege wird die Pflegedokumentation für einen Zeitraum von fünf Jahren beim Pflegedienst aufbewahrt und dann ordnungsgemäß vernichtet. Dieses Verfahren wird vom Verband der Angestelltenkrankenkassen in einem „Beispiel für einen Vertrag über ambulante pflegerische Versorgung“ empfohlen.

Eine gesetzliche Grundlage für die Führung von Pflegedokumentationen ist dem SGB XI nicht zu entnehmen. Die Verpflichtung hierfür ergibt sich insgesamt aus den Rahmenverträgen über die ambulante pflegerische Versorgung nach § 75 SGB XI, die auf Landesebene geschlossen werden. Auch die „gemeinsamen Grundsätze und Maßstäbe zur Qualität und Qualitätssicherung einschließlich des Verfahrens zur Durchführung von Qualitätsprüfungen nach § 80 SGB XI“ vom 31. Mai 1996 sehen in § 14 die Führung einer Pflegedokumentation vor.

Gegen die Führung der Pflegedokumentation in der dargestellten Form ist aus datenschutzrechtlicher Sicht grundsätzlich nichts einzuwenden. Sie ist mit den Aufzeichnungen der stationären Pflegeeinrichtungen bzw. auch mit Aufzeichnungen vergleichbar, wie sie üblicherweise bei der stationären Behandlung im Krankenhaus erfolgen.

Von der Führung der grundsätzlich beim Pflegebedürftigen aufzubewahrenden Pflegedokumentation ist jedoch die Zulässigkeit ihrer Nutzung im Einzelfall zu unterscheiden. Für welche Zwecke die Pflegekassen personenbezogene Daten erheben dürfen, ist in § 94 Abs. 1 SGB XI abschließend geregelt. Die Vorschrift korrespondiert insoweit mit § 284 SGB V für die gesetzliche Krankenversicherung. Zu anderen Zwecken dürfen die erhobenen und gespeicherten Sozialdaten nur verarbeitet oder genutzt werden, soweit dies durch Rechtsvorschriften des Sozialgesetzbuches angeordnet oder erlaubt ist (§ 94 Abs. 2 Satz 1 SGB XI).

Danach könnte eine Nutzung der Pflegedokumentation durch die Pflegekasse als Abrechnungsunterlage (§§ 84 bis 91 und 105 SGB XI) oder als Unterlage für die Überwachung der Wirtschaftlichkeit und Qualität der Leistungserbringung (§§ 79, 80 ff., 112 bis 115, 117 und 118 SGB XI) zulässig sein.

Die an der Pflegeversorgung teilnehmenden Leistungserbringer sind im Zusammenhang mit der Abrechnung der pflegerischen Leistungen verpflichtet, in Abrechnungsunterlagen die von ihnen erbrachten Leistungen nach Art, Menge und Preis einschließlich des Tages und der Zeit der Leistungserbringung aufzuzeichnen, ihr Kennzeichen sowie die Versichertennummer des Pflegebedürftigen anzugeben und bei der Abrechnung über die Abgabe von Hilfsmitteln die Bezeichnungen des Hilfsmittelverzeichnisses nach § 78 SGB XI zu verwenden (vgl. § 105 SGB XI). Dabei wird das Nähere über Form und Inhalt der Abrechnungsunterlagen von den Spitzenverbänden der Pflegekassen im Einvernehmen mit den Verbänden der Leistungserbringer festgelegt. § 106 SGB XI eröffnet die Möglichkeit, den Umfang der zu übermittelnden Daten einzuschränken. Eine Befugnis für zusätzliche Erhebungen wird demgegenüber aber gerade nicht eröffnet.

Als Abrechnungsunterlage für die Pflegekasse kommen daher nur solche Dokumente in Betracht, in denen (Dienst-) Leistungen des Pflegedienstes nach Art, Preis und Menge sowie die Abgabe von Hilfsmitteln nachgewiesen werden. Eine solche Abrechnungsunterlage stellt beispielsweise der so genannnte Leistungsnachweis dar, in dem die durchgeführten Leistungen des Pflegedienstes täglich einzutragen, von der Pflegekraft abzuzeichnen und durch den Pflegebedürftigen bzw. einer von ihm beauftragten Person zeitnah zu bestätigen sind. Zu einer Datenübermittlung, die über den Umfang der in § 105 SGB XI genannten, für die Abrechnung erforderlichen Daten hinaus geht, z. B. der Übermittlung medizinischer Daten der Pflegebedürftigen, wie sie in der Pflegedokumentation vorliegen, ist der Pflegedienst im Rahmen der Leistungsabrechnung mit der Pflegekasse weder verpflichtet noch befugt.

Eine klare Differenzierung zwischen den Abrechnungsunterlagen einerseits und der Pflegedokumentation andererseits ist besonders wichtig, weil die Pflegedokumentation unter anderem Anamnese- und Diagnosedaten und damit außerordentlich sensible Daten enthält und der Pflegeversicherte ein zentrales Interesse daran hat, dass diese Daten nicht unnötig weiterverarbeitet werden. Die Pflegedokumentation ist daher von den Abrechnungsunterlagen unbedingt zu trennen (s. a. LfD Thüringen, 3. TB Nr. 11.21).

Auch eine Einsichtnahme der Pflegekasse in die Pflegedokumentation in Zusammenhang mit der Überwachung der Wirtschaftlichkeit und Qualität der Leistungserbringung scheidet aus. Die Verfahren für diese Überprüfungen sind gesetzlich geregelt (§§ 79, 80 ff., 112 bis 115, 117 und 118 SGB XI). Danach ist es lediglich dem Medizinischen Dienst der Krankenversicherung (MDK) bzw. den bestellten Sachverständigen gestattet, im Rahmen ihrer Aufgaben und Prüfungen Einsicht in Unterlagen mit medizinischen Daten zu nehmen. Ein Recht der Pflegekassen, im Rahmen der Überwachung der Wirtschaftlichkeit und Qualität der Leistungserbringung in Unterlagen mit sensiblen Daten der Pflegebedürftigen einzusehen, sehen diese Regelungen gerade nicht vor.

Die Pflegekasse ist damit nicht befugt, Daten aus der Pflegedokumentation zu erheben. Gleiches gilt für eine entsprechende Übermittlung des Pflegedienstes.

Demgegenüber ist eine Übermittlung der Pflegedokumentation an den MDK anders zu bewerten. Der MDK darf personenbezogene Daten für Zwecke der Pflegeversicherung er-

heben, verarbeiten und nutzen, soweit dies für die Prüfungen, Beratungen und gutachtlichen Stellungnahmen, wie z. B. die Feststellung der Pflegebedürftigkeit oder die Notwendigkeit der Versorgung mit Pflegehilfsmitteln und technischen Hilfen erforderlich ist (§ 97 Abs. 1 Satz 1 SGB XI). Die konkreten Aufgaben des MDK, für die die Verarbeitung von Sozialdaten erforderlich ist, ergeben sich aus § 276 Abs. 6 SGB V sowie §§ 18, 40, 80, 112 bis 115, 117 und 118 SGB XI. Hier lässt sich erkennen, dass der MDK auch für den Bereich der Pflegeversicherung für die Beurteilung medizinischer Fragen zuständig ist. Damit wird der MDK in der Pflegeversicherung – ebenso wie in der gesetzlichen Krankenversicherung – als Gutachter tätig, sodass er in diesem Zusammenhang auch in die Pflegedokumentation von Pflegebedürftigen Einsicht nehmen darf. Zur Abgrenzung der Befugnisse zwischen dem MDK als Gutachter und der Krankenkasse hat das Bundessozialgericht in seinem o. g. Urteil ausgeführt, dass die Krankenkassen kein eigenes Recht auf Einsichtnahme in medizinische Behandlungsunterlagen haben, sondern insoweit auf ein Tätigwerden des MDK angewiesen sind.

Wie in der gesetzlichen Krankenversicherung ist auch in der Pflegeversicherung eine entsprechende Trennung der Aufgaben zwischen MDK und Pflegekasse vorgegeben, sodass die im Bereich der gesetzlichen Krankenversicherung geltenden Grundsätze auf die Pflegeversicherung zu übertragen sind. Damit ist auch in der Pflegeversicherung eine Einsichtnahme der Pflegekasse in die Pflegedokumentation unzulässig.

Aus diesem Grunde sind Abrechungsunterlagen und Pflegedokumentation sorgfältig voneinander zu trennen. Auch für eine Einwilligung durch den Pflegebedürftigen ist in diesem Zusammenhang – wie bei der gesetzlichen Krankenversicherung – kein Raum.

Ich werde die Pflegekassen dazu anhalten, den Umgang mit Pflegedokumentationen in dem aufgezeigten Rahmen zu regeln.

25 Rentenversicherung

25.1 Neue Richtlinien der Bundesversicherungsanstalt für Angestellte verbessern den Datenschutz in der Reha-Klinikgruppe weiter

Die Bundesversicherungsanstalt für Angestellte (BfA) betreibt mehrere Rehabilitationskliniken. In diesen Kliniken wird in hohem Maße mit Daten von Patienten umgegangen. Jeder Patient hat einen grundgesetzlich garantierten Anspruch darauf, dass seine Persönlichkeitsrechte durch den Umgang mit den ihn betreffenden Daten nicht beeinträchtigt werden. Dies gilt insbesondere für Gesundheitsdaten, die in den Kliniken anfallen. Aus diesem Grunde hat die BfA „Richtlinien der BfA für den Datenschutz in der Reha-Klinikgruppe (Datenschutz-Richtlinien)“ erstellt.

Bei der Erarbeitung dieser Richtlinien bin ich frühzeitig beteiligt worden. Schriftlich und in mündlichen Erörterungen sind Anregungen zu dem Entwurf der Richtlinien gegeben worden. Es ist zu begrüßen, dass die BfA diese Anregungen nahezu vollständig übernommen hat. Die Datenschutz-Richtlinien sind für alle Rehabilitationskliniken verbindlich; sie sind für alle Mitarbeiter jederzeit zugänglich. Sie befassen sich insbesondere mit den Grundsätzen des Datenschutzrechts, innerbetrieblichen Maßnahmen zur Sicherung des Datenschutzes, Patientenrechten, der Übermittlung von Sozialdaten an Dritte, Weitergabe des ärztlichen Entlassungsberichts und den Fragen der IT-Sicherheit.

Mit diesen Richtlinien ist es der BfA gelungen, den ohnehin schon sehr hohen Datenschutzstandard der Rehabilitationskliniken der BfA weiter zu verbessern.

25.2 Moderne Technik erleichtert das Verfahren für die Aufnahme von Anträgen auf Rentenversicherungsleistungen

Zu den Aufgaben der Versicherungsämter gehört es nach § 93 Abs. 2 SGB IV, Anträge auf Leistungen aus der Rentenversicherung entgegenzunehmen. Um die Antragstellung – auch für die Versicherten – zu vereinfachen, haben sich die Rentenversicherungsträger für bildschirmunterstützte Anträge eingesetzt. In dem erforderlichen Gesetzgebungsverfahren bin ich frühzeitig beteiligt worden. Durch das Hüttenknappschaftliche Zusatzversicherungs-Neuregelungs-Gesetz vom 21. Juni 2002 (BGBl. I 2002 S. 2167) wurden die erforderlichen gesetzlichen Regelungen in den §§ 148, 150 und 151a SGB VI getroffen. Diese Regelungen beschränken den Online-Zugriff der Versicherungsämter und der Gemeinden bezüglich der Daten des Versichertenkontos auf den tatsächlich hierfür erforderlichen Umfang („Stammdaten“ und einige weitere Daten). Auch ist ein Sicherheitskonzept vorgeschrieben, das die Rentenversicherungsträger und der Verband Deutscher Rentenversicherungsträger im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik zu erstellen haben; dieses muss die nach § 78a SGB X erforderlichen technischen und organisatorischen Maßnahmen enthalten. Außerdem ist die vorherige Zustimmung der jeweiligen Aufsichtsbehörde vor Einrichtung eines automatisierten Antragsaufnahmeverfahrens vorgeschrieben.

Damit ist ein Verfahren festgelegt worden, das den Anforderungen der Praxis und dem Datenschutz gerecht wird.

25.3 Kontrolle von Rehabilitationskliniken der Bundesversicherungsanstalt für Angestellte: Hoher Datenschutz-Standard!

Im Berichtszeitraum habe ich datenschutzrechtliche Kontroll- und Beratungsbesuche in zwei Rehabilitationskliniken in der Trägerschaft der BfA durchgeführt. In verschiedenen Bereichen der Kliniken (u. a. Patientenaufnahme, Stationen, Finanzbuchhaltung, Kasse, Patientenarchiv, Therapiebereich, psychologischer Dienst, Sekretariate der leitenden Ärzte) galt es, die Verarbeitung von Sozialdaten (personenbezogenen Daten der Patienten) hinsichtlich der Wahrung des Sozialgeheimnisses nach § 35 SGB I zu prüfen. Daneben dienten die Besuche dazu, vor Ort wichtige Anregungen für die Datenschutz-Richtlinien (s. a. Nr. 25.1) zu gewinnen.

Aufgrund früherer Kontrollfeststellungen (vgl. 18. TB Nr. 22.2) hat die BfA das Verfahren der Übersendung medizinischer Unterlagen von der Hauptstelle an die Rehabilitationskliniken umgestellt: So habe ich insbesondere geprüft, welche dem Arztgeheimnis unterliegenden personenbezogenen Daten nunmehr der Patienaufnahmestelle für deren Aufgabenerfüllung zugeleitet werden. Neben sonstigen Verwaltungsunterlagen übermittelt die Hauptstelle ihren Rehabilitationskliniken alle medizinischen Unterlagen, etwa

ärztliche Gutachten, nur in einem separaten und besonders gekennzeichneten verschlossenen Umschlag. Dies und die maßgeblichen Regelungen der BfA gewährleisten, dass nur hierzu Befugten, etwa dem zu ständigen Arzt, der vor der Aufnahme der Patienten die Art der Unterbringung festlegt, oder der jeweiligen Station während des Aufenthaltes in der Rehabilitationsklinik medizinische Unterlagen zugänglich sind. Die Patientenaufnahme erhält von den medizinischen Unterlagen keine Kenntnis, auch nicht von Entlassungsberichten. Anders verhält es sich bei Patienten, bei denen eine Anschluss-Heilbehandlung erforderlich ist. Hier erhält die Patientenaufnahmestelle zulässigerweise Kenntnis der medizinischen Daten, da ihr in diesem Bereich zusätzliche Aufgaben übertragen sind, die die Kenntnisnahme solcher Unterlagen erfordern. Gegen das vorgefundene Verfahren bestehen keine datenschutzrechtlichen Bedenken.

Auch der Umgang mit Patientendaten auf den Stationen ist ebenso in Ordnung wie der Inhalt der stichprobenartig überprüften Patientenakten sowie deren Aufbewahrung im Patientenarchiv nach der Entlassung der Patienten.

Einzelfeststellungen in anderen Bereichen der Kliniken, etwa das Auffinden von Unterlagen, die bereits hätten gelöscht sein müssen, habe ich unmittelbar mit den Verantwortlichen besprochen, sodass noch vor Ort die notwendigen Veranlassungen getroffen werden konnten.

Insgesamt habe ich es als sehr sinnvoll empfunden, dass während der beiden Besuche Gelegenheit bestand, mit den beteiligten Mitarbeitern der Hauptstelle der BfA, insbesondere aber mit den Verantwortlichen der Rehabilitationskliniken alle datenschutzrechtlich relevanten Punkte konstruktiv vor Ort zu erörtern. Auch die Tatsache, dass die Erkenntnisse der Beratungs- und Kontrollbesuche in die o. a. Datenschutz-Richtlinien eingeflossen und somit zwischenzeitlich für alle BfA-Rehabilitationskliniken verbindlich sind, bewerte ich als positiv.

Zusammenfassend habe ich vom Datenschutz in beiden Rehabilitationskliniken der BfA erneut einen positiven Eindruck gewonnen.

26 Unfallversicherung

26.1 Gutachtertätigkeit

Seit In-Kraft-Treten der Gutachterregelung des § 200 Abs. 2 SGB VII am 1. Januar 1997 war ich immer wieder mit der Gutachtertätigkeit in der gesetzlichen Unfallversicherung befasst und habe dabei verschiedene Aspekte dieser Problematik geprüft (vgl. 17. TB Nr. 23.4, 18. TB Nr. 23.1). Auch in diesem Berichtszeitraum haben sich wieder zahlreiche Petenten an mich gewandt, die sich in ihren Rechten nach § 200 Abs. 2 SGB VII verletzt fühlten. Daher habe ich wieder zahlreiche Gespräche zu dieser Thematik mit dem Bundesversicherungsamt, der Aufsichtsbehörde der Berufsgenossenschaften, dem Hauptverband der gewerblichen Berufsgenossenschaften (HVBG) und Vertretern einzelner Berufsgenossenschaften geführt, um die Rechte der Versicherten beim Umgang mit ihren persönlichen Daten im unfallversicherungsrechtlichen Feststellungsverfahren zu verbessern. Um mir einen Einblick in die Handhabung des § 200 Abs. 2 SGB VII in der Praxis zu verschaffen, habe ich bei drei Berufsgenossenschaften Kontrollen durchgeführt, die ich auf spezielle Fragestellungen beschränkt habe: Zahlreiche Akten der Berufsgenossenschaften wurden danach überprüft,

- in welchem Umfang dem Versicherten das Recht eingeräumt wurde, selbst einen Gutachter vorzuschlagen;
- ob bei der Einschaltung eines beratenden Arztes ein Gutachtenauftrag im Sinne des § 200 Abs. 2 SGB VII erteilt wurde, ohne dass dem Versicherten die in dieser Vorschrift genannten Rechte gewährt wurden;
- ob der Versicherte diese Rechte auch bei der Einschaltung eines Zusatzgutachters wahrnehmen konnte.

Ich werte es als großen Erfolg, der auf eine weitere Verbesserung der datenschutzrechtlichen Positionen der Versicherten im unfallversicherungsrechtlichen Feststellungsverfahren hoffen lässt, dass sich alle Beteiligten trotz der nunmehr lang andauernden Erörterungen und teilweise sehr divergierenden Auffassungen immer wieder zu gemeinsamen Gesprächen bereit finden, auch wenn in einzelnen Fragen eine gemeinsame Lösung noch offen ist.

26.1.1 Vorschlagsrecht der Versicherten: Gesetzliche Regelung endlich in Sicht?

In einer Vielzahl von Eingaben haben Versicherte beklagt, dass die Berufsgenossenschaften einen von ihnen vorgeschlagenen Gutachter nicht beauftragt haben. Die Berufsgenossenschaften müssen einem Gutachtervorschlag des Versicherten zwar nicht folgen, eine Ablehnung des Vorschlags muss jedoch nachvollziehbar begründet werden. In einigen Eingabefällen bestanden insoweit erhebliche Bedenken. So halte ich es nicht für eine tragfähige Begründung, wenn die Berufsgenossenschaft einen von einer Versicherten vorgeschlagenen Gutachter mit der Begründung ablehnt, dessen Praxis sei weiter vom Wohnort der Versicherten entfernt als die Praxis der von der Berufsgenossenschaft benannten Gutachter. Hier bietet sich als Lösung an, dass der Versicherte die durch die weitere Entfernung bedingten Kosten selbst übernimmt.

Bei meinen stichprobenhaften Kontrollen habe ich hinsichtlich des Rechts der Versicherten, selbst einen Gutachter vorschlagen zu können, wenig Schwierigkeiten festgestellt. Bei zwei Berufsgenossenschaften wurde in der Regel einem Gutachtervorschlag des Versicherten gefolgt. Bei der dritten Berufsgenossenschaft habe ich keine Akte gefunden, in der ein Versicherter einen Gutachter vorgeschlagen hatte.

Meiner Empfehlung, zur Stärkung dieser Rechtsposition der Versicherten zu Beginn des Verfahrens einen Hinweis auf das Gutachtervorschlagsrecht zu geben, sind die meisten Berufsgenossenschaften jedoch nicht gefolgt. In meinem 18. TB (Nr. 23.1.2) habe ich über die sehr positiven Erfahrungen mit einem diesbezüglichen Pilotverfahren berichtet. Dabei wurde der Versicherte auf dieses Recht hingewiesen und darüber informiert, ob und ggf. welcher Gutachter für die Berufsgenossenschaft auch als beratender Arzt tätig ist. Im Berichtszeitraum haben zwei weitere Berufsgenossenschaften dieses Verfahren durchgeführt und ebenfalls eine durchweg positive Bilanz gezogen: Nach ihren Erfahrungen mit dem Modellversuch sei nicht zu erwarten, dass in nennenswertem Umfang nicht verwertbare Gutachten erstellt würden, die zu unnötigen Nachbesserungen und Verfahrensverzögerungen führten. Zu meinem Bedauern hat sich der HVBG jedoch noch nicht entschließen

können, eine Empfehlung für alle Berufsgenossenschaften auszusprechen, dieses Verfahren allgemein umzusetzen.

Ich habe mich wiederholt für das Recht der Versicherten eingesetzt, im unfallversicherungsrechtlichen Feststellungsverfahren selbst einen Gutachter vorschlagen zu können. Auf meine Anregung im 18. TB hin hat der Deutsche Bundestag das zuständige Ressort beauftragt, die Aufnahme des Gutachtervorschlagsrechts der Versicherten in das SGB VII zu prüfen.

26.1.2 Einsatz des beratenden Arztes im Feststellungsverfahren

Wie in den Jahren zuvor lag auch in diesem Berichtszeitraum der Schwerpunkt der Gutachterproblematik darin, ob dem Versicherten die Rechte des § 200 Abs. 2 SGB VII auch dann zu gewähren sind, wenn ein beratender Arzt des Unfallversicherungsträgers (UVT) zu einer Stellungnahme aufgefordert wird. In zahlreichen Eingabefällen und bei Kontrollen habe ich festgestellt, dass viele UVT dem Versicherten nicht mehrere Gutachter zur Auswahl benennen und ihm kein eigenes Gutachtervorschlagsrecht gewähren, wenn ein Gutachtenauftrag an einen beratenden Arzt erteilt wurde. Die von den UVT vertretene Auffassung, dass der beratende Arzt wie ein Mitarbeiter der Verwaltung tätig sei, die Weitergabe der Daten des Versicherten keine Datenübermittlung, sondern eine interne Nutzung der Daten innerhalb der Verwaltung sei und deshalb ein Gutachten dieses Mitarbeiters ohne Berücksichtigung des § 200 Abs. 2 SGB VII eingeholt werden dürfe, widerspricht dem eindeutigen Wortlaut dieser Vorschrift. Mit der Formulierung „vor Erteilung eines Gutachtenauftrages“ knüpft diese Vorschrift inhaltlich an ein Gutachten an und unterscheidet nicht zwischen einem internen und externen Gutachter. Eine Aushebelung des Gutachterauswahl- und -vorschlagsrechts entgegen der eindeutigen Intention des Gesetzgebers durch Einführung eines im Gesetz nicht genannten Kriteriums habe ich als unzulässig bewertet. Die mit der Schaffung des § 200 Abs. 2 SGB VII vom Gesetz beabsichtigte Verbesserung der Verfahrenstransparenz und Stärkung der Mitwirkungsrechte des Versicherten lässt eine solche Auslegung nicht zu.

Auch das Bundesversicherungsamt (BVA), die Aufsichtsbehörde der Berufsgenossenschaften, hat sich dieser Argumentation nicht verschlossen. Zwar hält das BVA meine im 18. TB (Nr. 23.1) vorgestellten Fallkonstellationen, in denen eine beratungsärztliche Tätigkeit angenommen werden kann, für seine Aufgabenstellung nicht für hilfreich, da anhand dieser Kriterien eine nachträgliche Rechtsmäßigkeitsbewertung nur schwer nachvollziehbar sei. Ich habe jedoch mit dem BVA Übereinstimmung erzielt, dass die Kriterien zur Abgrenzung der Tätigkeit eines beratenden Arztes von denen eines Gutachters im Rahmen der Auftragsvergabe berücksichtigt werden können. Nach dem Wortlaut des § 200 Abs. 2 SGB VII werden dem Versicherten die genannten Rechte vor Erteilung eines Gutachtenauftrages gewährt. Für die aufsichtsrechtliche Überprüfung im Rahmen dieser Vorschrift bietet es sich daher an, der Prüfung die Formulierung des Gutachtenauftrages zugrunde zu legen. So kann beispielsweise anhand des Textes geprüft werden, ob damit nur eine allgemeine Erläuterung medizinischer Begriffe oder aber eine umfassende Begutachtung angefordert wird. Ich halte das für eine gute Diskussionsgrundlage, von der Definition eines Zusammenhangsgutachtens auszugehen, wie sie von den UVT für die Gebührenzahlung selbst entwickelt wurde. Danach ist ein Zusammenhangsgutachten die eigenständige Ursachenbewertung der vorliegenden und erhobenen Befunde unter Heranziehung und Würdigung der in der jeweiligen Anspruchsnorm aufgeführten Voraussetzungen. Übertragen auf den Gutachtenauftrag im Sinne des § 200 Abs. 2 SGB VII sind dem Versicherten die in dieser Vorschrift genannten Rechte dann zu gewähren, wenn die Bitte um Stellungnahme durch die Berufsgenossenschaft so formuliert ist, dass sie auf eine umfassende Bewertung ausgerichtet ist bzw. wenn die Formulierung unter Angabe der Berufskrankheit so offen gehalten ist, dass eine umfassende Bewertung zu erwarten ist. Ich bin zuversichtlich, dass dieser Lösungsansatz, der sowohl der Aufsichtsbehörde die Erfüllung ihrer Aufgaben ermöglicht als auch die mit dem HVBG bereits entwickelten Kriterien berücksichtigt, für alle Beteiligten akzeptabel ist. Bei den auch weiterhin zu führenden Gesprächen werde ich mich dafür einsetzen, dass die Rechte der Versicherten auf eine Verbesserung der Verfahrenstransparenz und Mitwirkung im unfallversicherungsrechtlichen Feststellungsverfahren in größtmöglichem Umfange gewährleistet werden.

26.1.3 Arzt im Gerichtsverfahren: beratender Arzt oder Gutachter?

In meinem 18. TB (Nr. 23.1.3.2) habe ich bereits berichtet, dass sich die Vorschrift des § 200 Abs. 2 SGB VII, wonach der UVT den Versicherten vor Erteilung eines Gutachtenauftrages mehrere Gutachter zur Auswahl benennen soll, hauptsächlich auf diesbezügliche Entscheidungen der Verwaltung bezieht. Nach ihrem Wortlaut ist diese Vorschrift jedoch auch anwendbar, wenn der UVT ein Gutachten während eines anhängigen Gerichtsverfahrens einholt. In dieser Fallkonstellation weicht zwar die Interessenlage in einigen Punkten von dem Hauptanwendungsfall ab; der Sozialdatenschutz bleibt jedoch auch hier erhalten. Die UVT können nicht nach Belieben über die Daten der Versicherten verfügen. Auch als Beteiligter eines Sozialgerichtsverfahrens bleiben sie – bezogen auf ihre eigene Datenverarbeitung – den Regelungen des Sozialgesetzbuches unterworfen, soweit nicht das Sozialgerichtsgesetz etwas anderes bestimmt. Damit gelten für die UVT für das Verfahren zur Beibringung eines Beweismittels nicht die Verfahrensregelungen des Sozialgerichtsgesetzes, sondern die Bestimmungen des Verwaltungsverfahrens nach dem Sozialgesetzbuch. Im Rahmen dieser Regelungen können die UVT als Partei eines Gerichtsverfahrens die Daten des Versicherten nutzen, um ihre Rechtsauffassung zu stützen. Sie können beispielsweise durch einen beratenden Arzt medizinische Sachfragen klären oder ein vom Gericht eingeholtes Gutachten erläutern lassen. Die Einholung eines Gegengutachtens ist aber nur im Rahmen der Vorschriften des Sozialgesetzbuches zulässig.

In letzter Zeit war ich mehrfach mit Eingaben befasst, in denen Versicherte der gesetzlichen Unfallversicherung sich darüber beklagten, dass die jeweils zuständigen UVT während eines anhängigen Sozialgerichtsverfahrens ein Gutachten des beratenden Arztes eingeholt hätten, ohne ihm die nach den datenschutzrechtlichen Regelungen des Sozialgesetzbuches vorgesehenen Rechte zu gewähren. Ich habe den UVT meine Auffassung mitgeteilt und die Löschung der unter Nichtbeachtung des § 200 Abs. 2 SGB VII eingeholten Gutachten empfohlen. Dieser Empfehlung sind die UVT

bislang nicht gefolgt. Ich werde mich daher weiter bemühen, mit den einzelnen Berufsgenossenschaften und auch mit dem HVBG eine praktikable und datenschutzfreundliche Lösung zu finden. Ein abschließendes Ergebnis konnte in dieser Frage bislang nicht erzielt werden.

26.1.4 Auswahlrecht auch bei Zusatzgutachten

Aus einer Vielzahl von Eingaben und auch bei Kontrollen habe ich den Eindruck gewonnen, dass die Gutachterauswahlregelung des § 200 Abs. 2 SGB VII insbesondere bei der Vergabe von Zusatzgutachten Schwierigkeiten bereitet. Der Wortlaut der Vorschrift ist insoweit eindeutig. Bei Zusatzgutachten handelt es sich ebenfalls um Gutachten im Sinne der Vorschrift, die zwischen Haupt- und Zusatzgutachten nicht unterscheidet.

In vielen Fällen hatten die UVT den Versicherten drei Gutachter zur Auswahl benannt. Dabei war den Versicherten mitgeteilt worden, der ausgewählte Gutachter werde den weiteren Verlauf mit ihnen absprechen, wenn Begutachtungen auf anderen Fachgebieten erforderlich seien. Dies wurde sogar bei äußerst schweren Unfällen so gehandhabt, obwohl absehbar war, dass Gutachten auf mehreren Fachgebieten benötigt wurden. So wurden beispielsweise einem schwer verletzten Versicherten drei Gutachter auf chirurgischem Fachgebiet vorgeschlagen. Der hieraus ausgewählte Gutachter vergab dann Gutachten auf neurologischem, psychiatrischem, HNO-ärztlichem und augenärztlichem Fachgebiet, ohne dass der Versicherte für diese weiteren Aufträge einen von drei benannten Gutachtern auswählen oder selbst einen von ihm gewünschten Gutachter vorschlagen konnte.

Der von einem UVT unter Beachtung des § 200 Abs. 2 SGB VII beauftragte Gutachter ist nicht befugt, eigenmächtig einen oder mehrere Zusatzgutachter zu beauftragen. Ein solches Vorgehen berücksichtigt nicht, dass die Berufsgenossenschaft in allen Verfahrensschritten die Herrin des Verfahrens bleibt. Es ist auch nicht mit der Intention des § 200 Abs. 2 SGB VII vereinbar, durch einen Gutachter ohne Wissen des Versicherten weitere Zusatzgutachter beauftragen zu lassen, weil dieser seine Mitwirkungsrechte und sein Widerspruchsrecht nach § 76 Abs. 2 SGB X gegen die Übermittlung seiner Sozialdaten an die Zusatzgutachter nicht ausüben kann. Daher sind dem Versicherten vor jeder Beauftragung mit einem Zusatzgutachten auch insoweit mindestens drei Gutachter zur Auswahl zu benennen. Das gilt auch dann, wenn ein von der Berufsgenossenschaft beauftragter Gutachter erst im Laufe der Untersuchung oder Bearbeitung feststellt, dass er ein weiteres Gutachten benötigt. Auch in diesem Fall müssen die Rechte des Versicherten beachtet werden. Bei meinen Kontrollen habe ich mit den meisten Berufsgenossenschaften eine Einigung darüber erzielt, dass der Versicherte zumindest in dem Schreiben zur Gutachterauswahl auf sein Recht hingewiesen wird, auch die Zusatzgutachter auswählen bzw. selbst vorschlagen zu können.

26.2 Verwertungsverbot bei unzulässiger Datenerhebung: Erschleichung eines Obduktionsergebnisses

Einer Petentin wurden Leistungen für Hinterbliebene nach dem SGB VII versagt, weil die Berufsgenossenschaft der chemischen Industrie sich unter Verstoß gegen datenschutzrechtliche Vorschriften den Obduktionsbericht ihres verstorbenen Mannes beschafft hatte. Nach dem Tode des Ehemanns, der seit längerer Zeit an einer als Berufskrankheit anerkannten Asbestose erkrankt war, ermittelte die Berufsgenossenschaft hinsichtlich der Todesursache. Nach § 63 Abs. 2 SGB VII besteht bei bestimmten Erkrankungen, zu denen auch eine Asbestose zählt, eine Rechtsvermutung dafür, dass der Tod des Versicherten infolge der Berufskrankheit eingetreten ist. Das Gesetz stellt ausdrücklich klar, dass eine Obduktion zum Zwecke einer solchen Feststellung nicht gefordert werden darf.

Im vorliegenden Fall hatte die Petentin auf Anfrage des behandelnden Arztes einer Obduktion zu ausschließlich wissenschaftlichen Zwecken zugestimmt. Den entsprechenden Obduktionsbefund wollte die Berufsgenossenschaft trotz der bestehenden Rechtsvermutung unbedingt zur Klärung von Kausalitätsfragen nutzen: Wenige Tage nach der Obduktion forderte sie die Petentin telefonisch unter Hinweis auf eine Verkürzung der Bearbeitungsdauer auf, den Obduktionsbericht zu übersenden. Dieses Vorgehen steht nicht im Einklang mit den datenschutzrechtlichen Voraussetzungen für eine Einwilligung. Nach § 67b SGB X ist eine Einwilligung des Betroffenen nur wirksam, wenn er auf den Zweck der vorgesehenen Verarbeitung oder Nutzung hingewiesen wird, die Einwilligung auf freier Entscheidung beruht und – entsprechend dem in Satz 3 der Vorschrift normierten Schriftformerfordernis – schriftlich erteilt worden ist. Auch die Anforderung des Obduktionsbefundes beim Krankenhaus war datenschutzrechtlich nicht zulässig. Der Obduktionsbericht konnte ausschließlich aufgrund der Zustimmung der Angehörigen zu der Obduktion erstellt werden, sodass eine Auskunftsverpflichtung der Ärzte nur im Umfang dieser Einwilligung bestehen konnte. Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen hat in ihrer Zuständigkeit für die Einhaltung datenschutzrechtlicher Vorschriften durch das Krankenhaus die Übersendung des Obduktionsbefundes an die Berufsgenossenschaft als unzulässig bewertet. Die Petentin war auch nicht – wie von der Berufsgenossenschaft behauptet – verpflichtet, den Obduktionsbericht aufgrund einer Mitwirkungsobliegenheit an die Berufsgenossenschaft herauszugeben, da sie die Einwilligung zur Obduktion auf die Entnahme des Tumors zu wissenschaftlichen Zwecken beschränkt hatte. Diese eindeutige Zweckbindung kann keine Mitwirkungsverpflichtung begründen.

Der somit unter Verletzung zahlreicher datenschutzrechtlicher Vorschriften erhobene Obduktionsbericht ist nach § 84 Abs. 2 SGB X zu löschen. Diese Auffassung wird von dem Bundesversicherungsamt geteilt sowie auch vom Petitionsausschuss des Deutschen Bundestages befürwortet. Dennoch hat die Berufsgenossenschaft den Antrag der Petentin abgelehnt. Der gegen diese Entscheidung erhobenen Klage wurde in erster Instanz stattgegeben. Die Berufsgenossenschaft hat hiergegen indes Berufung eingelegt. Ich werde mich auch im weiteren Verlauf dieser Angelegenheit für die Beachtung der datenschutzrechtlichen Vorschriften einsetzen.

26.3 Sozialdaten in Regressfällen

Eine Petentin war auf dem Weg zur Arbeit unverschuldet in einen Autounfall verwickelt worden und hatte dabei schwerste, bleibende Gesundheitsschäden erlitten. Sie

fühlte sich zumindest finanziell gut abgesichert, da sie die Übernahme der Kosten nicht nur von der gegnerischen Haftpflichtversicherung verlangen konnte, sondern auch von der gesetzlichen Unfallversicherung und ihrer privaten Unfallversicherung. In dieser Hoffnung wurde sie jedoch enttäuscht, da die Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege (BGW) als zuständiger gesetzlicher Unfallversicherungsträger unter Missachtung datenschutzrechtlicher Vorschriften ein Gutachten in Auftrag gab, das zu unrichtigen Ergebnissen kam. Über die Beanstandung in diesem Fall habe ich bereits im 18. TB (Nr. 23.1) berichtet. Das rechtswidrig eingeholte Gutachten, demzufolge die schweren Gesundheitsschäden nicht auf den Unfall zurückzuführen wären, gelangte über eine Indiskretion des beratenden Arztes auch zu der privaten Unfallversicherung und zur gegnerischen Haftpflichtversicherung. Obwohl sich die ärztliche Einschätzung später als falsch erwies und der Bescheid der BGW aufgehoben wurde, hatte die Petentin neben den körperlichen Leiden auch finanzielle Unsicherheiten und Einbußen zu ertragen, da die beiden privaten Versicherungen aufgrund des unrichtigen Gutachtens ebenfalls nicht zahlten.

Auch wenn grundsätzlich bei jedem Unfall Datenübermittlungen zwischen den gesetzlichen Unfallversicherungsträgern und den privaten Haftpflichtversicherern der Unfallgegner erfolgen und im Rahmen von so genannten „Teilungsabkommen“ zur Erleichterung der Regressabwicklung alle Daten übermittelt werden, die benötigt werden, um gegenüber der privaten Haftpflichtversicherung das Bestehen eines Anspruches nachzuweisen, halte ich allerdings eine Konkretisierung dieser Datenübermittlungen auch bei der Durchführung von Erstattungs- und Ersatzansprüchen für wichtig, da sich sonst ein Betroffener, der sich mit einer unrechtmäßigen Ablehnung seines Antrags durch die Berufsgenossenschaft auseinander setzen muss, aufgrund einer vorschnellen und übermäßigen Übermittlung seiner Daten möglicherweise mit den gleichen Einwänden durch den Haftpflichtversicherer des Unfallgegners konfrontiert sieht. Die BGW hat mir darin zugestimmt, dass im Hinblick auf die hohe Sensibilität der Daten und die Verantwortung der übermittelnden Stelle besonders hohe Anforderungen an die Erforderlichkeit der Übermittlung zu stellen sind. Ein von mir angeregtes Abwarten bis zur Bestandskraft des Bescheides hat die Berufsgenossenschaft aber abgelehnt, da in Regressverfahren zivilrechtliche Grundsätze und damit auch Verjährungsfristen gelten, und bei umfangreichen, komplizierten Fällen mit einer langen Verfahrensdauer gerechnet werden müsse. Dieses Argument vermag nicht vollständig zu überzeugen: In der Vielzahl der Fälle wird es – wie bei der geschilderten Eingabe – nicht um komplizierte Sachverhalte gehen. In den Fällen, in denen ein Versicherter Klage gegen den ablehnenden Bescheid der Berufsgenossenschaft erhebt, sodass es nunmehr auf die Rechtskraft und nicht mehr auf die Bestandskraft ankommt, könnten andere Kriterien für eine gestaffelte Übermittlung herangezogen werden, die sich an der Erforderlichkeit und der Verhältnismäßigkeit orientieren. Ich habe mich mit der BGW dahin gehend geeinigt, dass die BGW einige Fallgruppen von Datenübermittlungen an private Haftpflichtversicherer aufstellen wird, die sich jeweils an der Erforderlichkeit ausrichten. Die BGW hat zugesagt, wegen der grundsätzlichen Bedeutung dieser Frage auch an den Hauptverband der gewerblichen Berufsgenossenschaften heranzutreten.

26.4 Welche Daten sind zur Festsetzung der Beitragszahlungen erforderlich?

Im Berichtszeitraum lagen mir mehrere Anfragen von ambulanten Pflegediensten vor, ob die Praxis der zuständigen Berufsgenossenschaft, Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege (BGW), zulässig ist, nicht nur die nach dem SGB VII erforderlichen Angaben, sondern darüber hinaus die Herausgabe der Arbeitsverträge und Gesellschaftsverträge zu verlangen. Nach der gesetzlichen Regelung der §§ 191, 192 SGB VII sind die Unternehmen verpflichtet, dem zuständigen Unfallversicherungsträger alle für die Festlegung der Versicherungspflicht relevanten Angaben zu machen und insbesondere jede Veränderung in den Gesellschaftsverhältnissen mitzuteilen. Die Regelung des § 192 Abs. 3 SGB VII, wonach dem Unfallversicherungsträger auf Verlangen auch Beweisurkunden vorzulegen sind, steht unter dem allgemeinen Verhältnismäßigkeitsgrundsatz. Nach dem im Absatz 1 und 2 der Vorschrift festgeschriebenen Regelfall enthält der Unfallversicherungsträger die für ihn erforderlichen Angaben durch die Mitteilung der Gesellschafter. Dieses dem Verhältnismäßigkeitsgrundsatz entsprechende Verfahren würde durch eine generelle Vorlagepflicht eines Urkundsbeweises anstelle einer bloßen Mitteilung der Gesellschafter auf den Kopf gestellt. Ich kann mich zwar der Argumentation der BGW nicht ganz verschließen, wegen des hohen Anteils der Gesellschaftsform der GmbH und einer häufigen Änderung der Gesellschaftsanteile seien in der Vergangenheit vielfach die Änderungsmitteilungen unterblieben. Die generelle Anforderung von Gesellschafts- und Arbeitsverträgen entgegen einer vom Verhältnismäßigkeitsgrundsatz getragenen gesetzlichen Regelung scheint mir jedoch zu weit zu gehen, zumal das Problem der BGW bei möglichen Vertragsänderungen auch so nicht behoben ist. Ich habe der BGW ein klärendes Gespräch angeboten, um eine datenschutzfreundlichere Lösung zu finden, und werde mich weiterhin dafür einsetzen.

26.5 Hilfe für den Staatsanwalt?

Verschiedene Unfallversicherungsträger (UVT) waren von den jeweils zuständigen Staatsanwaltschaften aufgefordert worden, nach einem Arbeitsunfall eines Versicherten die Untersuchungsberichte des Technischen Aufsichtsdienstes herauszugeben, wenn der Verdacht bestand, der Unfall könnte auf ein rechtswidriges Tun oder Unterlassen eines anderen Beschäftigten zurückzuführen sein. Unter Berufung auf den Sozialdatenschutz hatten die UVT das Herausgabeverlangen abgelehnt, während die Staatsanwaltschaften eine Herausgabe nach den allgemeinen Übermittlungsnormen des Sozialgesetzbuches für zulässig erachteten. Dem Konflikt um die rechtliche Auslegung der datenschutzrechtlichen Vorschriften, die eine Herausgabe des Unfallberichts des Technischen Aufsichtsdienstes der Berufsgenossenschaften betreffen, liegen verschiedene und durchaus berechtigte Interessen zugrunde. Für die Staatsanwaltschaften ist es sinnvoll, auf vorhandene Unterlagen zurückzugreifen, der geschädigte Arbeitnehmer hat möglicherweise ein Interesse an einer umfassenden Aufklärung, da er nach einer Verurteilung wegen Körperverletzung auf diese Feststellung einen Schmerzensgeldanspruch stützen kann. Der Beschuldigte hingegen mag befürchten, dass die Ermittlungen verfälscht werden, da der Unfalluntersuchungsbericht von juristischen Laien in einem andern Zusammenhang erstellt wurde und bei

Befragungen der Beschäftigten die Zeugen- und Beschuldigtenrechte nach der Strafproze ssordnung nicht berücksichtigt werden. Die UVT ihrerseits sind für die gespeicherten Daten verantwortlich und haben die datenschutzrechtlichen V orschriften zu beachten.

Nach den abschließenden Übermittlungsnormen des Sozialgesetzbuches haben sich die UVT zu Recht geweigert, die Untersuchungsberichte des T echnischen Aufsichtsdienstes an die Staatsanwaltschaften herauszugeben. Die Übermittlungsnorm des § 69 Abs. 1 SGB X knüpft an gerichtliche Verfahren – einschließlich Strafverfahren – an, die mit der Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch zusammenhängen. Nur in diesen Fällen kann ein UVT die personenbezogenen Daten eines Versicherten weitergeben, wenn dies zur Erfüllung seiner gesetzlichen Aufgabe erforderlich ist. Die Datenübermittlungsbefugnis setzt immer einen in dieser Vorschrift genannten Tatbestand voraus: Die Übermittlung muss für Zwecke erfolgen, für die die Daten erhoben worden sind, für eine Aufgabe der übermittelnden Stellen nach dem Sozialgesetzbuch oder für die Aufgabe eines anderen Sozialleistungsträgers. Handelt es sich dagegen nicht um die Übermittlung zur Erfüllung einer Aufgabe nach dem Sozialgesetzbuch, ist § 69 SGB X nur anwendbar, wenn ein gerichtliches V erfahren anhängig ist. In diesen Fällen werden die Anforderungen an die Übermittlung von Sozialdaten an Ermittlungsbehörden und Staatsanwaltschaften dadurch verschärft, dass nach der Spezialregelung des § 73 SGB X die Datenübermittlung zur Durchführung eines Strafverfahrens durch einen Richter angeordnet werden muss. Im Hinblick auf die besondere Sensibilität der durch das Sozial geheimnis geschützten Daten erachte ich diese erhöhte Schutzschwelle für sachgerecht.

Um die UVT nicht dem Konflikt zwischen ihrer V erpflichtung zum Schutz der Sozialdaten und dem Herausgabeverlangen durch Staatsanwaltschaften, die zum T eil auch Durchsuchungs- und Herausgabebeschlüsse bei den Amtsgerichten erwirken konnten, auszusetzen, habe ich das Bundesministerium für Arbeit und Sozialordnung um eine gesetzliche Klarstellung gebeten.

26.6 Sozialdaten in der Mülltonne?

In einem Einzelfall wurden mir Sozialdaten einer Versicherten mit sehr sensiblen me dizinischen Angaben und Prüfungsunterlagen einer Mitarbeiterin einer Berufsgenossenschaft mit einem anonym verfassten Begleitschreiben zugesandt. Der namentlich nicht genannte Einsender äußerte seine Sorge über den angeblich unsachgemäßen Umgang mit Daten durch die Bezirksverwaltung einer Berufsgenossenschaft. Er gab an, dass er bereits mehrfach beobachtet habe, dass ein Mitarbeiter di eser Bezirksverwaltung, den er genau beschreiben konnte und dessen Autokennzeichen er nannte, ähnliche Schriftstücke in eine Mülltonne geworfen habe.

Zur Klärung dieser V orkommnisse habe ich eine datenschutzrechtliche Kontrolle in der betrof fenen Bezirksverwaltung durchgeführt. Im Ra hmen eines Gespräches ist nachvollziehbar dargelegt worden, dass sich der Verlust der Akte und der Prüfungsunterla gen nicht auf die Art und Weise zugetragen haben konnte, wie sie von dem Einsender der Unterlagen geschildert wurde. Es waren vielmehr deutliche Anhaltspunkte dafür vorhanden, dass die Unterlagen von einem „Insider“ der Berufsgenossenschaft aus dem Büro eines Mitarbeiters entwendet worden waren. Eine Anzahl von Formulierungen in dem anonymen Schreiben spricht für eine persönliche Animosität gegen den gut erkennbar skizzierten Mitarbeite r der Berufsgenossenschaft und die Absicht, diesem schaden zu wollen.

Von einer Beanstandung wegen V erletzung des Sozialgeheimnisses bzw. unzureichender Sicherung von Personalunterlagen habe ich in diesem Fall abgesehen. Zwar hätte die Bezirksverwaltung ihrer Verpflichtung, diese Daten nur Befugten zugänglich zu machen oder nur an diese weiterzugeben, in höherem Maße nachkommen müssen, zumal es sich auch um äußerst sensible Krankheitsdaten handelte. Die Entwendung der Unterlagen wurde durch die ungesicherte Aufbewahrung sehr erleichtert. Dennoch konnte die Berufsgenossenschaft mit dem Einsatz von beträchtlicher krimineller Energie nicht rechnen. Gegen eine solche Verhaltensweise – insbesondere, wenn hieran möglicherweise auch eigene Mitarbeiter beteiligt sind – ist ein vollkommener Schutz kaum zu gewährleisten. Dieser Fall verdeutlicht, dass die datenschutzrechtliche Forderung nach ausreichenden technischen und or ganisatorischen Sicherungsmaßnahmen zum Schutz von Daten für die Mitarbeiter , die diese Maßnahmen durchzuführen haben, nicht nur eine lästige Verpflichtung ist, sondern auch zu ihrem eigenen Schutz besteht. Deshalb hat die Berufsgenossenschaft sofort nach Bekanntwerden des Verlustes von Unterlagen durch entsprechende Anweisungen sicher gestellt, dass in Abwesenheit eines Mitarbeiters dessen Zi mmer stets verschlossen gehalten wird und die Akten auch innerhalb des Zimmers verschlossen aufbewahrt werden. Die Mitarbeiter der betrof fenen Bezirksverwaltung der Berufsgenossenschaft haben durch die Erfahrung mit dem vor liegenden Einzelfall eine hohe Akzeptanz hinsichtlich der neu eingeführten Maßnahmen zum Schutz von Akten und Unterlagen gezeigt.

27 Rehabilitations- und Schwerbehindertenrecht

27.1 Bundesarbeitsgemeinschaft für Rehabilitation: Gemeinsame Empfehlungen zum Wohl des Versicherten

Das Rehabilitations- und Schwerbehindertenrecht ist mit dem zum 19. Juni 2002 in Kraft getretenen SGB IX (BGBl. I 2001 S. 1046) neu geregelt worden. Dieses Gesetz gibt indes nur einen Rahmen vor , um die Ziele des Gesetzgebers zu erreichen, nämlich die Zusammenarbeit der beteiligten Rehabilitationsträger zu sichern und Beratungen für behinderte Menschen, Präventions ansätze oder erforderliche Leistungen im Einzelfall zu verbessern und aufeinander abzustimmen. Die konkreten Maßnahmen und auch die Datenerhebungs- und Datenverarbeitungsschritte werden in den gemeinsamen Empfehlungen nach § 13 SGB IX von den beteiligten Rehabilitationsträgern vereinbart. Diese Aufgabe, die gemeinsamen Empfehlungen zu einer V ielzahl von Regelungssachverhalten, wie beispielsweise zur Früherkennung und Frühförderung behinderter Kinder oder zur Zusammenarbeit der Hausärzte mit Betriebsärzten, auszuarbeiten und den T rägern vorzuschlagen, wird von der Bundesarbeitsgemeinschaft für Rehabilitation wahr genommen, die bereits seit vielen Jahren die gemeinsame Repräsentanz der Verbände der beteiligten Rehabilitationsträger und einer

Vielzahl anderer Stellen im Rehabilitationsbereich ist. Im Rahmen meiner Beteiligung an der Erarbeitung der gemeinsamen Empfehlungen habe ich mich immer – unter Berücksichtigung der jeweiligen sachlichen Regelung – für die Beachtung folgender datenschutzrechtlichen Grundsätze eingesetzt, um das informationelle Selbstbestimmungsrecht der behinderten Menschen in größtmöglichem Umfange zu gewährleisten:

– Erforderlichkeitsgrundsatz

  Ein wesentlicher Grundsatz des allgemeinen Datenschutzrechtes ist die Erforderlichkeit. Danach ist eine Offenbarung von personenbezogenen Angaben nur zulässig, wenn ohne die Erhebung, Verarbeitung oder Nutzung der Daten eine Aufgabe nicht oder nicht sach- bzw. zeitgerecht erfüllt werden kann. Mit dieser datenschutzrechtlichen Forderung soll vermieden werden, dass einzelne speichernde Stellen eine Vielzahl von Informationen über einen Betroffenen ansammeln, die zumindest zurzeit nicht benötigt werden.

– Zweckbindung

  Personenbezogene Daten dürfen nur zu dem Zweck verarbeitet oder genutzt werden, zu dem sie erhoben bzw. gespeichert wurden und dieser Verwendungszweck muss für den Betroffenen klar erkennbar festgelegt sein. Von diesem Grundsatz sind Ausnahmen vorgesehen, wenn sie gesetzlich vorgeschrieben sind, wie beispielsweise die Überprüfung der Angaben eines Betroffenen, soweit dies zur Erfüllung einer Aufgabe des Sozialleistungsträgers erforderlich ist. Im Hinblich auf die im SGB IX festgelegte Zusammenarbeit verschiedener Leistungsträger und anderer beteiligter Stellen ist zu beachten, dass dem Aspekt der Vertrauensbildung eine entscheidende Rolle zukommt. Ein behinderter Mensch wird einer Erhebung oder Übermittlung seiner Daten eher und beruhigter zustimmen, wenn er genau weiß, zu welchem Zweck die Datenerhebung oder die Datenübermittlung erfolgt und er sich darauf verlassen kann, dass er nicht zu einem späteren Zeitpunkt in einem völlig anderen Zusammenhang mit diesen Daten konfrontiert wird.

– Gesetzlich normierte Regelung

  Das Datenschutzrecht geht von der Grundkonzeption des Verbots mit Erlaubnisvorbehalt aus. Zur Wahrung des Persönlichkeitsrechts in der Form des informationellen Selbstbestimmungsrechts des Betroffenen ist für jede Erhebung oder Verarbeitung personenbezogener Daten eine gesetzliche Grundlage erforderlich, die nach dem bekannten „Volkszählungsurteil“ normenklar sein muss. Das bedeutet, ein Gesetz, das Eingriffe in das informationelle Selbstbestimmungsrecht des Betroffenen vorsieht und damit auch eine Abwägung des Gesetzgebers zwischen diesem Recht und anderen schützenswerten Positionen wiedergibt, muss klar und für den Betroffenen transparent aufzeigen, welche Datenverarbeitungsschritte unter Berücksichtigung der datenschutzrechtlichen Grundvorgaben zulässig sind. Da das SGB IX für eine Informationsverarbeitung lediglich einen Rahmen vorgibt, die inhaltliche Ausfüllung dieser Vorgaben aber den beteiligten Rehabilitationsträgern überlässt, müssen die dazu dienenden gemeinsamen Empfehlungen den Umfang des informationellen Selbstbestimmungsrechts und dessen Einschränkungen klar ergeben.

– Einwilligung

  Das Datenschutzrecht kennt neben der gesetzlich normierten Erlaubnis für die Erhebung, Verarbeitung oder Nutzung von Daten auch die Einwilligung des Betroffenen als Erlaubnistatbestand. Im Sozialleistungsbereich kann dies aber nur beschränkt gelten. Die Erbringung von Leistungen kann nicht davon abhängig sein, dass der Versicherte – im Rahmen des SGB IX der behinderte Mensch – zugleich auch ohne Beschränkungsmöglichkeit in die Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einwilligt. Dies könnte zu unbilligen Ergebnissen führen. Würde ein behinderter Mensch aufgrund datenschutzrechtlicher Bedenken seine Einwilligung zu einer Rehabilitationsmaßnahme zur Erhaltung des Arbeitsplatzes oder zur Teilhabe am Leben nicht geben, würde er eine Sozialleistung, auf die er einen Anspruch hat, überhaupt nicht erhalten. Vor diesem Hintergrund erscheint es sinnvoll, für bestimmte Rehabilitationsmaßnahmen im Rahmen gesetzlicher Vorgaben stärkere Mitwirkungs- und Gestaltungsrechte für die behinderten Menschen vorzusehen.

Für die Beachtung dieser Grundsätze werde ich mich auch künftig bei der Formulierung weiterer gemeinsamer Empfehlungen einsetzen.

27.2 Aufnahme der Arbeit der Servicestellen: Koordinierung der Sozialleistungsträger

Die mit der Einordnung des SGB IX (BGBl. I 2001 S. 1046) in das Sozialgesetzbuch erstmals eingerichteten Servicestellen für behinderte Menschen haben nicht nur die Aufgabe, diese zu beraten und zu unterstützen, sondern sollen nach dem Wortlaut des Gesetzes auch die Tätigkeit der Sozialleistungsträger koordinieren und deren Entscheidungen vorbereiten. Vor diesem Hintergrund habe ich ein besonderes Augenmerk auf die Datenerhebungen und Datenübermittlungen bei der Tätigkeit der Servicestellen gelegt. In einem ersten sondierenden Gespräch mit der Bundesarbeitsgemeinschaft für Rehabilitation im Oktober 2001 habe ich mich über die Organisation und Aufgabenstellung der Servicestellen informiert. Im Juni 2002 habe ich, nachdem die ersten Servicestellen ihre Arbeit zum 1. Januar 2002 aufgenommen hatten, drei Servicestellen in Berlin besucht. Weder die geplante Organisation und Aufgabenstellung noch die in der Praxis umgesetzte Arbeitsweise begegnen schwerwiegenden datenschutzrechtlichen Bedenken. Die Servicestellen sollen nur auf Wunsch des behinderten Menschen tätig werden. Auch für die weiteren Bearbeitungsschritte ist stets ein Mandat des Betroffenen erforderlich. Nach der Planung sollen die Servicestellen auch Anträge, die das Verfahren eines anderen Leistungsträger betreffen, bearbeiten. In diesen Fällen wären Abschottungsfragen datenschutzrechtlich zu prüfen. In dem von mir beobachteten tatsächlichen Ablauf kommt dieser Fall jedoch nicht vor. Im Juni 2002 waren die Servicestellen nur von sehr wenigen behinderten Menschen in Anspruch genommen worden. Die Größenordnung lag bei ca. fünf bis 15 Personen. Die Arbeit der Servicestellen beschränkte sich in der Anlaufphase im Wesentlichen auf die Weiterleitung der gestellten Leistungsanträge an die zuständigen Leistungsträger. Dabei handelte es sich ausschließlich um das Ausfüllen von Formularen; eine elektronische Datenverarbeitung wurde nicht benutzt.

Wegen der großen Bedeutung, die mit der Erhebung und Übermittlung von sensiblen Daten behinderter Menschen von und an verschiedene Stellen verbunden ist, werde ich die weitere Entwicklung der Organisation und der Aufgabenstellung in den Servicestellen weiterhin im Auge behalten.

28 Gesundheit

28.1 Telematik im Gesundheitswesen

Die Entwicklung im Gesundheitswesen ist im Berichtszeitraum durch demographische Veränderungen, Fortschritte in medizinischer Forschung und Technik und nicht zuletzt durch eine zunehmende europäische Integration und Globalisierung geprägt worden. In meinem letzten Tätigkeitsbericht habe ich über die langsam anlaufenden Aktivitäten auf dem Gebiet der Gesundheitstelematik, worunter Anwendungen von **Tele**kommunikation und Infor**matik** im Gesundheitswesen zu verstehen sind, berichtet (Nr. 25.1). Es ist also nicht weiter überraschend, dass dieses Thema inzwischen ein zentrales gesellschaftspolitisches Anliegen geworden ist, das auch im politischen Bereich große Aufmerksamkeit findet. Das Aktionsforum für Telematik im Gesundheitswesen, in dem Vertreter aller Selbstverwaltungspartner zusammenarbeiten, hat inzwischen so genannte Managementpapiere zu den Themen elektronisches Rezept, elektronischer Arztbrief, Sicherheitsinfrastruktur und internationale Perspektiven von Telematik beschlossen. Diese Papiere enthalten eine Bestandsaufnahme der Ist-Situation, beschreiben den Handlungsbedarf und zeigen auch Lösungsansätze auf. Eine Umsetzung dieser Vorschläge ist jedoch noch nicht erfolgt.

Der Einsatz moderner Informationstechnologie soll die Qualität der medizinischen Versorgung optimieren, patientenorientierte Angebote verbessern und Wirtschaftspotenziale im Gesundheitswesen erschließen. Vorgesehen ist somit eine Leistungsverbesserung bei gleichzeitiger Effizienzsteigerung und Kostenreduzierung, und alles soll insgesamt zum Wohle und Nutzen der Patienten sein. Vor dem Hintergrund des allgemeinen Misstrauens gegenüber dem Einsatz neuer Techniken wird über Erfolg oder Misserfolg des Einsatzes von Informationstechnik im Gesundheitswesen die Akzeptanz bei den Menschen entscheiden. Die Patienten müssen sich mit ihren Daten im Netz eines modernen Gesundheitswesens geborgen fühlen, sie dürfen nicht den Eindruck haben als seien sie Objekte, die in diesem Netz gefangen sind. Aus Sicht des Datenschutzes ist ein entscheidender Punkt, dass die Patienten nicht schlechter gestellt werden dürfen als sie vorher standen. Wenn alles nur dem Wohle der Patienten dienen soll, dann darf sich auch deren datenschutzrechtliche Position nicht verschlechtern. Der Patient ist bislang Herr seiner Daten und das muss auch so bleiben. Das bedeutet, dass die Patienten – im Rahmen der gesetzlichen Vorschriften – über eine Teilnahme an und einen Ausstieg aus einem Projekt selbst entscheiden können müssen. Wenn die Akzeptanz für die neuen Techniken vorhanden ist, weil die Patienten die sich für sie ergebenden Vorteile erkennen, werden sie sich auch freiwillig beteiligen.

In einer „Gemeinsamen Erklärung des Bundesministeriums für Gesundheit und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen“ vom 3. Mai 2002 (s. Anlage 29) haben sich alle Partner für einen verstärkten Einsatz von Telematikanwendungen ausgesprochen. Die Erklärung enthält auch die Aussage, dass Modellversuche nur unter strenger Beachtung des Datenschutzes und des Selbstbestimmungsrechts der Patienten durchgeführt werden dürfen. Es besteht ferner Einigkeit, dass die mit dem Ausbau zur Gesundheitskarte verbundene Speicherung und Verarbeitung von Gesundheitsdaten als freiwilliges Angebot an die Versicherten zu gestalten ist. Schließlich finden sich in dieser Erklärung meine zentralen datenschutzrechtlichen Forderungen, an denen sich alle vorgesehenen Vorhaben messen lassen müssen. Sie lassen sich wie folgt zusammenfassen:

- Die Datenhoheit der Patienten und der Grundsatz der Freiwilligkeit der Speicherung von Gesundheitsdaten müssen bewahrt werden.
- Die Patienten müssen darüber entscheiden können, welche ihrer Gesundheitsdaten aufgenommen und welche gelöscht werden.
- Die Patienten müssen darüber entscheiden können, ob und welche Daten sie einem Leistungserbringer zugänglich machen.
- Es dürfen keine zentral gespeicherten Datensammlungen über Patienten entstehen.
- Die Patienten müssen das Recht haben, die über sie gespeicherten Daten zu lesen.
- Die Verwendung der gespeicherten Patientendaten muss sich innerhalb des gesetzlichen Rahmens unter Wahrung des bestehenden Schutzniveaus (z. B. Beschlagnahmeschutz in der Arztpraxis) bewegen.

Diese datenschutzrechtlichen Parameter gilt es bei der Einführung telematischer Anwendungen zu erfüllen, gleichgültig ob es sich um das elektronische Rezept, die Gesundheitskarte oder die elektronische Patientenakte handelt.

28.2 Elektronisches Rezept – Wie kommt das Rezept zur Apotheke?

Das elektronische Rezept soll nach übereinstimmender Auffassung aller in diesem Bereich tätigen Akteure den Einstieg in die Gesundheitstelematik bilden. Die Gründe für diese dem elektronischen Rezept zugedachte Schuhlöffelfunktion liegen in erster Linie in dem enormen finanziellen Einsparungspotenzial, das bei jährlich durchschnittlich 600 Millionen Rezepten mit 900 Millionen Verordnungen im Wert von über 20 Milliarden Euro erwartet wird. Darüber hinaus dürfte dieses Projekt – im Vergleich zu anderen telematischen Vorhaben – bei den Patienten leichter zu vermitteln sein und damit auf die erforderliche Akzeptanz stoßen. Ungeachtet dieser positiven Vorzeichen ist aber im Berichtszeitraum der entscheidende Durchbruch noch nicht gelungen.

Bereits in meinem letzten Tätigkeitsbericht habe ich die mögliche technische Ausgestaltung eines elektronischen Rezepts ausführlich beschrieben (s. Nr. 25.1.3). Unverändert sind zwei Grundmodelle im Gespräch, die sich wie folgt kurz zusammenfassen lassen:

1. Das Rezept wird auf einer Chipkarte gespeichert, auf der neben der aktuellen Verschreibung auch weitere Rezepte gespeichert werden können. Die Chipkarte bleibt im Besitz des Patienten, sodass nur mit dessen Einwilligung der Apotheker oder der Arzt auf den Inhalt zugreifen können.
2. Der Arzt übermittelt das Rezept elektronisch an einen speziellen Server, auf den – neben den Ärzten – auch

Apotheker zugreifen können. Der Patient bekommt als Beleg seiner Verschreibung weiterhin ein Papierformular ausgehändigt, auf dem ein Barcode aufgebracht wird, der eindeutig auf das elektronische Rezept verweist. Der Zugriff auf das Rezept erfolgt in der Apotheke nunmehr über eine Netzwerkverbindung zu diesem Server mithilfe des eindeutigen Barcodes. Ein typisches Beispiel für diese Konzeption stellt das „Kölner Modell" dar.

Aus datenschutzrechtlicher Sicht sind beide Modelle akzeptabel, wenn die erforderlichen technisch-organisatorischen Maßnahmen ergriffen werden, um die medizinischen Daten sicher zu verarbeiten. Bei dieser Verarbeitung müssen insbesondere die Vertraulichkeit, Authentizität, Integrität und Verfügbarkeit der Daten des elektronischen Rezepts sichergestellt sein. Hierzu sind einerseits elektronische Signaturen und andererseits die kryptographische Speicherung der Daten notwendig. Von einer Verschlüsselung könnte nur abgesehen werden, wenn es gelänge, eine anonymisierte Verarbeitung der Daten einzuführen. Grundvoraussetzung ist ferner auf jeden Fall die Einführung einer so genannten „Health Professional Card", die eine eindeutige Identifizierung eines Arztes bzw. eines Apothekers sowie deren jeweilige Zugriffsberechtigungen gewährleistet.

Die Einführung des elektronischen Rezepts betrifft die Erhebung und Verarbeitung von Gesundheitsdaten, die nach § 3 Abs. 9 BDSG personenbezogene Daten besonderer Art und deshalb besonders schutzwürdig sind. Jede Erhebung oder Verarbeitung dieser Daten bedarf entweder der Einwilligung des Betroffenen oder einer gesetzlichen Legitimation. Diese Voraussetzung gilt natürlich auch für die herkömmliche Verarbeitung dieser Daten auf Papierrezept. Die Offenlegung der personenbezogenen Daten gegenüber dem Apotheker erfolgt derzeit auf der Grundlage der freiwilligen Entscheidung des Patienten, in einer von ihm ausgewählten Apotheke die ärztliche Verordnung bedienen zu lassen. An dieser freiwilligen Entscheidung des Patienten sollte sich auch durch die Einführung des elektronischen Rezepts nichts ändern. Ich werde die in absehbarer Zeit zu erwartenden Modellversuche aufmerksam begleiten.

28.3 Elektronische Gesundheitskarte für alle Bürger?

Das Bundesministerium für Gesundheit (BMG) hat Ende 2001 infolge des Lipobay-Skandals, bei dem zahlreiche Patienten wegen bis dahin unbekannter Nebenwirkungen dieses Medikaments starben, eine Projektgruppe „Gesundheitspass" eingerichtet mit dem Auftrag, Eckpunkte für einen elektronischen Gesundheitspass zu erarbeiten. Ziele des Passes waren insbesondere:

- die Verbesserung der Qualität der medizinischen Behandlung, besonders der Arzneimittelsicherheit;
- Stärkung der Eigenverantwortung und -initiative der Patienten;
- Optimierung von Arbeitsprozessen und
- Beitrag zur Wirtschaftlichkeit und Leistungstransparenz.

Das Konzept des Gesundheitspasses sah im Wesentlichen vor, dass wichtige Gesundheits- und Notfalldaten von Patienten, verordnete Arzneimittel und Selbstmedikation, Hinweise auf bereits erfolgte Untersuchungen, die technischen Voraussetzungen zur papierlosen Übermittlung von Rezepten und Arztbriefen sowie die Daten der bisherigen Krankenversichertenkarte in eine multifunktionale Mikroprozessorkarte integriert werden. Gleichzeitig sollte dieser Pass auch eine Schlüssel- und Pointerfunktion erhalten, um Daten auf Servern speichern und einlesen zu können. Die Nutzung des Gesundheitspasses durch die Versicherten sollte auf freiwilliger Basis erfolgen.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich in ihrer 62. Konferenz mit den datenschutzrechtlichen Anforderungen an eine Medikamentenchipkarte befasst (s. Entschließung, Anlage 21). Dabei wurde als grundlegende Voraussetzung der Grundsatz der Freiwilligkeit hervorgehoben, um die freie und unbeeinflusste Entscheidung der Patienten über Einsatz und Verwendung der Karte zu gewährleisten.

In der „Gemeinsamen Erklärung des BMG und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen" vom 3. Mai 2002 (s. Nr. 28.1) hat das BMG erklärt, die jetzige Krankenversichertenkarte künftig auch zusätzlich als Gesundheitskarte anbieten zu wollen. Diese Gesundheitskarte solle auch Werkzeug für den datengeschützten Zugriff auf personenbezogene Gesundheitsdaten sein. Sie solle den europäischen Notfalldatensatz des Patienten, seine persönliche Identifikation/Authentifizierung sowie Verweisfunktionen u. a. auf die Arzneimitteldokumentation und das elektronische Zuzahlungsmanagement des Patienten enthalten. Erfreulicherweise hat das BMG die Gesundheitskarte als freiwilliges Angebot an die Versicherten vorgesehen. Positiv zu betonen ist ferner die volle Übereinstimmung des BMG mit meinen datenschutzrechtlichen Anforderungen, die in dieser Erklärung enthalten sind.

Die Absicht des BMG zur Einführung eines Gesundheitspasses findet auch ihren Niederschlag im Koalitionsvertrag zwischen SPD und BÜNDNIS 90/DIE GRÜNEN vom 16. Oktober 2002. Dort wird bekräftigt, dass zur Erhöhung der Transparenz und der Sicherung von Wirtschaftlichkeit und Effizienz im System auf freiwilliger Basis eine Gesundheitskarte eingeführt werden soll. Diese soll vor unnötigen Doppeluntersuchungen schützen, unerwünschte Arzneimittelnebenwirkungen schneller erkennen lassen und die Datensicherheit stärken. Sie soll die Notfalldaten enthalten und über erforderliche Vorsorgeuntersuchungen informieren. Da die Patienten Anspruch auf vollständige Informationen hätten, soll auch eine Patientenquittung eingeführt werden, mit der die Behandlungen nachvollzogen werden können.

Diese politischen Vorgaben an die Einführung eines Gesundheitspasses erscheinen datenschutzrechtlich ausgewogen. An ihrer Umsetzung werde ich wie in der Vergangenheit konstruktiv mitwirken.

28.4 Elektronische Patientenakte – Schneller, besser, billiger?

Eine wichtige Rolle bei den Überlegungen, die Kostensteigerung im Gesundheitswesen zu reduzieren und gleichzeitig zur Verbesserung der Qualität der medizinischen Versorgung beizutragen, spielt die Einführung einer elektronischen Patientenakte (EPA) oder auch elektronischen Gesundheitsakte. Dabei geht es um mehr als um die bloße Ersetzung einer papiergebundenen ärztlichen Dokumentation durch eine informationstechnologische Speicherung der Patientendaten. Der Begriff „Elektronische Patientenakte" wird vielmehr in

unterschiedlichen Ausprägungen verwendet. Zum einen wird unter einer EPA eine Sammlung medizinischer Informationen zu einem Patienten innerhalb einer Institution auf digitalen Datenträgern verstanden. Dies kann die Krankenakte über einen Patienten in einem Krankenhaus sein, aber auch die ärztliche Dokumentation in einer Praxis. Zum anderen wird der Begriff aber zunehmend auch werbewirksam von kommerziellen Anbietern benutzt. Sie bieten an, medizinische Daten über eine Person über das Internet zur Verarbeitung oder/und zum Abruf durch einen Arzt, ein Krankenhaus etc. bereitzuhalten.

Im Rahmen der Diskussion der Reform im Gesundheitswesen ist unter dem Begriff EPA die jederzeit verfügbare, institutionsübergreifende und unter Kontrolle des Patienten und (eines) Arztes befindliche Kopie aller relevanten Daten der Krankengeschichte zu verstehen. Auf der Basis dieser Definition wurden von verschiedenen Gruppen Konzepte entwickelt, die einerseits die Vorteile der informationstechnischen Verarbeitung medizinischer Daten nutzen und andererseits durch den Einsatz datenschutzfreundlicher Techniken die Datensicherheit für diese Informationen gewährleisten wollen.

Für die Verarbeitung personenbezogener Patientendaten im Rahmen einer EPA gelten grundsätzlich die allgemeinen rechtlichen Rahmenbedingungen, die auch für die Verarbeitung personenbezogener Patientendaten außerhalb telemedizinischer Anwendungen gelten. Die Einführung der elektronischen Verarbeitung von Gesundheitsdaten darf nicht zu einer rechtlichen oder faktischen Verschlechterung der Patientenrechte führen. Dies bedeutet andererseits aber auch, dass der Arzt unverändert entsprechend seiner Berufsordnung verpflichtet bleibt, die erforderlichen Aufzeichnungen über die in Ausübung seines Berufes gemachten Feststellungen und getroffenen Maßnahmen anzufertigen. Die jedem Arzt obliegende Dokumentationspflicht wird durch die Einführung einer EPA nicht tangiert.

Die Durchsetzung bzw. Konkretisierung der Patientenrechte unter den veränderten technischen Bedingungen bedarf teilweise neuer datenschutzrechtlicher Konzepte. Auf jeden Fall müssen zur Verwirklichung der Patientenrechte besondere technische Maßnahmen ergriffen werden. Die technische Grundkonzeption aller EPA-Modelle geht dabei von einer Kombination einer Chipkarte mit Schlüsselfunktion zur Verschlüsselung und Authentisierung und einem gesicherten Zugang entweder zu verschlüsselten oder zu pseudonymisierten Daten aus. Mit diesen Maßnahmen soll sichergestellt werden, dass

- ein Zugang zur EPA technisch nur mit den beiden Chipkarten des Arztes und des Patienten und der Einwilligung des Patienten überhaupt möglich ist,
- das technische System es ermöglicht, die Einwilligung auf einzelne Ärzte oder Krankenhäuser zu beschränken und
- ein Widerruf sowie – auf Wunsch des Patienten – auch die Löschung aller Daten jederzeit möglich ist.

Die bekannten Modelle unterscheiden sich hauptsächlich darin, dass der Speicherplatz der Daten variiert; es ist dies entweder die Chipkarte des Patienten oder ein zentraler oder regionaler Server. Unterschiedlich ist auch der Umfang der medizinischen Daten in der EPA, die z. B. den Arztbrief, das Rezept oder Röntgenaufnahmen enthält. Der Zugang zu den medizinischen Daten steht allerdings immer unter der Prämisse, dass keine Daten des Patienten aus dem System gelangen und damit von Unbefugten gelesen werden können. Dadurch ist gewährleistet, dass der Patient den Zugang zu seinen Daten auch gegenüber Ärzten kontrollieren kann. Eingeschränkt wird dieser Zugang des Patienten in manchen Modellen dadurch, dass für den Zugang auch ein Arzt benötigt wird. Die Speicherung der medizinischen Daten erfolgt in der Regel in pseudonymisierter Form, wobei technisch der Zugang zu den Daten mithilfe von Verschlüsselungsverfahren sichergestellt wird. Die datenschutzrechtliche Grundkonzeption bei der Realisierung einer EPA enthält eine Reihe von Sicherheitszielen, die von Systemen zur medizinischen Datenverarbeitung gewährleistet werden müssen. Dazu zählen insbesondere die Vertraulichkeit, die Authentizität oder auch Zurechenbarkeit der Daten zu einem Verantwortlichen, die Integrität und Verfügbarkeit der Daten. Ferner ist die Revisionsfähigkeit und Validität der Daten zu gewährleisten und Rechtssicherheit für jeden Verarbeitungsvorgang sicherzustellen.

Zur Festlegung dieser Eckpunkte bei der Verarbeitung von medizinischen Daten in elektronischen Patientenakten habe ich mich im Berichtszeitraum an einer Arbeitsgruppe des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und Länder beteiligt, die die Anforderungen in einem Werkpapier zusammengestellt hat. Diese Zusammenstellung „Datenschutz und Telemedizin – Anforderungen an Medizinnetze“ kann unter meiner Webadresse im Internet abgerufen werden.

28.5 Genomanalysen – die neue Herausforderung für den Datenschutz

Durch den technischen Fortschritt, den die Medizin auf dem Gebiet der molekulargenetischen Forschung in den letzten Jahren gemacht hat, stellen sich immer neue Fragen hinsichtlich Bedeutung und Auswirkungen von heute schon technisch möglichen Gentests. Genetische Daten – darunter fallen alle Informationen über das Erbgut eines Menschen – besitzen eine Reihe von Eigenschaften, die dazu führen, dass ihr Schutz vor missbräuchlicher Verwendung besonders schwierig, gleichzeitig aber auch in besonderer Weise erforderlich ist, um Persönlichkeitsrechtsverletzungen – von der Stigmatisierung bis hin zur Kündigung von Arbeitsverhältnissen oder zum Ausschluss von Versicherungsmöglichkeiten – zu verhindern.

Bereits in meinem 18. TB (Nr. 25.2) habe ich dem Gesetzgeber empfohlen, den Bereich der molekulargenetischen Analysen umfassend zu regeln. Dabei sollten sowohl die einschlägigen Bereiche, in denen schon heute Gentests eine Rolle spielen bzw. spielen könnten, wie Medizin und Forschung, als auch die der Arbeitsverhältnisse und Versicherungen umfassend geregelt werden. Vordringlich wäre allerdings die Schaffung eines gegen jedermann gerichteten, ausdrücklichen und strafbewehrten Verbotes, 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. Denn durch die Einführung moderner Testmethoden reichen die vorhandenen rechtlichen Rahmenbedingungen nicht mehr aus, um deren Auswirkungen wirksam lenken zu können.

Das zuständige BMJ hielt es allerdings für problematisch, eine solche Norm losgelöst von der Entscheidung über den

Umfang und über die Verwendungsweise von Gentests in den einschlägigen Bereichen zu entwickeln. Deshalb sollte der Bericht einer vom Deutschen Bundestag eingesetzten Kommission „Recht und Ethik der modernen Medizin" abgewartet werden, der sich intensiv mit der Frage nach dem Umgang mit molekulargenetischen Analysen und den daraus resultierenden Problemfeldern beschäftigt.

Dieser Schlussbericht liegt inzwischen vor. Die Kommission ist darin nahezu auf alle relevanten Fragestellungen eingegangen und hat sich – gerade im Hinblick auf das Recht auf informationelle Selbstbestimmung – meiner Position, die sich in einer entsprechenden Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder aus dem Oktober 2001 wiederfindet (s. Anlage 19), angeschlossen.

Die Diskussion über den Bereich der Gentests sollte aber nicht mehr nur auf nationaler Ebene, sondern aufgrund der länderübergreifenden Auswirkungen der technischen Neuerungen auch auf europäischer Ebene behandelt werden. Daher habe ich wegen der grundsätzlichen Bedeutung der Thematik die Diskussion in der Brüsseler Datenschutzgruppe nach Artikel 29 der EG-Richtlinie bereits angestoßen.

28.6 Fragen zum Umgang mit Patientendaten

Im Berichtszeitraum haben mich verstärkt Eingaben erreicht, die zum einen ganz praktische Probleme im Umgang mit Patientendaten – nämlich die Aufbewahrung von Krankenunterlagen – und zum anderen auch den fortschreitenden Einsatz von Informationstechnik in der täglichen Praxis der Arztpraxen, z. B. in der Arztkommunikation, betreffen.

So ist vielen Patienten unklar, wie und vor allem wie lange Krankenunterlagen über sie aufgehoben werden müssen und wie es sich mit ihren Einsichtsrechten in diese Unterlagen verhält. Auf diese Fragen geben die jeweiligen Berufsordnungen der Ärzte Auskunft, die im Grundsatz auf der Musterberufsordnung für Ärztinnen und Ärzte (MBO-Ä von 1997, letztmalig geändert durch die Beschlüsse des 105. Deutschen Ärztetages 2002) beruhen. Rechtswirkung entfalten diese Regelungen allerdings erst, wenn sie von den einzelnen Kammerversammlungen der Ärztekammern als Satzung beschlossen und von den zuständigen Aufsichtsbehörden genehmigt werden. Nach § 10 Abs. 1 MBO-Ä hat der Arzt die in Ausübung seines Berufes gemachten Feststellungen und getroffenen Maßnahmen zu dokumentieren. Diese Aufzeichnungen dienen nicht nur dem Arzt als Gedächtnisstütze, sie dienen auch dem Patienten als Dokumentationen der ärztlichen Behandlung. Diese Dokumentationen sind gem. § 10 Abs. 3 MBO-Ä mindestens zehn Jahre nach Abschluss der Behandlung aufzubewahren, es sei denn, andere gesetzliche Vorschriften regeln eine längere Aufbewahrungsfrist. Werden diese Dokumentationen auf elektronischen Datenträgern oder anderen Speichermedien aufgezeichnet, so hat der Arzt nach § 10 Abs. 5 MBO-Ä besondere Sicherungs- und Schutzmaßnahmen zu treffen, um deren Veränderung, Vernichtung oder unrechtmäßige Verwendung zu verhindern. Nach § 10 Abs. 2 MBO-Ä hat der Arzt dem Patienten auf dessen Verlangen grundsätzlich Einsicht in die ihn betreffenden Krankenunterlagen zu gewähren. Die MBO-Ä nimmt allerdings subjektive Eindrücke oder Wahrnehmungen des Arztes – im Gegensatz zu verschiedenen tatsächlich von den Ärztekammern umgesetzten Berufsordnungen – von der Einsichtnahme aus. Der Patient muss daher im Zweifelsfall die für ihn gültige Berufsordnung zu Rate ziehen.

Bei den Ärzten unter den Petenten ist die Unsicherheit über die datenschutzgerechte Nutzung neuer Informationstechnologien in der Kommunikation spürbar, denn im privaten Bereich nimmt der Informationsaustausch zwischen den Bürgern per E-Mail rasant zu, vielen Ärzten ist aber unklar, ob und unter welchen Voraussetzungen z. B. Arztbriefe oder andere patientenbezogene medizinische Informationen über das Internet versandt werden dürfen bzw. wie diese hierbei zu schützen sind.

Zu den Fragen nach den datenschutzrechtlichen Anforderungen an den Einsatz moderner Informationstechnologie bei der Kommunikation kann ich nur grundsätzlich auf das Erfordernis besonderer Sicherheitsmaßnahmen bei der Verarbeitung medizinischer Daten verweisen. Die Gefahr des Datenmissbrauchs in elektronischen Netzen ist mittlerweile allgemein bekannt. Deshalb ist zumindest der Einsatz einer Verschlüsselung und der digitalen Signatur der Daten zwingend erforderlich. Durch geeignete Sicherungsmaßnahmen kann das Risiko eines unbefugten Zugriffs auf diese Daten allerdings nur verringert werden, gänzlich auszuschließen ist ein Missbrauch in offenen Netzen, wie z. B. dem Internet, jedoch nicht.

28.7 Einzelfragen aus dem Düsseldorfer Kreis

28.7.1 Chip mit Altersangabe für Zigarettenkauf an Automaten

Zigarettenautomaten sollen künftig für Jugendliche unter 16 Jahren gesperrt werden. Das am 23. Juli 2002 verkündete neue Jugendschutzgesetz (BGBl. I S. 2730 ff.) sieht in § 10 Abs. 2 vor, dass aus Gründen des Jugendschutzes Tabakwaren in der Öffentlichkeit nicht mehr in Automaten angeboten werden dürfen. Dieses Verbot soll jedoch dann nicht gelten, wenn durch „technische Vorrichtungen" in Automaten sichergestellt ist, dass Kinder und Jugendliche unter 16 Jahren Tabakwaren nicht entnehmen können. Um den betroffenen Unternehmen die Möglichkeit zu geben, die technischen Voraussetzungen zu schaffen, tritt diese Vorschrift nach einer Übergangsfrist von viereinhalb Jahren am 1. Januar 2007 in Kraft.

Vor diesem Hintergrund hat der Bundesverband Deutscher Tabakwaren-Großhändler und Automatenaufsteller e.V. ein Beratungsunternehmen beauftragt, eine Lösung zu erarbeiten. Man favorisierte die Aufbringung eines Altersmerkmals auf der kontogebundenen Geldkarte, die nach einer Altersauthentifizierung auf der Geldkarte den Kauf von Zigaretten mit Bargeld oder bargeldlos durch Abrechnung über das Konto ermöglichen sollte. Der Zentrale Kreditausschuss entwickelte ein technisches Konzept zur Aufbringung der notwendigen Merkmale auf der Geldkarte. Sowohl die originär zuständige Datenschutzaufsichtsbehörde, die Landesdatenschutzbeauftragte Nordrhein-Westfalen, als auch der Düsseldorfer Kreis sind frühzeitig in die Beratungen über das geplante Verfahren einbezogen worden. Die Datenschutzaufsichtsbehörden sahen einen erheblichen Gesprächsbedarf zu diesem Thema, nicht zuletzt wegen der neuen Regelung über mobile personenbezogene Speicher- und Verarbeitungsmedien in § 6c BDSG mit seinen Verpflichtungen zur Unterrichtung, zur Bereithaltung der für die Wahrnehmung des Auskunftsrechts erforderlichen

Geräte und Einrichtungen und der Verpflichtung, den Betroffenen eindeutig Kommunikationsvorgänge erkennbar zu machen, die auf dem Medium eine Datenverarbeitung auslösen. Von besonderer datenschutzrechtlicher Bedeutung war das vorgesehene Altersmerkmal auf der Chipkarte, das als personenbezogenes Datum der Einwilligung der Betroffenen bedarf, und die Frage der Verantwortlichkeit für diese Zusatzfunktion auf der Geldkarte.

Nach intensiven Beratungen der Beteiligten mit den Datenschutzaufsichtsbehörden und mehrmaliger Überarbeitung des technischen Konzeptes hat man sich nunmehr auf ein Verfahren geeinigt, gegen das keine datenschutzrechtlichen Bedenken mehr bestehen. Nach diesem Verfahren wird die kontogebundene Geldkarte mit einem „Legitimationsvermerk“ versehen, der zum Zigarettenkauf an Automaten berechtigt. Diesen Vermerk erhalten die Karteninhaber auf ihre Chipkarte, die das 18. Lebensjahr vollendet haben. Dieser Vermerk ist ohne jegliches Datum, sodass eine Personenbeziehbarkeit nicht vorhanden ist und es einer Einwilligung des Karteninhabers zur Aufbringung auf die Chipkarte nicht bedarf. Lediglich bei minderjährigen Karteninhabern erhält der Vermerk das verschlüsselte Datum, an dem der Karteninhaber volljährig wird. Von diesem Datum aus kann das Lesegerät zurückrechnen und überprüfen, ob der Inhaber der Karte bereits 16 Jahre alt ist und dementsprechend den Zugang zu dem Automaten eröffnen oder verweigern. Die Einholung der datenschutzrechtlich erforderlichen Einwilligung zu der Aufbringung des Datums auf der Geldkarte bei minderjährigen Kunden erfolgt mit dem Antragsformular bei der Kontoeröffnung.

Insgesamt ist dies ein Beispiel für gute Zusammenarbeit zwischen Unternehmen und Datenschutzbehörden im Vorfeld technischer Investitionen.

28.7.2 Anforderungen von OP-Protokollen durch private Krankenversicherer

Im Berichtszeitraum beschwerten sich Patienten bzw. Ärzte über die pauschale Anforderung von OP-Protokollen durch private Krankenversicherer. Eine solche Anforderung eines OP-Protokolls darf nur erfolgen, wenn eine entsprechende Datenerhebung auch erforderlich ist. Sie muss sich aus den Gründen des Einzelfalles, z. B. bei konkreten Zweifeln an der Abrechnung, ergeben. Die zuständige Datenschutzaufsichtsbehörde erhielt von der betroffenen Krankenversicherung die Auskunft, dass Anforderungen von OP-Protokollen nur in seltenen Einzelfällen vorgenommen würden, wenn sie zur Feststellung der Leistungspflicht des Versicherers erforderlich seien. Im Ergebnis war daher festzustellen, dass eine pauschale Anforderung von OP-Protokollen nach übereinstimmender Auffassung von Datenschutzaufsichtsbehörden und der betroffenen Versicherung nicht zulässig ist.

28.7.3 Apotheken-CD

Zur Abwicklung der Kostenerstattung der von den gesetzlich Krankenversicherten eingereichten Rezepte mit den Krankenkassen schalten Apotheken vielfach Apotheken-Rechenzentren ein. Hierfür bietet § 300 Abs. 2 SGB V die Rechtsgrundlage. In der bis zum 15. Februar 2002 gültigen Fassung der Vorschrift hieß es im Wortlaut: „Die Apotheken und weitere Anbieter von Arzneimitteln können zur Erfüllung ihrer Verpflichtungen nach Abs. 1 Rechenzentren in Anspruch nehmen. Die Rechenzentren dürfen die Daten für im Sozialgesetzbuch bestimmte Zwecke verarbeiten und nutzen, soweit sie dazu von einer berechtigten Stelle beauftragt worden sind; anonymisierte Daten dürfen auch für andere Zwecke verarbeitet und genutzt werden.“ Im Rahmen des Gesetzes zur Begrenzung von Arzneimittelausgaben der gesetzlichen Krankenversicherung vom 15. Februar 2002 (BGBl. I S. 684) wurde die Vorschrift wie folgt ergänzt: .... „Die Rechenzentren dürfen die Daten für im Sozialgesetzbuch bestimmte Zwecke und ab dem 1. Januar 2003 nur in einer auf diese Zwecke ausgerichteten Weise verarbeiten und nutzen, soweit ....“. Anlässlich von Prüfungen von Datenschutzaufsichtsbehörden aus dem nicht öffentlichen Bereich wurde festgestellt, dass verschiedentlich Apotheken personenbezogene Rezeptdaten über Abrechnungszwecke hinaus für andere Zwecke durch Apotheken-Rechenzentren aufbereiten ließen und in Form einer CD mit verschiedenen Auswertemöglichkeiten verwandten, ohne dass es hierfür eine Rechtsgrundlage aufgrund Gesetzes oder Einwilligung gab. Dies wurde von den jeweils zuständigen Aufsichtsbehörden beanstandet. In der Folge wurde im Düsseldorfer Kreis die Frage kontrovers diskutiert, inwieweit solche Verfahren über Einwilligungserklärungen der Patienten legitimiert werden könnten. Ich habe hier ebenso wie die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen die Rechtsauffassung vertreten, dass es sich bei der Vorschrift des § 300 Abs. 2 SGB V, dessen Ausrichtung auf Zwecke des Sozialgesetzbuches durch die erwähnte Gesetzesänderung noch verstärkt wurde, um eine vorrangige Rechtsvorschrift handelt, die aus einem allgemeinen Interesse heraus die personenbezogene kommerzielle Verwertung der sensiblen Gesundheitsdaten in Rezepten nicht zulässt. Die hier vorhandene spezialrechtliche Regelung kann daher nicht durch eine Einwilligung außer Kraft gesetzt werden. Das Bundesministerium für Gesundheit, das mit der Rechtsfrage wiederholt befasst wurde, hat sich letztlich meiner Auslegung angeschlossen und die Ausrichtung der Verarbeitung der personenbezogenen Rezeptdaten auf Zwecke des Sozialgesetzbuches bekräftigt.

29 Verkehr

29.1 LKW-Maut – droht eine generelle Verkehrsüberwachung?

Das „Gesetz zur Einführung von streckenbezogenen Gebühren für die Benutzung von Bundesautobahnen mit schweren Nutzfahrzeugen“ (Autobahnmautgesetz), an dessen Gestaltung ich in den letzten Jahren intensiv beteiligt war (vgl. 18. TB Nr. 28.4), ist am 12. April 2002 in Kraft getreten (BGBl. I S. 1234). Am 20. September 2002 wurde ein Firmenkonsortium mit dem Aufbau und Betrieb eines satelliten- und mobilfunkgestützten Mauterfassungssystems beauftragt. Ab August 2003 sollen Schwerlaster ab zwölf Tonnen elektronisch erfasst und die Maut berechnet werden. Je nach Achsenzahl und Schadstoffklasse müssen sie zwischen 10 und 17 Cent pro Kilometer zahlen. Betroffen sind schätzungsweise 1,2 bis 1,5 Millionen Fahrzeuge, davon 500 000 ausländische. Die Mautschuldner sind verpflichtet, bei der Mauterhebung mitzuwirken, z. B. durch Mitführen eines Gerätes in der Größe eines Autoradios (so genanntes On Board Unit – OBU), das über GPS den Standort erfasst und über Mobilfunk mit der Abrechnungsstelle kommuniziert. Auf den Autobahnen werden rund 300 Messbrücken als Kontrolleinrichtungen errichtet. Neben der automati-

schen Abrechnung kann die Maut auch mit herkömmlichen Zahlungsmitteln an ca. 3 500 Zahlstellen entrichtet werden (vgl. Abbildung 5).

Im Autobahnmautgesetz sind die mautpflichtigen Fahrzeuge, die Autobahnstrecken, die Mautschuldner sowie die Berechnungsgrundlagen der Maut sätze festgelegt. Für die Mautentrichtung dürfen zweckgebunden neben dem Kennzeichen des Fahrzeugs nur technische Angaben wie Strecke, Ort, Zeit, Kfz-Merkmale und Mauthöhe verarbeitet werden. Der Betreiber des Mauterhebungssystems hat die gespeicherten Daten unverzüglich nach Abschluss des V erfahrens zu löschen. Die Einhaltung der gesetzlichen Vorschriften obliegt in erster Linie dem Bundesamt für Güterverkehr, daneben auch den Zollbehörden. Zu diesem Zweck dürfen der Name des Mautschuldners, Bi ld, Kennzeichen und technische Merkmale des LKW sowie Ort und Zeit der Bundesautobahnbenutzung gespeichert werden. Für die meisten Daten gilt, dass sie nach der Mautentrichtung zu löschen bzw . für statistische Zwecke zu anonymisieren sind. Bilder und Daten von Fahrzeugen, die nicht der Mautpflicht unterliegen, sind unmittelbar nach dem Kontrollvorgang zu löschen.

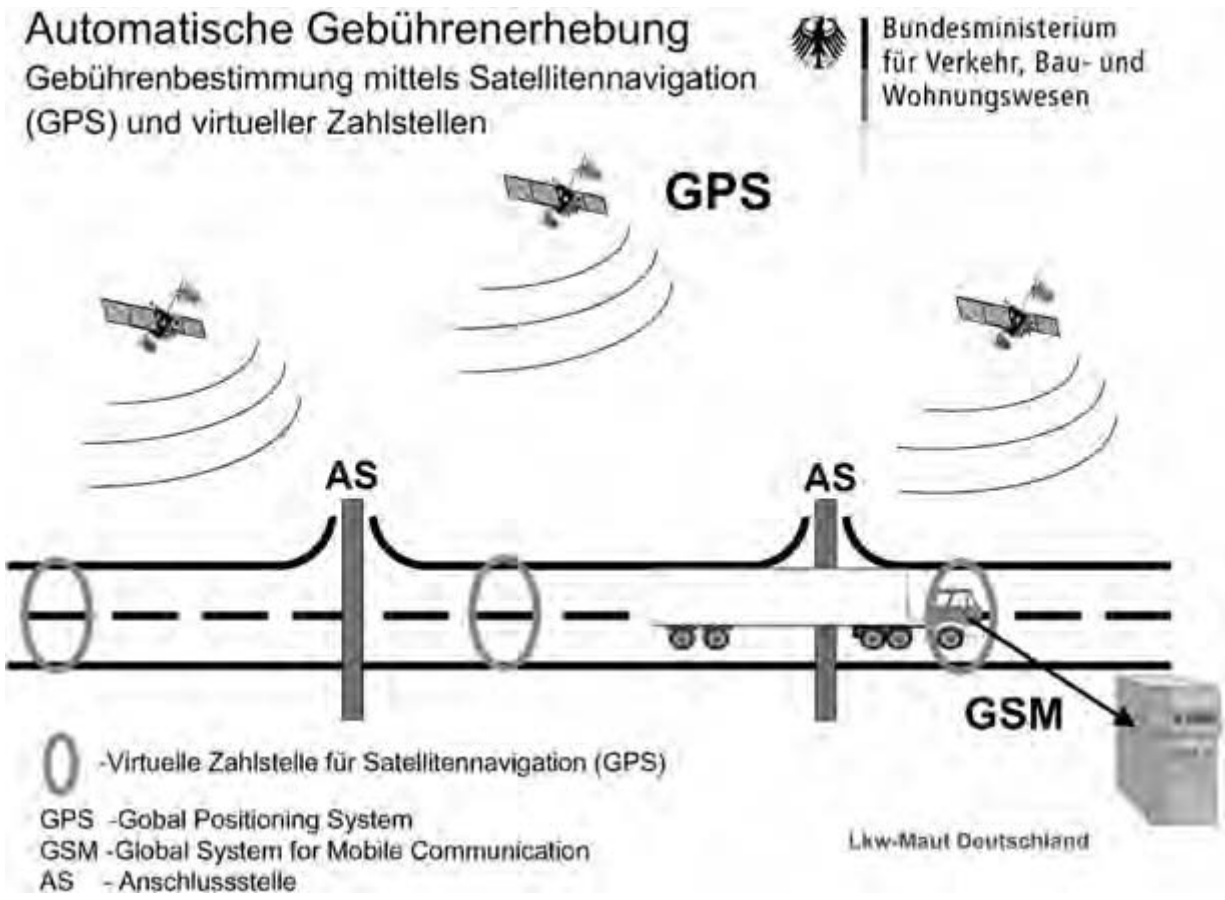
Mit diesem Maßnahmenbündel zum Datenschutz sind generelle Verkehrsüberwachungen oder gar die Erstellung von Bewegungsprofilen von Fahrzeugen ausgeschlossen. Die Regelungen zur Datenverarbeitung werden dem datenschutzrechtlichen Grundsatz der Datensparsamkeit (§ 3a BDSG) gerecht. Jedwede Erweiterung der Mautpflicht oder der Kontrollmaßnahmen unterliegt dem Gesetzesvorbehalt und damit auch der Einflussna hme des Datenschutzes. Ich werde Änderungen auf diesem Gebiet kritisch begleiten und Befürchtungen in Richtung auf einen „big brother“ im Straßenverkehr weiter entgegentreten.

29.2 Ärztliche Schweigepflicht kontra Qualitätssicherung bei medizinisch-psychologischen Gutachten

Bei Zweifeln an der Fahreignung kann die Fahrerlaubnisbehörde vom Betroffenen die Vorlage eines medizinisch-psychologischen Gutachtens verlangen. Die Begutachtungsstellen müssen sich bei der Bundesanstalt für Straßenwesen (BASt) akkreditieren lassen und für die bei ihnen tätigen Ärzte und Psychologen einen besonderen Qualifikationsnachweis erbringen. Für die Erstellung der Gutachten gelten die in Anlage 15 zu § 1 1 Abs. 5 Fahrerlaubnisverordnung (FeV) genannten Grundsätze. Die BASt überprüft aus Gründen der Qualitätssicherung die Stellen vor Ort und fordert

Abbildung 5 (zu Nr. 29.1)

Mauterfassung in Deutschland



stichprobenartig Gutachten an (etwa 500 pro Jahr , das sind 0,5 %), die nach Auswertung zurückgegeben werden.

Mir wurde mit einer Eingabe die Frage gestellt, wie die Einsichtnahme der BASt in die Gutachten mit der ärztlichen Schweigepflicht zu vereinbaren sei. Ich habe mich daraufhin an Ort und Stelle kundig gemacht und festgestellt, dass nahezu alle Gutachten im Original und mit vollen Namensangaben vorliegen. Diese V erfahrensweise habe ich moniert. Zwar steht der BASt das Recht zu Kontrollmaßnahmen nach § 72 Abs. 2 FeV z u, um die bundeseinheitliche Anwendung der o. g. Grundsätze durch die Gutachter zu gewährleisten; dies rechtfertigt jedoch keinen Eingrif f in das gesetzlich geschützte Arzt-Patienten-Verhältnis.

Die BASt bestätigte mir, dass der Personenbezug zum Auftraggeber des Gutachtens für ihre Arbeit ohne Bedeutung ist, da sich die Qualitätssicherungsmaßnahmen ausschließlich auf die Begutachtungsstellen und die bei ihnen tätigen Gutachter bezögen. Die Begutachtungsstellen seien auch schon darauf hingewiesen worden, die Gutachten anonymisiert bzw. pseudonymisiert (d . h. ohne direkt identifizierende Angaben) zuzusenden, allerdings ohne nachhaltigen Erfolg. Die BASt fühle sich durch den Hinweis exkulpiert, weil die Wahrung der Verschwiegenheitspflicht Aufgabe der begutachtenden Ärzte und Psychologen sei.

Ich habe dieser Auf fassung widersprochen und dem Amt eine Mitverantwortung zugewiesen. Es erhält durch den Personenbezug Informationen, die für die Aufgabenerfüllung des Amtes nicht erforderlich sind. Nicht erforderliche Daten dürfen nach den Bestimmungen des BDSG nicht verarbeitet oder sonst genutzt werden (§§ 13 f f. BDSG) und zwar unabhängig von den eingesetzten V erfahren. Auch sind die Vorgaben zur Datenvermeidung zu beachten und von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen (§ 3a BDSG). Um nicht selbst mit Schutz- und Sicherungsmaßnahmen in die Pflicht genommen zu werden, muss di e BASt darauf dringen, dass ihr die Gutachten nur in anonymisierter bzw . pseudonymisierter Form zugesandt werden. Dies ist m. E. gegenüber den Begutachtungsstellen auch durchsetzbar . Der Fortbestand ihrer Akkreditierung kann vom Amt mit der Auflage verknüpft werden, bestehende gesetzliche Schutzauflagen einzuhalten, denn die Wahrung des Arzt-Patienten-Vertrauensverhältnisses obliegt den Gutachtern. Andernfalls könnte das Amt den Begutachtungsstellen die Kosten für die nachträgliche Anonymisierung in Rechnung stellen.

Zur organisatorischen Erleichterung habe ich den Vorschlag gemacht, die den Auftraggeber identifizierenden Angaben nur auf dem Deckblatt des Gutachtens festzuhalten und im Gutachten selbst nur vom Auftraggeber oder einem anderen Synonym zu sprechen. Deckblatt, Gutachten und die übrigen anonymisierten Unterlagen erhalten eine vorgangsbezogene einheitliche Referenz-Nummer. Der BASt wird nur das Gutachten ohne Deckblatt übermittelt. Das Amt hat zugesagt, die Begutachtungsstellen auf ihre datenschutzrechtlichen Verpflichtungen hinzuweisen und bei Nichtbeachtung Konsequenzen zu ziehen. Ich werde mich über die weitere Entwicklung auf dem Laufenden halten.

29.3 Ahndung von Verkehrsverstößen im Ausland – Dürfen Daten übermittelt werden?

Manche Bürger werden nach einer Fahrt ins Ausland mit einem besonderen Souvenir an ihre Reise erinnert, das allerdings wenig Freude macht: Sie bekommen Post von der in London ansässigen Firma Euro Parking Collection (EPC), die sie unmissverständlich auf nicht bezahlte Park-„Knöllchen“, Mautgebühren oder andere V erkehrsverstöße hinweist und eine Zahlungsauf forderung gleich beifügt. Das Anschreiben enthielt bis vor kurzem sogar eine Drohung, dass bei Nichtzahlung innerhalb einer Frist die Kreditwürdigkeit des Halters beeinträchtigt werden könne. Da fragt sich natürlich der Betrof fene, woher eine private englische Firma seine Anschrift hat und dazu kommt, Bußgeld z. B. für einen Parkverstoß in Am sterdam, Oslo oder Kopenhagen zu „verhängen“ und Beträge einzutreiben, die teilweise dem Vielfachen deutscher Verhältnisse entsprechen? Woher nimmt die Firma das Recht, ihn bei Kreditunternehmen anzuschwärzen?

Hinter dem „unfreundlichen Ak t“ verbirgt sich folgender Sachverhalt: Die Firma EPC wird von zahlreichen ausländischen Behörden beauftragt, Buß- und V erwarnungsgelder für nicht bezahlte V erkehrsverstöße einzuziehen. Die örtliche Behörde weist in jedem Einzelfall durch V orlage von Strafzetteln oder Fotos die Rechtmäßigkeit der Bußgeldforderung nach, deren Höhe sich nach den gültigen ausländischen Gebührensätzen richtet, die häufig wesentlich höher als in Deutschland sind. EPC wendet sich als eine Art V erwaltungsgehilfe mit dem Beleihungsnachweis an das Kraftfahrt-Bundesamt (KBA) in Flensbur g, das nach § 37 Straßenverkehrsgesetz (StVG) Auskunft über die gespeicherten Fahrzeug- und Halterdaten über mitteln darf. Die englische Firma wird nach § 37 Abs. 2 StVG darauf hingewiesen, dass die Daten ausschließlich zur V erfolgung von Verkehrsverstößen genutzt werden dürfen. An diese Auflage hat sich EPC bisher auch strikt gehalten, auch wenn in dem Anschreiben an den Halter der Hinweis auf die Beeinträchtigung seiner Kreditwürdigkeit anderes vermuten lässt. W eder das KBA noch ich haben Anhaltspunkte, dass von EPC gegen die Zweckbindung verstoßen wurde.

Auf meine Intervention hin hat EPC unverzüglich auf die beanstandete „Drohgebärde“ in seinen Anschreiben verzichtet. Darüber hinaus best ehen keine datenschutzrechtlichen Bedenken gegen die Vorgehensweise.

29.4 Einrichtung einer Fliegerdatenbank beim Luftfahrt-Bundesamt

In meinem letzten Tätigkeitsbericht (vgl. 18. TB Nr. 28.5.2) habe ich über die geplante Ei nrichtung einer Fliegerdatenbank beim Luftfahrt-Bundesamt (LBA) berichtet. Es war vorgesehen, sämtliche bei den fliegerärztlichen Untersuchungen festgestellten Einzelbe funde zentral zu speichern. Dagegen habe ich erhebliche datenschutzrechtliche Bedenken vorgebracht und darauf gedrungen, nur solche medizinischen Befunddaten dem LBA zu melden, die für die Verwaltungsaufgaben des Amtes, Erlaubnisse und Berechtigungen zu erteilen und zu registrieren, erforderlich sind.

Im Entwurf des § 24b der „Änderung der Luftverkehr -Zulassungs-Ordnung“ wird meinen Bedenken Rechnung getragen: Danach speichert das LBA im Falle festgestellter

– „uneingeschränkter Tauglichkeit“ nur Angaben zur Identifizierung des Betroffenen, die ausgestellte Fluglizenz-Klasse sowie die Referenznummer zum ärztlichen Gutachten, das jedoch beim untersuchenden Fliegerarzt verbleibt;

- „eingeschränkter Tauglichkeit“ zusätzlich zu den vorgenannten Angaben die erteilten Auflagen und Beschränkungen sowie die damit zusammenhängenden Einzelbefunde, die jedoch nicht in die Datenbank gelangen, sondern aktenmäßig getrennt und sicher aufbewahrt werden;
- „Untauglichkeit“ lediglich die identifizierenden Personenangaben sowie die den medizinischen Befund erhebende Stelle mit dem Erhebungsdatum.

Sofern der Betroffene auf eigenen Wunsch den Fliegerärztlichen Untersuchungsausschuss beim LBA als Revisionsinstanz anruft und um Überprüfung der Erstuntersuchung bittet, werden die Befunder gebnisse der Erstuntersuchung angefordert und von einem unabhängigen Ärztegremium ggf. unter Heranziehung weiterer Befunde bewertet. Dieser Vorgang führt zu keiner Datenspeicherung beim LBA. Sobald der Fliegerärztliche Untersuchungsausschuss seine Entscheidung getroffen hat, wird das Ergebnis in die Fliegerdatenbank übernommen – analog den Ergebnissen von Erstuntersuchungen. Die ärztlichen Unterlagen der Erstuntersuchung werden zurückgesandt. Die im Rahmen der Überprüfung angefallenen medizinischen Unterlagen werden getrennt beim Fliegerärztlichen Untersuchungsausschuss als Medizinalakte gemäß den ärztlichen Bestimmungen aufbewahrt.

Mit diesen gestaffelten Regelungen werden die datenschutzrechtlichen Grundsätze der Datensparsamkeit, Erforderlichkeit und Zweckbindung umgesetzt.

30 Verteidigung

30.1 Der behördliche Datenschutzbeauftragte

In meinen letzten Tätigkeitsberichten (17. TB Nr. 26.1 und 18. TB Nr. 26.3) habe ich mich ausführlich der Organisation des Datenschutzes in der Bundeswehr und insbesondere der Rolle gewidmet, die dem behördlichen Datenschutzbeauftragten innerhalb der Bundeswehr zukommen soll. Erfreulicherweise ist dieses Thema nach dem In-Kraft-Treten der BDSG-Novelle sehr konstruktiv zwischen dem BMVg und mir diskutiert worden.

Die Bundeswehr soll danach einen eigenen behördlichen Datenschutzbeauftragten (BfDBw) erhalten, dessen Aufgabenschwerpunkte in der Vorabkontrolle nach § 4d Abs. 5 und 6 BDSG, der datenschutzrechtlichen Schulung (§ 4g Abs. 1 Nr. 2 BDSG) und der nachträglichen Kontrolle (§ 4g Abs. 1 Nr. 1 BDSG) liegen werden. Ihm werden nach § 4f Abs. 5 Satz 1 BDSG Hilfskräfte zur Seite gestellt, die ebenso wie er selbst „Vollzeitdatenschützer“ sein werden. Daneben bleibt die bisherige Datenschutzorganisation der Bundeswehr – bei der der Bereich Datenschutz dem Führungsgrundgebiet 1 (Personalwesen, Innere Führung, Presse- und Öffentlichkeitsarbeit) zugeordnet war – unter der Bezeichnung „administrative Datenschutzkomponente“ erhalten. Dem hier eingesetzten Personal (i. d. R. der so genannte S1-Offizier) obliegt eine beratende und in der jeweiligen Dienststelle bzw. in dem jeweiligen Verantwortungsbereich eine schulende Aufgabe. Der dem Datenschutz zuzuordnende Anteil bei den Dienstposten ist von der Größe der Dienststelle und des Verantwortungsbereichs abhängig.

Einerseits wird durch die gefundene Lösung meine Kritik an der Anbindung des Bereichs Datenschutz an das Führungsgrundgebiet 1 wegen möglicher Interessenkonflikte aufgegriffen: Mit der Schaffung des BfDBw wird eine andere, neutralere Stelle mit den datenschutzrechtlichen Kontrollaufgaben beauftragt. Andererseits wird dadurch, dass die bisherige Datenschutzorganisation als Ansprechpartner für den Datenschutz erhalten bleibt, sichergestellt, dass der Weg für den Soldaten bzw. zivilen Mitarbeiter zum förmlich bestellten Datenschutzbeauftragten nicht zu weit ist. Für das BMVg und seinen Geschäftsbereich wurde damit eine gute Lösung gefunden.

30.2 PERFIS – Das Personalinformationssystem der Bundeswehr auf neuen Wegen

In meinem letzten Tätigkeitsbericht habe ich über die datenschutzrechtliche Kontrolle des Personalamts der Bundeswehr und darüber berichtet, dass das dort federführend betreute Personalführungs- und Informationssystem der Bundeswehr (PERFIS) durch ein neues System ersetzt werden soll (18. TB Nr. 26.2). Im Berichtszeitraum hat das BMVg zum einen den dort kritisierten, veralteten Erlass über die Führung der Personalunterlagen der Soldaten aus dem Jahr 1965 durch die „Bestimmungen über die Führung der Personalakten der Soldaten und der Personalunterlagen mit Personalaktenqualität“ vom 6. August 2001 ersetzt, die auch einen Abschnitt über die Führung von automatisierten Personalunterlagen enthalten. Zum anderen hat es damit begonnen, unter dem Stichwort PERFIS II das Datenbanksystem SAP R/3 HR für die Verwaltung der Personaldaten von Soldaten und zivilen Angehörigen der Bundeswehr und des übrigen Geschäftsbereichs des BMVg einzuführen. Zu diesem Datenbanksystem habe ich in meinem 18. TB (Nr. 8.6.4) ausführlich Stellung genommen.

Bei einer Wehrbereichsverwaltung habe ich mir die Implementierung der Software angesehen. Dabei habe ich auf zahlreiche Mängel hinweisen müssen, da die für die automatisierte Personaldatenverarbeitung geltenden gesetzlichen Regelungen (§ 29 Soldatengesetz für die Personaldaten der Soldaten und die §§ 90 ff. Bundesbeamtengesetz für die Personaldaten der Beamten und Angestellten) nicht vollständig eingehalten worden sind.

Insbesondere habe ich bemängelt, dass

- eine Vielzahl von Daten erhoben und in das System eingestellt werden, deren Erforderlichkeit für Zwecke der Personalplanung und -verwaltung nicht hinreichend dargetan werden konnte;
- die bestehende Zugriffsregelung so ausgestaltet ist, dass alle Berechtigten, die Zugang zu PERFIS II haben, auch auf alle dort abgelegten Daten zugreifen können, gleichgültig, ob dies für die Erfüllung ihrer Aufgaben erforderlich ist oder nicht;
- eine Schnittstelle zum Programm MS-Excel besteht, sodass selbst dann, wenn für das System SAP R/3 HR eine datenschutzgerechte Zugriffsregelung bestehen sollte, diese durch die Excel-Schnittstelle wieder ausgehebelt wird;
- die Möglichkeit besteht, ungeprüft und unkontrolliert Abfragen über Soldaten und Mitarbeiter im System anzustoßen (freie Abfragen);

– die Übermittlung der Personaldaten unverschlüsselt zwischen der personaldatenbearbeitenden Stelle und dem Rechenzentrum erfolgt;

– keine Regelung für die Protokollierung der Daten existiert, die im Rechenzentrum die Firewall passieren, und damit auch nicht protokolliert wird, wer auf welche Daten im System SAP R/3 HR zugreift.

Von einer förmlichen datenschutzrechtlichen Beanstandung habe ich bislang nur deshalb abgesehen, weil es sich bei der Implementierung des Datenbanksystems SAP R/3 HR um ein Pilotprojekt handelt und mir anlässlich des Beratungs- und Kontrollbesuchs mündlich zugesichert wurde, die festgestellten Mängel abzustellen. Die weitere Entwicklung bei der Einführung von PERFIS II werde ich im Auge behalten.

30.3 Datenschutz im Kreiswehrersatzamt

30.3.1 Die Einführung der elektronischen Akte im Kreiswehrersatzamt – WEWIS

Die Unterstützung von Verwaltungsverfahren durch moderne Technik macht auch vor den Kreiswehrersatzämtern nicht halt. So habe ich mir bei einem Besuch eines Kreiswehrersatzamtes die neueste Entwicklung beim Wehrersatzwesen-Informationssystem (WEWIS) angesehen.

Das System WEWIS unterstützt die Wehrersatzbehörden bei der Erledigung ihrer Aufgaben – angefangen von der Erfassung über die Musterung bis hin zum Ausscheiden der Wehrpflichtigen aus der Wehrüberwachung. Das ursprüngliche WEWIS (alt) wurde durch die Neuentwicklung von WEWIS II ergänzt. Wesentlicher Bestandteil von WEWIS II ist ein Dokumentenmanagementsystem, das eine weitgehend papierlose Bearbeitung des Musterungsverfahrens zum Ziel hat. Es setzt insofern auf WEWIS (alt) auf, als dessen Datenbanksysteme weiterhin genutzt werden. Eine zunächst beabsichtigte Weiterentwicklung von WEWIS II wurde allerdings aufgegeben. Stattdessen ist vorgesehen, das System WEWIS II im Rahmen der Einführung des Datenbanksystems SAP R/3 HR in das System PERFIS II (s. o. Nr. 30.2) einzubinden.

Im System WEWIS II, das in das lokale Netzwerk des Kreiswehrersatzamtes integriert ist, werden alle eingehenden Dokumente per Scanner digitalisiert und indiziert, d. h. der entsprechenden Personalakte (PA) zugeordnet. Darüber hinaus werden die Schreiben ihrer Art nach verschiedenen Indexklassen (z. B. PA Allgemein, PA Ärztlicher Dienst) zugeordnet und entsprechend archiviert. Die Post wird in digitaler Form an die zuständigen Mitarbeiter zur Bearbeitung weitergeleitet. Diese haben nur Zugriff auf die Daten der Akten, die sie zu ihrer Aufgabenerfüllung jeweils benötigen. Darüber hinaus werden durch das in WEWIS II vorhandene Teilprogramm „Ablaufsteuerung ABZ“ die Wehrpflichtigen zeitlich optimal und ohne zusätzlichen Austausch von Papierdokumenten zu den einzelnen Stationen der Musterung geleitet. Bereits die Einladung zur Musterung wie auch die Vorbereitungen für den jeweiligen Musterungstag erfolgen mit Unterstützung von WEWIS II. Anhand seiner Auftragsübersicht kann jeder Mitarbeiter erkennen, welcher Wehrpflichtige im Tagesablauf als nächstes von ihm zu betreuen ist. Anlässlich der Musterung werden zunächst die bereits gespeicherten Personaldaten überprüft. Dokumente, die der Wehrpflichtige zur Musterung mitbringt (z. B. Schulbescheinigungen, ärztliche Gutachten), werden ebenfalls gescannt und seiner digitalen Akte beigefügt. Auch der Ärztliche Dienst des Kreiswehrersatzamtes und der Psychologische Dienst sind in den von WEWIS II geführten Tagesablauf integriert.

Grundlegende datenschutzrechtliche Bedenken habe ich gegen den Einsatz des Systems WEWIS II nicht. Ich habe allerdings auf einige Aspekte hingewiesen, die mir bei meinem Besuch aufgefallen waren und die Benutzung des Systems aus datenschutzrechtlicher Sicht noch verbessern können. Das BMVg hat mir mittlerweile mitgeteilt, dass es diesen Anregungen folgen wird.

Datenschutzrechtlich beanstanden musste ich in diesem Zusammenhang jedoch, dass der Psychologische Dienst des Kreiswehrersatzamtes die Eignungsuntersuchung und -feststellung durchführt, bevor die Wehrdienstfähigkeit des Wehrpflichtigen feststeht. Dies hatte mich auch deshalb überrascht, weil ich diesen Sachverhalt bereits einmal beanstandet hatte (s. 11. TB S. 72). Der Hinweis des Kreiswehrersatzamtes, nach den Änderungen des Wehrpflichtgesetzes durch das Wehrrechtsänderungsgesetz vom 15. Dezember 1995 (BGBl. I S. 1726) sei es zulässig, die Wehrpflichtigen vor der Feststellung ihrer Wehrdienstfähigkeit auf ihre Eignung zu untersuchen, hat mich nicht überzeugt. Nach § 17 Abs. 8 Wehrpflichtgesetz ist es weiterhin nur zulässig, Wehrpflichtige auf ihre Eignung für Verwendungen in den Streitkräften zu untersuchen, soweit dies „erforderlich und notwendig“ ist. Erforderlich und für eine sinnvolle Einplanung der Einberufung notwendig ist die Eignungsuntersuchung und -feststellung jedoch nach wie vor ausschließlich bei wehrdienstfähigen Wehrpflichtigen. Nur in diesem Fall ist auch die Erhebung von psychologischen Daten im Rahmen der Eignungsuntersuchung und -feststellung zulässig. Das BMVg hat mir aufgrund der datenschutzrechtlichen Beanstandung mitgeteilt, dass es anstrebe, die rechtlichen Regelungen so zu ändern, dass eine Eignungsuntersuchung und -feststellung bereits vor der Feststellung der Wehrdienstfähigkeit durchgeführt werden könne. Es begründet dies im Wesentlichen mit verfahrensökonomischen Gesichtspunkten. Dem Wehrpflichtigen solle es erspart werden, für die Eignungsuntersuchung und -feststellung zu einem zweiten Vorstellungstermin beim Kreiswehrersatzamt erscheinen zu müssen. Aus ablauforganisatorischen Gründen könnten Wehrpflichtige nicht in jedem Fall an einem Tag zunächst ärztlich und dann psychologisch untersucht werden. Aus diesem Grund solle bei einigen Wehrpflichtigen die psychologische Untersuchung vorgezogen werden. Sollte sich dann bei der anschließenden ärztlichen Untersuchung herausstellen, dass der Wehrpflichtige wehrdienstunfähig ist, würden die bereits erhobenen psychologischen Daten unverzüglich gelöscht. Bis zum Erlass der hierfür notwendigen gesetzlichen Regelung soll aufgrund einer Einwilligung der betroffenen Wehrpflichtigen bereits so verfahren werden.

Der Argumentation des BMVg kann ich mich nicht verschließen. Insbesondere ist zu berücksichtigen, dass die Wehrpflichtigen zum Teil erhebliche Wege – insbesondere in ländlichen Gebieten – zum zuständigen Kreiswehrersatzamt zurücklegen müssen. Es liegt daher auch im Interesse der Betroffenen – aber auch von deren Arbeitgeber –, die für die Musterung notwendigen Untersuchungen möglichst an einem Tag hinter sich zu bringen. Die notwendige Änderung des Wehrpflichtgesetzes sollte daher so schnell wie möglich angegangen werden.

30.3.2 Erhebung von Daten hinter dem Rücken Wehrpflichtiger

Verschiedene Wehrersatzbehörden (Kreiswehrersatzämter, Wehrbereichsverwaltungen) haben im Rahmen der Bearbeitung von Anträgen auf Zurückstellung oder Befreiung vom Wehrdienst versucht, personenbezogene Daten der Antragsteller ohne deren Beteiligung bei anderen Stellen, wie Hochschulen und Universitäten, zu erheben. Erbeten wurden u. a. Auskünfte zum Ausbildungsstand, zu Prüfungsterminen und zum voraussichtlichen Ende der Studiengänge. Die betroffenen Wehrpflichtigen wurden über diese Datenerhebungen weder informiert noch wurde ihre Einwilligung hierzu eingeholt. Diejenigen, die sich mit dieser Angelegenheit an mich gewandt haben, ha tten lediglich durch Zufall von dieser Verfahrensweise erfahren.

Entgegen meiner Auffassung, dass die zur Entscheidungsfindung der W ehrersatzbehörden im Antragsverfahren erforderlichen Daten in Ermangelung einer weitreichenderen Erlaubnisnorm – etwa im W ehrpflichtgesetz – beim Betroffenen selbst zu erheben sind (§ 13 Abs. 2 Satz 1 BDSG in der bis zum 22. Mai 2001 gültigen Fassung, § 4 Abs. 2 Satz 1 BDSG-neu), vertrat das BMVg zunächst die Ansicht, dass die Auskunftserteilung dur ch die ausbildende Einrichtung in vielen Fällen unverzichtbar sei, da sachgerechte Entscheidungsgrundlagen nur durch umfassende Ermittlungen direkt bei diesen zu erlangen seien. Das BMVg berief sich darauf, dass es zulässig sei, personenbezogene Daten ohne Mitwirkung des Betroffenen zu erheben, wenn die zu erfüllende Verwaltungsaufgabe ihrer Art nach eine Erhebung bei anderen Stellen erforderlich macht und keine Anhaltspunkte dafür bestehen, dass überwie gende schutzwürdige Interessen des Betrof fenen beeinträchtigt werden (§ 13 Abs. 2 Satz 2 Nr. 2 Buchstabe a) BDSG in der bis zum 22. Mai 2001 gültigen Fassung, § 4 Abs. 2 Satz 2 Nr. 2 Buchstabe a) BDSG-neu). An die Erforderlichkeit sind insoweit jedoch strenge Anforderungen zu stellen. Welche Gründe die Datenerhebung direkt bei den Bildungseinrichtungen in den vorliegenden Fällen tatsächlich im Sinne der genannten V orschrift erforderlich gemacht haben sollen, konnte das BMVg mir nicht überzeugend darlegen. Ich hatte insbesondere auch deshalb Zweifel an der Erforderlichkeit der Datenerhebung ohne Beteiligung der betroffenen Wehrpflichtigen, weil es in den mir bekannt gewordenen Fällen durchaus möglich gewesen wäre, diese aufzufordern, die zur Entscheidung der Wehrersatzbehörde benötigten Informationen selbst beizubringen und ggf. durch eine von der Hochschule einzuholende Stellungnahme zu belegen.

Letztendlich habe ich mich mit dem BMVg darauf verständigen können, dass die zur Bearbeitung von Zurückstellungs- und ähnlichen Anträgen erforderlichen Daten grundsätzlich beim Antragsteller erhoben werden. Dieser legt auch selbst die notwendigen Nachweise vor . Sollten diese im Einzelfall nicht zur Entscheidungsfindung ausreichen, wird beim Antragsteller eine schriftliche Einwilligung zur Datenerhebung bei der in Frage kommenden anderen Stelle eingeholt. Für den Fall, dass der Betroffene die Einwilligung nicht erteilt, entscheide t die Behörde nach Aktenlage. Das BMVg hat die betrof fenen Dienststellen angewiesen, entsprechend zu verfahren und auch in den Fällen, in denen bereits Auskunftsersuchen ohne Einwilligung der Betrof fenen gestellt worden waren, von diesen abzusehen. Die V erfahrensanweisung für das Wehrersatzwesen wurde ebenfalls der beschriebenen Regelung angepasst.

Mit diesem datenschutzgerechten Verfahren ist es gelungen, einen angemessenen Interessenausgleich zwischen dem Recht der W ehrpflichtigen auf W ahrung ihres informationellen Selbstbestimmungsrechts und dem Bestreben der zuständigen Behörden nach sachgerechten Entscheidungen im Wehrersatzwesen zu finden.

31 Zivildienst

31.1 Unzulässige Aufbewahrung von Unterlagen über ein Strafverfahren

Eine Eingabe machte mich darauf aufmerksam, dass das Bundesamt für den Zivildienst (BAZ) durch ein strafgerichtliches Verfahren entstandene Verwaltungsvorgänge unter Hinweis auf die Anwendung einschlägiger V orschriften des Bundeszentralregistergesetzes (BZRG) erst nach Ablauf von drei Jahren aus den Personalakten betrof fener Zivildienstleistender entfernt. Unterlagen aus Disziplinarverfahren (im mir vor getragenen Fall aus gleichem Anlass eingeleitet) werden gem. § 69a Zivildienstgesetz (ZDG) mit Zustimmung des Betroffenen hingegen bereits ein Jahr nach Abschluss des V erfahrens aus den Personalakten entfernt und vernichtet. Für den betroffenen ehemaligen Zivildienstleistenden war nicht nachvollziehbar , warum der im Rahmen des Strafverfahrens angefallene V erwaltungsvorgang länger in seiner Personalakte aufbewahrt werden sollte als der aus gleichem Anlass angelegte V organg über ein Disziplinarverfahren.

Das BAZ begründete die dreijährige Aufbewahrung der strafgerichtlichen Vorgänge damit, dass sich diese Frist in Ermangelung einer einschlägigen gesetzlichen Regelung aus der analogen Anwendung von § 34 Abs. 1 Nr . 1 BZRG ergäbe, wonach eine Verurteilung nach Ablauf von drei Jahren nicht mehr in ein Führungszeugnis aufgenommen wird.

Eine solche analoge Anwendung von Fristen des BZRG auf die Personalakten von Zivildienstleistenden halte ich nicht für zulässig. So dient die Führung einer Personalakte vollkommen anderen Zwecken als die Führung des Bundeszentralregisters. Unter Berücksichtigung der Tatsache, dass die Dienstzeit der Zivildienstleistenden selbst nur elf Monate beträgt und auch aus Gründen der Resozialisierung sollten im Rahmen eines Strafverfa hrens angefallene Unterlagen nicht länger in der Personalakte aufbewahrt werden als dies zur Aufgabenerfüllung der Personalverwaltung erforderlich ist. Gründe, die es tatsächlich nötig machen, die im strafgerichtlichen Verfahren entstandenen V erwaltungsvorgänge zwei Jahre länger in der Personalakte aufzubewahren als die aus gleichem Anlass im Disziplinarverfahren entstandenen Vorgänge, sind für mich nicht ersichtlich und konnten auch vom BAZ nicht vor gebracht werden. Im vorliegenden Fall kam hinzu, dass das Strafverfahren – ebenso wie das Disziplinarverfahren – eingestellt worden war und schon aus diesem Grund für das Dienstverhältnis nicht von so großer Bedeutung gewesen sein kann, dass die hierüber entstandenen Unterlagen drei Jahre in der Personalakte hätten aufbewahrt werden müssen.

Nicht zuletzt auch unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit halte ich die analoge Anwendung der in § 69a ZDG festgelegten Aufbewahrungsfristen für die

im strafgerichtlichen Verfahren entstandenen Verwaltungsvorgänge für wesentlich sachgerechter und bin der Ansicht, dass auch diese Vorgänge – genau wie Disziplinarvorgänge – nach einem Jahr aus der Personalakte der Zivildienstleistenden zu entfernen und zu vernichten sind. Ich habe das BAZ daher aufgefordert, die im strafgerichtlichen Verfahren entstandenen Verwaltungsvorgänge in dem an mich herangetragenen Fall aus der Personalakte zu entfernen und zu vernichten und auch die Personalakten aller anderen Zivildienstleistenden und ehemaligen Zivildienstleistenden auf vergleichbare Vorgänge, die ebenfalls zu vernichten sind, zu überprüfen. Das BAZ hat meine Rechtsauffassung letztendlich akzeptiert und auch seine internen Richtlinien über die Aufbewahrung und Vernichtung der durch ein strafgerichtliches Verfahren entstandenen Verwaltungsvorgänge, die in einigen Fällen sogar eine achtjährige Aufbewahrung vorsahen, meinem Vorschlag entsprechend auf der Grundlage der Fristen des § 69a ZDG neu gefasst.

31.2 Datenspeicherung bis zum Rentenalter?

Anlässlich eines Kontrollbesuchs beim Bundesamt für den Zivildienst (BAZ) hatte ich festgestellt, dass dort die mikroverfilmten Personalakten der Zivildienstleistenden bis zur Vollendung des 60. Lebensjahres aufbewahrt und gleichzeitig in einer Archivdatenbank ebenfalls bis zum 60. Lebensjahr gespeichert werden. Die Rechtmäßigkeit dieser – noch dazu doppelten – Datenspeicherung konnte ich nicht erkennen, da gem. § 36 Abs. 5 Zivildienstgesetz die Personalakten nur solange aufzubewahren sind, wie dies zur Erfüllung der Dienstpflicht oder aus versorgungsrechtlichen Gründen tatsächlich erforderlich ist. Ich forderte daher die Löschung der Datensätze derjenigen Zivildienstleistenden aus der Archivdatenbank, denen seit Mitte der Achtzigerjahre eine Dienstzeitbescheinigung ausgestellt wurde, bereits mit Vollendung des 45. Lebensjahres.

Seine ablehnende Haltung hinsichtlich der Löschung dieser Datensätze begründete das BAZ mit der Vielzahl der Zivildienstleistenden und Bausoldaten der ehemaligen DDR. Bei diesem Personenkreis wurden die Dienstzeiten gem. Einigungsvertrag erst ab dem 3. Oktober 1990 an die Rentenversicherungsträger übermittelt. Die davor liegenden Dienstzeiten sind nur im BAZ nachgewiesen. Ohne diese Daten kann das BAZ keine der häufigen Rückfragen der Rentenversicherungsträger beantworten; die Betroffenen verlören ohne die Auskünfte des BAZ einen Teil ihrer Rentenansprüche. Das gleiche gilt für die Vordienstzeiten bei der ehemaligen Nationalen Volksarmee, wenn der Dienstpflichtige später als Kriegsdienstverweigerer anerkannt wurde. Das BAZ macht geltend, dass eine Unterscheidung der einzelnen Personenkreise maschinell nicht möglich sei und eine Datenlöschung daher nur „von Hand“, d. h. nach vorher gehender Akteneinsicht, erfolgen könnte. Dies sei aber aus Kostengründen nicht zu vertreten.

Da die Vordienstzeiten der genannten Personenkreise teilweise mit automatisiertem Datensatz gespeichert, teilweise aber auch nur den mikroverfilmten Wehrstammakten entnommen werden können, ist nach Darstellung des BAZ auch die doppelte Datenspeicherung unverzichtbar.

Eine maschinelle Löschung der Datensätze werde allerdings ab dem Jahrgang 1973 erfolgen, da ab diesem Jahrgang entsprechende Dienstzeiten nicht mehr anfallen können.

Die Begründung des BAZ halte ich für zutreffend. Im Interesse der Betroffenen habe ich gegen die vorgeschlagene Regelung keine datenschutzrechtliche Bedenken erhoben. Hinsichtlich der Behandlung der mikroverfilmten Akten ab dem Jahrgang 1973 bin ich mit dem Bundesministerium für Familie, Senioren, Frauen und Jugend noch im Gespräch.

32 Internationale Zusammenarbeit und Datenschutz im Ausland

32.1 Der 11. September 2001 – Auswirkungen auf den Datenschutz auch international

Die Terroranschläge vom 11. September 2001 haben die Situation des Datenschutzes grundlegend verändert, und zwar nicht nur innerhalb der USA, sondern weltweit. Als erste Reaktion verabschiedete der Kongress noch im Oktober 2001 den USA Patriot Act, der vor allem für Strafverfolgung und Geheimdienste erweiterte Kontrollbefugnisse im Bezug auf die Telekommunikation und das Internet und schärfere Maßnahmen gegen die Geldwäsche brachte. Parallel dazu laufen Anstrengungen zur Intensivierung des internationalen Datenaustausches (vgl. dazu auch Nr. 2).

Im November 2002 hat der Präsident dem Kongress den „Homeland Security Bill“ vorgelegt. Es handelt sich dabei um eine Vielzahl von neuen Regelungen und Änderungen geltender Bestimmungen. Sein Kernstück ist die Schaffung des „Departement of Homeland Security (DHS)“ einer Art Super-Sicherheitsbehörde. In ihr sollen 22 bestehende Bundesbehörden zusammengeführt werden, darunter Geheimdienste, die Küstenwache, der Zoll und die Grenzpolizei. Das DHS wird etwa 170 000 Menschen beschäftigen. Neben umfangreichen organisatorischen und dienstrechtlichen Bestimmungen enthält der Entwurf z. B. ein Programm zur Förderung von Anti-Terror-Technologien, Erleichterungen des Datenexports an andere Staaten – und damit des Austausches – einschließlich solcher Daten, die durch elektronische Abhörverfahren gewonnen wurden. Weiterhin werden „kritische Infrastrukturen“ vom Freedom of Information Act ausgenommen und damit der öffentlichen Information entzogen. Innerhalb der neuen Sicherheitsbehörde sollen ein Beauftragter für Menschenrechte und Bürgerfreiheiten ernannt werden, der Hinweisen auf Grundrechtsverletzungen nachgehen soll, und ein Privacy Policy Officer (also ein interner Datenschutzbeauftragter), der für den Datenschutz primär verantwortlich sein soll. Der Datenschutz findet damit zwar Erwähnung, von einer effektiven unabhängigen Kontrolle nach europäischem Standard bleibt die Regelung aber weit entfernt.

Parallel zu dieser Neuorganisation des Sicherheitsbereichs hat die US-Regierung unter dem Namen „Total Information Awareness“ ein außerordentlich umfangreiches und ehrgeiziges Entwicklungsprojekt mit einem Volumen von mehreren hundert Millionen Dollar aufgelegt. Es zielt darauf, vorhandene Informationstechnik im größtmöglichen Maßstab einzusetzen und neue Technologien zu entwickeln, um anhand von Mustern, Modellen und Algorithmen im Wege eines gigantischen data mining terroristische Aktivitäten frühzeitig zu entdecken, die Akteure zu erkennen und zu orten und so den Sicherheitsorganen einen raschen Zugriff zu ermöglichen. Binnen fünf Jahren soll dazu ein Prototyp entstehen. Neben der Nutzung vorhandener Datenbestände sollen neue Datenquellen erschlossen werden, etwa durch

Videoüberwachung und Biometrie. Das Ergebnis wäre eine Datenbank einer völlig neuen Größenordnung.

Das Programm wurde dem dazu neu errichteten „Information Awareness Office (IAO)“ übertragen, das Teil des militärischen Forschungsinstituts DARPA ist. Das Logo des IAO zeigte ein alles sehendes Auge auf der Spitze einer Pyramide und den Slogan „Scientia est Potentia“ (Wissen ist Macht). Ein Kommentator der Washington Post bemerkte, niemand hätte sich einen Plan ausdenken können, der besser geeignet wäre, das Orwell lesende Publikum in Angst und Schrecken zu versetzen (Editorial vom 16. November 2002 S. A 20).

Das Auge und der Slogan wurden zwar inzwischen entfernt. Aber in der amerikanischen Öffentlichkeit – und nicht nur dort – bleibt die Befürchtung, dass die Maßnahmen zu einem dichten Netz modernster Massenüberwachungstechnologie führen wird, mit dessen Hilfe in einem bisher kaum vorstellbaren Ausmaß Daten über rechtmäßige Aktivitäten gesetzestreuer Bürger gesammelt werden, die dann – legal oder illegal – für die verschiedensten Zwecke Verwendung finden könnten.

Die amerikanischen Vorhaben sind auch für Nicht-US-Bürger von größter Bedeutung. Einbezogen werden nicht nur die Datenbestände des Finanz- und des Verkehrssektors (Geld- und Reisebewegungen), sondern prinzipiell jeder Datenbestand, also beispielsweise Kunden- oder Arbeitnehmerdaten der gesamten Wirtschaft, gleichgültig ob sie über das Internet zugänglich sind. So können die Käufer bestimmter Waren ebenso relevant werden wie die Leser bestimmter Medien, Patienten mit bestimmten Diagnosen oder Verschreibungen und die Besucher bestimmter Veranstaltungen. Spätestens wenn amerikanische Unternehmen oder deren europäische Töchter oder auch europäische Unternehmen mit Niederlassungen in den USA über solche Daten verfügen, werden diese Gegenstand der „Total Information Awareness“. Die Drohung der US-Regierung, ausländischen Fluglinien die Landerechte in den USA zu entziehen, wenn sie nicht bereit sind, den amerikanischen Behörden umfassenden Zugriff auf ihre Online-Buchungs-Systeme zu gewähren, macht nur zu deutlich, wie schnell auch Daten von Personen, die sich weit ab vom Einfluss amerikanischer Sicherheitsbehörden wähnen, in deren Reichweite gelangen werden.

Es zeigt sich, dass die Maßnahmen zur Bekämpfung des Terrorismus und ihre datenschutzmäßigen Implikationen nicht weniger international sind wie die terroristische Bedrohung selbst. Die Konsequenz kann nur in einer stärkeren internationalen Koordination der Datenschutzpolitik bestehen. Sie muss wesentlich auch von den unabhängigen Datenschutzbehörden geleistet werden. Es ist daher dringender denn je, dass endlich auch die USA über eine unabhängige Datenschutzinstanz verfügen.

32.2 Datenschutz im Europarat

Mit der Aufnahme von Armenien und Aserbaidschan ist die Zahl der Mitglieder des Europarates auf 43 angewachsen. Mit Verabschiedung der Ratifikationsgesetze in Lettland und Litauen aus dem Jahre 2001 sind mittlerweile 23 Staaten dem „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten“ – der Europaratskonvention 108 – aus dem Jahre 1981 beigetreten (die Konvention und die dazu ergangenen Empfehlungen und Berichte sind – in englisch und französisch – abrufbar über http://www.coe.int/T/E/Legal_affairs/Legal_cooperation/Data_protection/).

Einer Bestandsaufnahme der Konvention 108 und Überlegungen für ihre Weiterentwicklung diente eine vom Europarat und meiner polnischen Kollegin am 19. und 20. November 2001 in Warschau organisierte Konferenz. Weitere Themenschwerpunkte befassten sich mit den grenzübergreifenden Antwortversuchen des Datenschutzes auf die Herausforderungen der Informationsgesellschaft und den Rechten des Einzelnen in der globalisierten vernetzten Welt.

Nach der Verabschiedung eines Empfehlungsentwurfs über den Schutz von personenbezogenen Daten, die zu Versicherungszwecken erhoben und verarbeitet werden (zu den Vorarbeiten s. 16. TB, 17. TB und 18. TB je Nr. 32.1), schloss die Projektgruppe Datenschutz (CJ-PD) den dazugehörigen Begleitbericht ab. Das Gesamtpaket wurde vom Ministerkomitee am 18. September 2002 verabschiedet und als Empfehlung R(02)9 angenommen. Die CJ-PD beschäftigte sich außerdem mit einem Sachverständigenbericht über den Schutz der Privatsphäre im Zusammenhang mit der Videoüberwachung und beschloss die Ausarbeitung eines Katalogs von Leitgrundsätzen zum Schutz des Einzelnen bei der Erhebung und Verarbeitung personenbezogener Daten. Das Ziel der Leitgrundsätze liegt darin, die Garantien für die Betroffenen beim Einsatz von videogestützter Überwachungstechnik zu präzisieren und je nach Sachlage (Beobachten, Beschaffen oder Speichern von personenbezogenen Daten) zu erweitern. Auch diese Arbeiten standen unter dem Eindruck des 11. September 2001, was u. a. dadurch zum Ausdruck kam, dass verschiedene Staaten eine Ausklammerung der Videoüberwachung der Polizeibehörden vom Anwendungsbereich der Leitgrundsätze forderten. Allerdings stellte sich die Mehrheit der Gruppenmitglieder diesem Ansinnen mit dem Hinweis entgegen, dass die Leitgrundsätze den Einsatz von Videoüberwachung zu polizeilichen Zwecken nicht grundsätzlich verbieten, sondern das Gleichgewicht zwischen Sicherheitsbedürfnis und der Achtung der Grundrechte und Grundfreiheiten garantieren wollen.

Auch der Beratende Ausschuss des Europaratsübereinkommens (T-PD) führte einen Meinungsaustausch zur Situation nach den Anschlägen vom 11. September 2001 durch. Das Gremium sah sich zu dem Hinweis veranlasst, dass der Schutz personenbezogener Daten einerseits und die Verfolgung von Straftaten und insbesondere der Kampf gegen den Terrorismus andererseits kein Gegensatzpaar bilden, jedoch die Notwendigkeit der Terrorismusbekämpfung und die Achtung der Grundrechte und Grundfreiheiten im Gleichgewicht bleiben müssen. Da unverhältnismäßige Maßnahmen diese Rechte und Freiheiten nachhaltig beeinflussen können, plädierte der Ausschuss T-PD für die Berücksichtigung entsprechender datenschutzrechtlicher Regelungen im Rahmen der von den Justizministern beabsichtigten Maßnahmenpakete.

32.3 Ein Blick in europäische Länder außerhalb der Union

32.3.1 Der Europäische Wirtschaftsraum und die Schweiz

Nachdem Norwegen und Island 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), ihre Datenschutzgesetze an die Vorgaben der Richtlinie angepasst haben (vgl. 18. TB Nr. 32.2.1), hat nun auch Liechtenstein ein Datenschutzgesetz erlassen (Gesetz vom 14. März 2002, Landesgesetzblatt Nr. 55 vom 8. Mai 2002).

In der Schweiz soll das eidgenössische Bundesgesetz über den Datenschutz aus dem Jahre 1992 einer Teilrevision unterzogen werden. Hierzu verabschiedete der Schweizerische Bundesrat am 5. September 2001 einen Entwurf. Die vorgesehenen Änderungen beziehen sich u. a. auf den grenzüberschreitenden Datenverkehr, die Datensicherheit, die Meldepflichten, das Auskunftsrecht und den Rechtsschutz des Betroffenen.

32.3.2 Die Mittel- und Osteuropäischen Staaten

Der dem Parlament in Lettland seit dem Jahre 1998 vorliegende Regierungsentwurf gelangte im Jahre 2001 zur Gesetzesreife. Die durch das Gesetz eingerichtete staatliche Datenschutzbehörde ist allerdings nicht unabhängig, da sie ihrerseits der Kontrolle durch das Justizministerium unterliegt.

Auch die gesetzgeberischen Vorhaben auf Kabinetts- und Parlamentsebene, über die ich im 17. und 18. TB (jeweils Nr. 32.2.2) betreffend Bulgarien, Moldawien und Rumänien berichtet hatte, wurden in allen drei Ländern im Jahre 2001 in die Tat umgesetzt. Während das bulgarische Datenschutzgesetz ein unabhängiges öffentliches Kontrollorgan vorsieht, dessen Leiter vom Parlament gewählt wird, ist die Kontrollinstanz in Moldawien in die staatliche Behördenstruktur eingebunden. In Rumänien überwacht ein so genannter Volksanwalt die Einhaltung des Datenschutzgesetzes; den Betroffenen steht in Schadensfällen der Rechtsweg offen.

In der Ukraine brachte die Regierung im Jahr 2001 den Entwurf eines Datenschutzgesetzes in das Parlament ein.

Die Mitglieder der neu eingerichteten bulgarischen Datenschutzkommission habe ich im Dezember 2002 zu einem einwöchigen Besuch in meiner Dienststelle empfangen, um ihnen Erfahrungen der Kontrollpraxis zu vermitteln.

32.4 Entwicklungen im nicht europäischen Ausland

Nachdem Chile im Jahre 1999 als erstes südamerikanisches Land die Verarbeitung personenbezogener Daten im öffentlichen und privaten Bereich einer gesetzlichen Regelung zugeführt hatte (vgl. 18. TB Nr. 32.3), besitzt nunmehr auch Argentinien ein Datenschutzgesetz, das als „Habeas Data“ im Wesentlichen auf dem spanischen Datenschutzgesetz und auf Elementen der EG-Datenschutzrichtlinie aufbaut. An bereichsspezifischen Regelungen wurden im Jahre 2001 in Peru ein „Gesetz über die Kreditauskunfteien“ und in Venezuela ein „Gesetz zur Datenübertragung und digitalen Signatur“ verabschiedet. Dem brasilianischen Parlament liegt ein stark an die EG-Datenschutzrichtlinie angelehnter Regierungsentwurf für ein allgemeines Datenschutzgesetz vor, während sich in Chile als erste sektorielle Regelung für das dortige Datenschutzrecht der Entwurf eines Gesetzes über die digitale Signatur im parlamentarischen Verfahren befindet; in den Ausschussberatungen fand u. a. das deutsche Signaturgesetz aus dem Jahre 1997 in vergleichender Perspektive Berücksichtigung.

Das Datenschutzbewusstsein in den USA nahm im Berichtszeitraum weiter zu. Votierten vor der Jahrtausendwende noch 57 % aller US-Bürger grundsätzlich für eine gesetzliche Regelung des Umgangs mit personenbezogenen Daten (vgl. 18. TB Nr. 32.3), so waren es nach einer Gallup-Umfrage aus dem Jahre 2001 bereits zwei Drittel aller Befragten, die die Auffassung teilten, der Bundesgesetzgeber müsse entsprechend tätig werden. Laut Umfrage sind nahezu 80 % aller E-Mail-Nutzer und Internetsurfer beunruhigt über den Schutz ihrer Privatsphäre und 28 % sind sehr beunruhigt, insbesondere wenn es online um die Preisgabe der Kreditkartennummer oder der Sozialversicherungsnummer geht. Die hoffnungsvollen Ansätze aus der Zeit der Clinton-Administration (vgl. 18. TB Nr. 32.2) wurden jedoch nicht weiterverfolgt. Die derzeitige amerikanische Regierung konzentriert sich – zumal seit dem 11. September 2001 – ganz auf das Thema Sicherheit; im gleichen Zuge wird der Datenschutz abgebaut (vgl. oben 32.1). Als Reaktion treten Nichtregierungsorganisationen aus Verbraucher- und Bürgerrechtsorganisationen zunehmend gemeinsam auf, um auf die Schaffung und Durchsetzung von Datenschutzregeln zu drängen. Insbesondere sollen die Kongressabgeordneten auf die bestehenden rechtlichen Defizite und die Forderungen aus Datenschutzsicht aufmerksam gemacht werden, zu denen insbesondere die Offenlegung der Datenverarbeitungspraktiken der Unternehmen („notice“), das Wahlrecht der Konsumenten hinsichtlich der Datenverarbeitung („choice“) sowie eine unabhängige Kontrollinstanz zählen.

Der „Personal Information Protection and Electronic Documents Act“, der in Kanada den Datenschutz im privaten Bereich erstmals umfassend regelt, war in einer ersten Stufe am 1. Januar 2001 in Kraft getreten (vgl. 18. TB Nr. 32.3). Er galt bisher nur für personenbezogene Daten über Kunden und Beschäftigte, die von Organisationen, die unter Bundesrecht fallen, im Zuge ihrer kommerziellen Tätigkeit verarbeitet werden. Seit dem 1. Januar 2002, dem Beginn der zweiten Stufe seines In-Kraft-Tretens, findet das Gesetz auch auf alle Gesundheitsdaten Anwendung, über die dem Bundesrecht unterfallende Organisationen verfügen. In einer dritten und letzten Stufe wird das Gesetz ab dem 1. Januar 2004 für alle Organisationen gelten, die im Zuge ihrer kommerziellen Tätigkeit personenbezogene Daten verarbeiten, unabhängig davon, ob sie dem Bundesrecht unterliegen oder nicht. Auch Unternehmen, die der gesetzlichen Regelung durch die Provinz unterliegen, werden erfasst, solange die betreffende Provinz noch keine entsprechenden Datenschutzregelungen erlassen hat.

Das bisher nur auf öffentliche Stellen anwendbare australische Datenschutzgesetz aus dem Jahre 1988 wurde durch ein Änderungsgesetz in seinem Anwendungsbereich auf private Stellen ausgedehnt. Der im Dezember 2001 in Kraft getretene „Privacy Amendment (Private Sector) Act“ hält allerdings an den zahlreichen bedeutsamen Ausnahmeregelungen fest, die schon bei der Gesetzesvorlage kritisiert wurden (vgl. 18. TB Nr. 32.3). So bleibt es bei einer Reihe von Durchbrechungen des Zweckbindungsgedankens und dem Ausschluss so wichtiger Bereiche wie des Arbeitnehmerdatenschutzes, der Medien und der politischen Parteien.

In Neuseeland, das bestrebt ist, sein Datenschutzgesetz aus dem Jahre 1993 an die Adäquanzkriterien der Artikel 25 und 26 der EG-Datenschutzrichtlinie anzupassen, liegt derzeit dem Parlament ein entsprechender Regierungsentwurf vor.

Die Besuche japanischer Regierungsdelegationen in meiner Dienststelle haben sich mittlerweile zu einer kleinen T radition verfestigt (vgl. 17. TB und 18. TB, jeweils Nr . 32.3). Der zurückliegende Gedanke naustausch aus dem Jahre 2001 hatte die Novellierung des BDSG und die japanischen Reformüberlegungen für den bislang nicht gesetzlich geregelten privaten Bereich zum Gegenstand. Der schon jetzt als „Grundgesetz für den Datenschutz" bezeichnete Entwurf, der den öffentlichen und den nicht öf fentlichen Bereich gemeinsam regeln soll, befindet sich noch in der parlamentarischen Beratung.

Auch in Malaysia liegt der Entwurf eines „Personal Data Protection Act" vor, während die Bundesregierung in Indien einen IT-Aktionsplan verabschiedete, der Regelungen für den Umgang mit computerisierten Daten beinhaltet.

32.5 Die Internationale Datenschutzkonferenz

Als Pendant zu den Frühjahr skonferenzen der europäischen Datenschutzbeauftragten (s. o. Nr. 3.9) tagten die 23. und 24. Internationale Datenschutzkonferenz vom 24. bis 26. September 2001 in Paris und vom 9. bis 11. September 2002 in Cardiff.

Die Herbstkonferenz, die in der Universität Sorbonne über 50 Delegationen aus allen Erdteilen zusammenführte, dokumentierte auf eindrucksvolle W eise den weltweiten Anspruch des Grundrechts auf Da tenschutz. Angesichts der erst wenige Tage zurückliegenden Ereignisse des 1 1. September mahnte die Konferenz wohlüberlegte Vorgehensweisen in dem sensiblen Spannungsfeld zwischen Sicherheit und Freiheit an. Der grund- und menschenrechtliche Charakter des Datenschutzes wu rde auch von Premierminister Jospin hervorgehoben, der gerade unter dem Eindruck des jüngsten Geschehens eine für den Datenschutz ermutigende Rede hielt. Die Arbeitssitzungen waren einem weit gespannten Themenkatalog gewidmet, der vor allem den einzelnen (the data subject) in den Blick nahm und dabei die unterschiedlichen Rollen des Betrof fenen, etwa als Konsument, Internetsurfer, Arbeitnehmer oder Patient näher beleuchtete. In meinem Beitrag zu aktuellen Fragen des Gesundheits- und Patientendatenschutzes habe ich besonders betont, dass in Deutschland ein breiter Konsens darüber besteht, auch bei der gebotenen Automatisierung der Verarbeitung und Nutzung von Gesundheitsdaten die Selbstbestimmung der Patienten unverändert zu beachten. Für die Teilnahme an künftigen Konferenzen wurde ein Akkreditierungsverfahren festgelegt.

Wie die Europäische Frühjahrskonferenz 2001 in Athen (s. o. Nr. 3.9) befasste sich auch die Internationale Konferenz von Cardiff mit dem Thema der Aufbewahrung von Verkehrsdaten. In einer Entschließung stellte sich die Konferenz Überlegungen im Rahmen des Dritten Pfeilers der Europäischen Union entgegen, in allen Bereich der T elekommunikation und des Internet Mindestspeicherfristen von einem Jahr oder länger für die bei der Nutzung dieser Medien anfallenden Verbindungsdaten einzuführen. Derart umfassende systematische Speicherungen personenbezogener Daten zu Zwecken einer möglichen Strafverfolgung oder zur Wahrung anderer Sicherheitsinteressen bezeichnete sie als eindeutig unverhältnismäßig und in keinem Fall akzeptabel (s. Anlage 4). Wie bereits anlässlich der Vorjahreskonferenz in Paris widmeten sich die Delegierten – neben aktuellen Fragen etwa des Internet, des E-Government und der Videoüberwachung – auch in Cardif f eingehend den Terroranschlägen vom 1 1. September und den Folgen für die Menschenrechte und Grundfreiheiten und insbesondere für den Datenschutz. In einer entsprechenden Entschließung mahnen die Datenschutzbeauftragten das richtige Gleichgewicht zwischen Sicherheitsbedürfnissen und Achtung der individuellen Freiheiten an, da ansonsten genau die Grundfreiheiten unterlaufen würden, deren Schutz beabsichtigt sei (s. Anlage 5).

32.6 Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD)

Auch im Rahmen der Gremie narbeit der OECD (Arbeitsgruppe Informationssicherheit und Schutz der Privatsphäre, WISP) fand im Berichtszeitraum eine Reihe von datenschutzrechtlichen Aktivitäten statt. Unter anderem befassten sich eine Konferenz und Arbeitsgruppensitzungen in Den Haag und Paris mit Lösungsmöglichkeiten für die außer gerichtliche Beilegung von grenzüberschreitenden Streitigkeiten zwischen Konsumenten und Unternehmen auf dem Gebiet von Online-T ransaktionen. Im V ordergrund standen dabei bislang Fragen des inte rnationalen Privatrechts, nach dem sich das bei transnationalen Streitigkeiten anzuwendende Recht bestimmt. Für die weitere zu erwartende Diskussion wird die OECD eine Zusammenschau unterschiedlicher Modelle und Mechanismen zur Beilegung von Konflikten und Streitigkeiten in der Welt des Netzes ohne gerichtliche Inanspruchnahme erarbeiten. Deren datenschutzrechtliche Tauglichkeit soll in einer späteren Beratungsphase auf den Prüfstand kommen.

Große Aufmerksamkeit widmete die OECD auch in den zurückliegenden Jahren der V erbreitung von datenschutzfreundlichen Technologien (Privacy Enhancing T echnologies, PETs) zum Schutz der Privatsphäre im Internet. Kritik fanden die bei vielen PET-Produkten fehlenden Informationen über deren Funktionalität im Einzelnen und die oft mangelhaften Aussagen die Hersteller betreffend, was auf Seiten der Anwender entweder blindes V ertrauen voraussetzt oder zur Zurückhaltung führt.

Im Rahmen ihrer Befassung mit genetischen Untersuchungen hebt die OECD die besonde re Sensibilität genetischer Daten hervor, die – im Vergleich zu medizinischen Daten – eines weiteren, besonderen Schutzes bedürfen. Ein Lenkungsausschuss soll für die Erstellung einer Übersicht sorgen, die die einzelnen Problembereiche beim Umgang mit genetischen Daten unter Berücksichtigung bereits vorliegender Arbeiten des Europarats zusammenfasst.

33 Aus meiner Dienststelle

33.1 25 Jahre Bundesdatenschutzgesetz

Anlässlich des 25-jährigen Jubiläums des Bundesdatenschutzgesetzes habe ich am 1 1. Juni 2002 zu einem Festakt nach Berlin eingeladen. Gäste waren viele Mitglieder des Deutschen Bundestages, Behördenleiter sowie Datenschutzbeauftragte von Behörden und Unternehmen. Grußworte sprachen der Präsident des Deutschen Bundestages, W olfgang Thierse, sowie der Staatssekretär im Bundesministerium des Innern, Claus Henning Schapper . Die Festrede hielt die Präsidentin des Bundesverfassungsgerichts a. D., Frau Prof. Dr. Jutta Limbach.

Einen Schwerpunkt der Veranstaltung bildete die Entwicklung des Datenschutzes seit Ende der Siebzigerjahre. Das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983, mit dem der Datenschutz Grundrechtscharakter erhielt, sowie die Implementierung des Datenschutzes auf europäischer Ebene mit der EU-Richtlinie zum Datenschutz vom 24. Oktober 1995 waren Meilensteine auf diesem Weg. Die letzte große Herausforderung für den Datenschutz waren die Folgen des 11. September. Bei den Maßnahmen zur Terrorismusbekämpfung wurde deutlich, wie notwendig, aber auch schwierig es für den Staat ist, eine Balance zu finden zwischen der Wahrung von Sicherheit und Ordnung einerseits und der gleichzeitigen Gewährleistung der Freiheitsrechte der einzelnen Bürger andererseits. Schließlich wurden die künftigen Anforderungen an den Datenschutz thematisiert. Hierzu zählen beispielsweise die fortschreitende Informationstechnik oder auch der datenschutzgerechte Umgang mit den entschlüsselten Informationen des menschlichen Genoms.

Bundestagspräsident Wolfgang Thierse würdigte das Bundesdatenschutzgesetz in seinem Grußwort als „wesentlichen Beitrag zu unserer Demokratie kultur". Dies schätze er als ehemaliger DDR-Bürger besonders; dabei nahm er Bezug auf die Erfahrungen mit der Stasi.

Staatssekretär Claus Henning Schapper bezeichnete das Gesetz als Meilenstein in der Geschichte der Persönlichkeitsrechte. Ein wesentliches Ziel der Modernisierung des Datenschutzrechts sollte es sein, die vielfach unübersichtlichen Datenschutzregelungen zu vereinfachen und ihre Effektivität zu steigern.

Im Rahmen ihrer Festrede warnte die ehemalige Präsidentin des Bundesverfassungsgerichts, Frau Prof. Dr. Jutta Limbach, vor einer ausufernden Erhebung von Daten. Wegen der zunehmenden Bedeutung des Datenschutzes forderte sie, das Recht auf informationelle Selbstbestimmung in das Grundgesetz aufzunehmen und auch das Amt des Bundesdatenschutzbeauftragten in der Verfassung zu verankern.

33.2 Erfolgreiches Symposium in Bonn

Seit September 2000 lade ich einmal jährlich zu einem Datenschutzsymposium nach Bonn ein. Diese Veranstaltung wurde vom Fachpublikum als Wissens- und Diskussionsforum mit großem Interesse angenommen. So konnte ich in den vergangenen Jahren jeweils mehr als 80 Teilnehmer in Bonn begrüßen.

In den ersten beiden Jahren beschäftigte sich das Symposium noch ausschließlich mit datenschutzrechtlichen Fragestellungen aus dem Bereich der Telekommunikation, so etwa mit der Novellierung der Telekommunikations-Datenschutzverordnung oder mit datenschutzrechtlichen Problemen bei der Telekommunikationsüberwachung. Insbesondere das Zusammenwachsen der verschiedenen Kommunikations- und Informationstechnologien und die darauf aufbauenden Geschäftsmodelle machten es erforderlich, das Themenspektrum des Symposiums zu erweitern. So wurden erstmals im Jahr 2002 auch Themen aus dem Bereich des Teledienstedatenschutzes erörtert.

Nach dem bisherigen Erfolg der Veranstaltung werde ich auch in den nächsten Jahren ein Symposium zu Datenschutzfragen aus den neuen Medien anbieten, um damit Fachleuten die Gelegenheit zu geben, sich in Bonn aktuell informieren und austauschen zu können.

33.3 Der Datenschutzbeauftragte im Internet

Seit Februar 1999 ist meine Dienststelle mit einem eigenen Informationsangebot im Internet vertreten. Die Homepage meiner Dienststelle (s. Abbildung 6) ist unter der Adresse http://www.datenschutz.bund.de oder http://www.bfd.bund.de erreichbar.

Im Berichtszeitraum 2001/2002 konnte ich ca. 7,3 Millionen Seitenanfragen verzeichnen. Das entspricht im Durchschnitt etwa 10 000 Seitenanfragen pro Tag. Dabei entwickelten sich die Zugriffszahlen insbesondere im Jahre 2002 zu meiner Freude kontinuierlich nach oben (s. Abbildung 7).

Die meisten Zugriffe entfielen mit ca. 73 % auf die Rubrik „Materialien zum Datenschutz", die unter anderem meine Tätigkeitsberichte, meine Informationsbroschüren „BfD-INFO 1 bis 5" wie auch Entschließungen der Datenschutzkonferenzen und einschlägige Gesetze und Verordnungen enthält.

Mein Internetangebot unterliegt einer stetigen Weiterentwicklung. So habe ich die in 2002 überarbeiteten BfD-Infos 1 und 5 bereitgestellt und das Layout meiner Tätigkeitsberichte aus 1995/96 und 1997/98 vereinheitlicht. Diese Maßnahmen und weitere geplante Verbesserungen sind auch mit dem eGovernment-Projekt „BundOnline 2005" der Bundesregierung abgestimmt.

Mein Internetangebot ist auf einem Server beim Competencecenter 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.

33.4 Einführung der gleitenden Arbeitszeit

Seit dem 1. Mai 2001 nimmt meine Dienststelle mit Unterstützung des Bundesverwaltungsamtes an dem Modellprojekt „Arbeitszeitflexibilisierung" teil. Hierzu habe ich eine Dienstvereinbarung mit dem Personalrat im Bundesministerium des Innern abgeschlossen. Bei dem Modellvorhaben wird auf eine so genannte Kernarbeitszeit, in der alle Bediensteten anwesend sein müssen, verzichtet. Stattdessen ist eine Servicezeit eingerichtet, in der in jeder Organisationseinheit der Behörde ein kompetenter Ansprechpartner erreichbar sein muss. Auf eine Einwirkung oder Kontrolle durch Vorgesetzte wird weitgehend verzichtet. Gefordert werden dagegen die Eigenverantwortung der Mitarbeiter und die Absprache der Bediensteten untereinander.

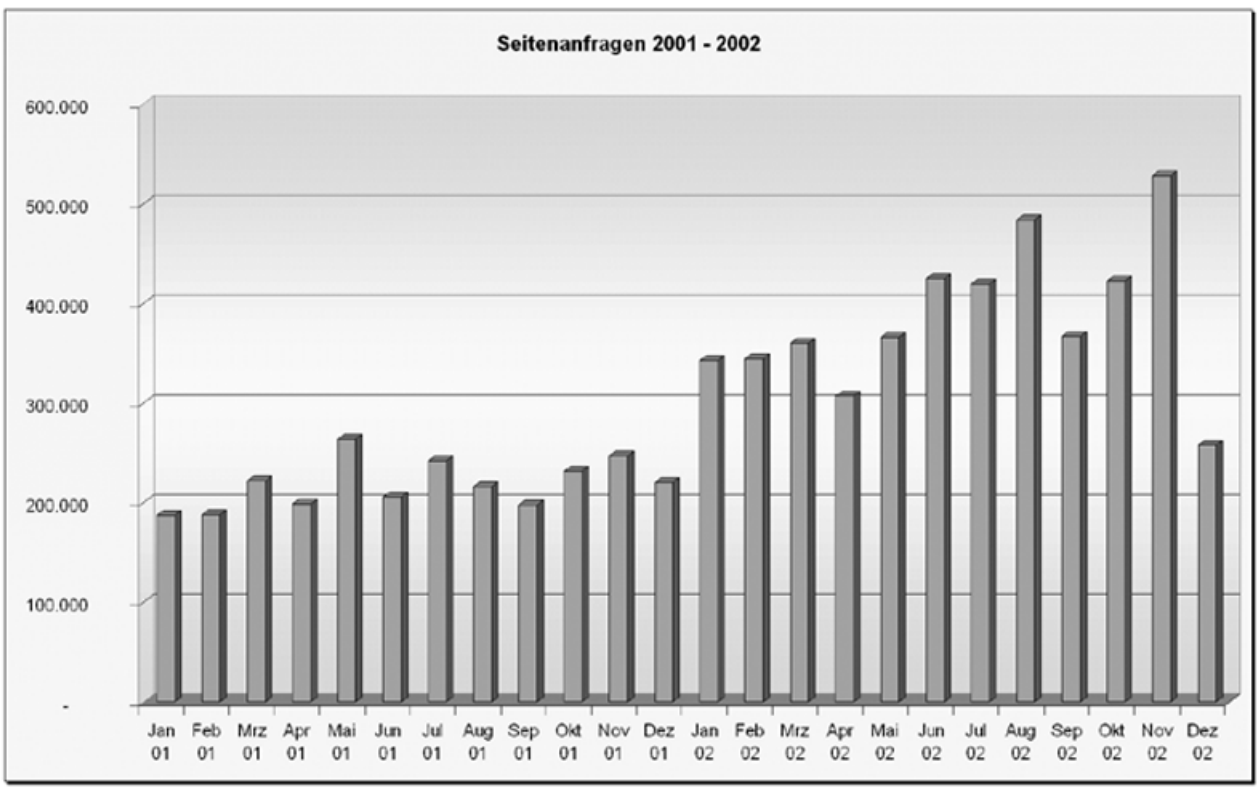
Die bisherigen Erfahrungen mit dem Modellprojekt zeigen ein hohes Maß an Zufriedenheit der Mitarbeiter, eine intensivere Kommunikation und eine verbesserte Zusammenarbeit.

33.5 Neues Informationsmaterial

Die Umsetzung der Europäischen Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 in deutsches Recht mit der am 23. Mai 2001 in Kraft getretenen Novellierung des Bundesdatenschutzgesetzes erforderte auch eine Überarbeitung der vom BfD herausgegebenen Informationsbroschüren. Mit der neu konzipierten „BfD-INFO 1" wurde eine Basisinformation bereitgestellt, die neben dem Gesetzestext und

Abbildung 6 und 7 (zu Nr. 33.3)

Der Datenschutzbeauftragte im Internet



weiteren wichtigen Materialien eine kurze Einführung in das BDSG enthält. Diese soll helfen, sich die nicht immer einfache Materie des Datenschutzrechtes zu erschließen. Die mit 25 000 Exemplaren aufgelegte INFO 1 wurde von den Bürgerinnen und Bürgern gut angenommen und ist nach wenigen Monaten nahezu vergriffen. Eine Neuauflage ist in Vorbereitung.

Die zum Ende des Jahres 2002 neu erstellte „BfD-INFO 4" informiert über die in der Novelle erfolgten Regelungen für die behördlichen und betrieblichen Datenschutzbeauftragten. Sie soll eine Hilfestellung geben für diejenigen, die mit der wichtigen Aufgabe des internen Datenschutzbeauftragten betraut werden. Zugleich sollen aber auch interessierte Bürger und Mitarbeiter in einem Unternehmen oder einer Verwaltung Gelegenheit haben, sich über die Aufgaben „ihres" Datenschutzbeauftragten zu informieren.

Die in der Telekommunikation eingesetzten Technologien erzeugen eine Vielzahl von Daten, bei denen in der Mehrzahl ein Personenbezug zu dem jeweiligen Nutzer des Telekommunikationsdienstes besteht. Vor diesem Hintergrund bestand schon früh ein Informationsbedürfnis der Bürger, zu erfahren, wie in diesem auch durch das Gebot des Fernmeldegeheimnisses gekennzeichneten Bereich mit ihren Daten umgegangen werden darf. Seit März 1998 wird unter dem Titel „Datenschutz in der Telekommunikation" die „BfD-INFO 5" herausgegeben, die mittlerweile in der fünften Auflage vorliegt. Darin wird ein Überblick über die einschlägigen gesetzlichen Regelungen und ihre Auslegung in der Praxis gegeben.

33.6 Mehr E-Mail-Sicherheit mit SPHINX

Sowohl im dienstlichen als auch im privaten Bereich werden immer häufiger Informationen oder Dokumente in elektronischer Form ausgetauscht. Öffentliche Stellen streben eine interaktive Kommunikation untereinander, mit den Bürgern und der Wirtschaft an, um z. B. die Auskunftserteilung, die Bearbeitung und Versendung von Verwaltungsvorgängen und die Kommunikation untereinander einfacher und kostengünstiger über das Internet durchführen zu können.

Der bisher geübte, meist ungesicherte E-Mail-Austausch wird durch die Einführung von elektronischen Signaturen und Verschlüsselungen sicherer und rechtsverbindlicher; leider aber auch komplizierter und technisch aufwendiger. Solche Verfahren ermöglichen aber die Sicherstellung der Vertraulichkeit der Daten durch deren Verschlüsselung sowie den Nachweis der Integrität der Daten und der Überprüfung ihres Urhebers.

Um eine sichere Übertragung insbesondere personenbezogener Daten zu gewährleisten, wurde in der Bundesverwaltung unter Führung des Bundesministeriums des Innern und fachlicher Unterstützung durch das Bundesamt für Sicherheit in der Informationstechnik – unter anderem auch mein Haus – mit einer Signier- und Verschlüsselungssoftware aus der Produktfamilie „SPHINX" ausgestattet.

SPHINX soll im Rahmen einer Verschlüsselung/Signatur Ende-zu-Ende-Sicherheit vom Sender bis zum Empfänger sicherstellen. Die Ver- bzw. Entschlüsselung einer E-Mail erfolgt ausschließlich in den Rechnern der E-Mail-Partner. Diese Ende-zu-Ende-Verschlüsselung bietet einen größtmöglichen Schutz der Nachrichten vor externen Eingriffen. Ein Schutz vor Viren und ähnlichen Risiken in einer E-Mail ist jedoch nur dann gewährleistet, wenn entsprechende Schutzmaßnahmen auf den beteiligten Computern installiert sind. In den zentralen Sicherheitssystemen – wie Firewall oder Virenscanner – kann eine verschlüsselte E-Mail nicht geprüft werden.

Die Planungen gehen derzeit dahin, in der Bundesverwaltung die elektronische Signatur und die Verschlüsselung für E-Mail und schutzwürdige Dateien in breitem Umfang unter Nutzung der genannten Produktfamilie einzuführen. Als Zertifizierungsdiensteanbieter wird das Trust-Center der Deutschen Telekom AG (Telesec) genutzt.

Die derzeitigen Anwendungsmöglichkeiten zeigen jedoch, dass die flächendeckende Einführung noch auf sich warten lassen muss, da der Nutzerkreis noch sehr eingeschränkt ist. Eine beschleunigte Verbreiterung innerhalb der Behörden – nicht nur der Bundesverwaltung – wäre wünschenswert, zumal verschiedene Behörden auf andere Verschlüsselungssoftware setzen, um eine datenschutzgerechte Kommunikation sicherzustellen.

33.7 Dienstanweisung E-Mail – Vertretungsregelung bei privater Nutzung

Wie auch schon in meinem 18. TB (Nr. 33.4.2) berichtet, werden die Möglichkeiten der elektronischen Datenübermittlung auch in meiner Dienststelle immer stärker genutzt. Der Schwerpunkt der Korrespondenz liegt zwar noch bei der „guten alten" Briefpost und beim Fax, allerdings geht der Trend heute unübersehbar zum elektronischen Dokumentenaustausch (E-Mail). Dies nicht allein aus wirtschaftlichen Überlegungen, sondern auch weil E-Mail die Übermittlung und weitere Bearbeitung von Dokumenten vereinfacht und die kurzen Laufzeiten der Nachrichten die Arbeit effektiver machen – dies sowohl innerhalb der Dienststelle als auch mit externen Kommunikationspartnern. Für den Umgang und den Geschäftsgang innerhalb meiner Dienststelle habe ich eine „Dienstanweisung E-Mail" erlassen (Abdruck s. 18. TB Anlage 28).

In Diskussion geriet seit dem In-Kraft-Treten dieser Dienstanweisung die Vertretungsregelung bei Abwesenheit eines Beschäftigten. Dadurch, dass die private Nutzung in eingeschränktem Umfang erlaubt ist, bestand bei der bisher favorisierten Regelung die Gefahr, dass durch die automatische Weiterleitung auch private Zusendungen von Kollegen zur Kenntnis genommen werden konnten. Im Zuge der Überarbeitung der „Dienstanweisung E-Mail" habe ich nunmehr folgende Regelung in Kraft gesetzt: Durch eine automatische Antwort, die durch den Abwesenheitsassistenten aktiviert wird, kann der Absender einer E-Mail aufgefordert werden, die Mitteilung erneut zu senden und an das angegebene Referatspostfach zu adressieren. Alternativ kann auch die bisherige Weiterleitungsfunktion genutzt werden, wenn der betreffende Nutzer dies so wünscht. Wenn der Nutzer keine Regelung im Abwesenheitsassistenten generieren kann, z. B. bei unvorhersehbarer längerer Abwesenheit, richtet der Systemadministrator für den PC des Abwesenden ein neues Passwort ein, mit dessen Hilfe der Vertreter des Abwesenden in Anwesenheit des Systemadministrators oder eines weiteren Angehörigen des betreffenden Referats das elektronische Postfach auf dienstliche Einsendungen hin

sichtet und im Abwesenheitsassistenten die Regel zur automatisierten Antwort an den Einsender hinterlegt. Danach wird der PC herunter gefahren, vom Systemadministrator mit einem neuen Passwort versehen und somit bis zur Rückkehr des Nutzers für den Zugang gesperrt.

Der geänderten „Dienstanweisung E-Mail“ hat die Personalvertretung zugestimmt. Sie wird auch in Zukunft immer wieder überarbeitet werden, wenn technische Entwicklungen, aber auch praktische Erfordernisse dies notwendig machen.

33.8 Neuerungen aus der Informationstechnik

– Umstellung auf ein modernes Netzwerk

In meiner Dienststelle wurde im Mai 2002 das Netzwerk auf eine neue Plattform gestellt. Das bisherige ATM-Netzwerk entsprach nicht mehr den heutigen Anforderungen an schnelle und wartungsarme Netzwerke auf der Grundlage des Internetprotokolls (IP). Neben den hohen jährlichen Wartungskosten trat beim ATM-Netzwerk der unangenehme Nebeneffekt auf, dass keine Unterstützung im Bereich von Netzwerkkarten mehr stattfand. Durch die Rückzahlung der nicht verbrauchten Wartungsleistungen wurden die Anschaffungskosten für die neuen aktiven Netzkomponenten (IP-Switche) abgedeckt; gleichzeitig wurden in den Arbeitsplatzrechnern preiswerte Netzwerkkarten eingesetzt. Die neuen Netzwerkkomponenten sind vollkommen wartungsfrei und bilden nunmehr die Basis für ein 100 Mb/s Netz; den Backbone bildet ein Gigabit-Netzwerk.

– Neuanschaffung der Server und Einsatz von freier und offener Software

Ende 2002 erfolgte die Umrüstung fast aller Server auf Open-Source-Software (s. hierzu Nr. 4.4 und zur Definition von Open-Source-Software mit den dazugehörenden Lizenzbedingungen Nr. 8.8 im 18. TB). Die Umstellung wurde in mehreren Schritten vorgenommen. Nach der Lieferung im November 2002 wurden die Systeme zunächst grundkonfiguriert. Bisher wurde zur Datenhaltung der Benutzerdaten ein Novell-File-Server eingesetzt. Dieser Server wurde durch einen gedoppelten Server ersetzt, der auch die Anmeldedienste übernimmt. Konkret kommen hier Samba und OpenLDAP unter Linux (SuSE Enterprise) zum Einsatz. Die Kopplung der Systeme wird durch Heartbeat überwacht und die Daten werden über drbd (Distributed Replicated Block Device) gespeichert. Damit wird das alte System durch ein hochausfallsicheres System ersetzt.

Ein weiteres ausfallsicheres System wird als Intranet-Web-Server eingesetzt. Auf diesem System werden auch die Netzwerkbasisdienste DHCP und DNS bereitgestellt. Die Systeme sind seitens der Technik mit den oben genannten identisch.

Für den Aufbau der Internetservices im Rahmen von BundOnline 2005 ist ein weiteres System vorgesehen. Künftig soll das Internetangebot des BfD auf diesem System zur Verfügung gestellt werden.

Der Server für das Dokumentenmanagementsystem wird voraussichtlich erst 2003 umgestellt; die Ablösung des (kleinen) Systems für den Virenschutz der Clients ist noch offen (s. Abbildung 8).

Für 2003 plane ich – zunächst probeweise – den Einsatz von Open-Source-Clients unter Linux. Die zum Einsatz kommende Software soll hauptsächlich unter der GNU General Public License stehen oder zumindest an diese angelehnt sein. So wird z. B. an KDE als Benutzeroberfläche gedacht; als Office-System soll OpenOffice und zum Surfen im Internet Mozilla genutzt werden. K-Mail soll mit Sphinx-Zusatz als Mail-Client dienen, Kroupware soll als Ersatz der derzeitigen Nutzerumgebung des Personal Information Manager mit Kolab als Serverkomponente eingesetzt werden.

Ausschlaggebende Überlegungen für die Migration sind Kostenvorteile, Sicherheitsaspekte und die strategische Ausrichtung der Bundesregierung zur Open-Source-Software hin. Auch hinsichtlich Verfügbarkeit und leichterer Wartung werden Vorteile gesehen. Ziel ist es, die einseitige Abhängigkeit von einzelnen Herstellern zu lösen. Der Einsatz von Open-Source-Software wird durch Beschlüsse des Bundestags gefordert und vom BMI/Bundesamt für Sicherheit in der Informationstechnik gefördert. Die Ablösung der Server war notwendig, da die Hardware z. T. älter als fünf Jahre war und die Software nicht mehr unterstützt wurde.

Ein erhöhter Schulungsaufwand im Serverbereich ist nicht zu befürchten, da – wie in vielen Unternehmen und Behörden – Unix/Linux Kenntnisse vorhanden sind. Bei den Anwenderinnen und Anwendern müssen umfangreiche Schulungsmaßnahmen durchgeführt werden. Allerdings ist eine Neuschulung auch bei proprietärer Software notwendig, da sich dort die neuen Produkte erheblich von den heute eingesetzten (alten) Produkten unterscheiden.

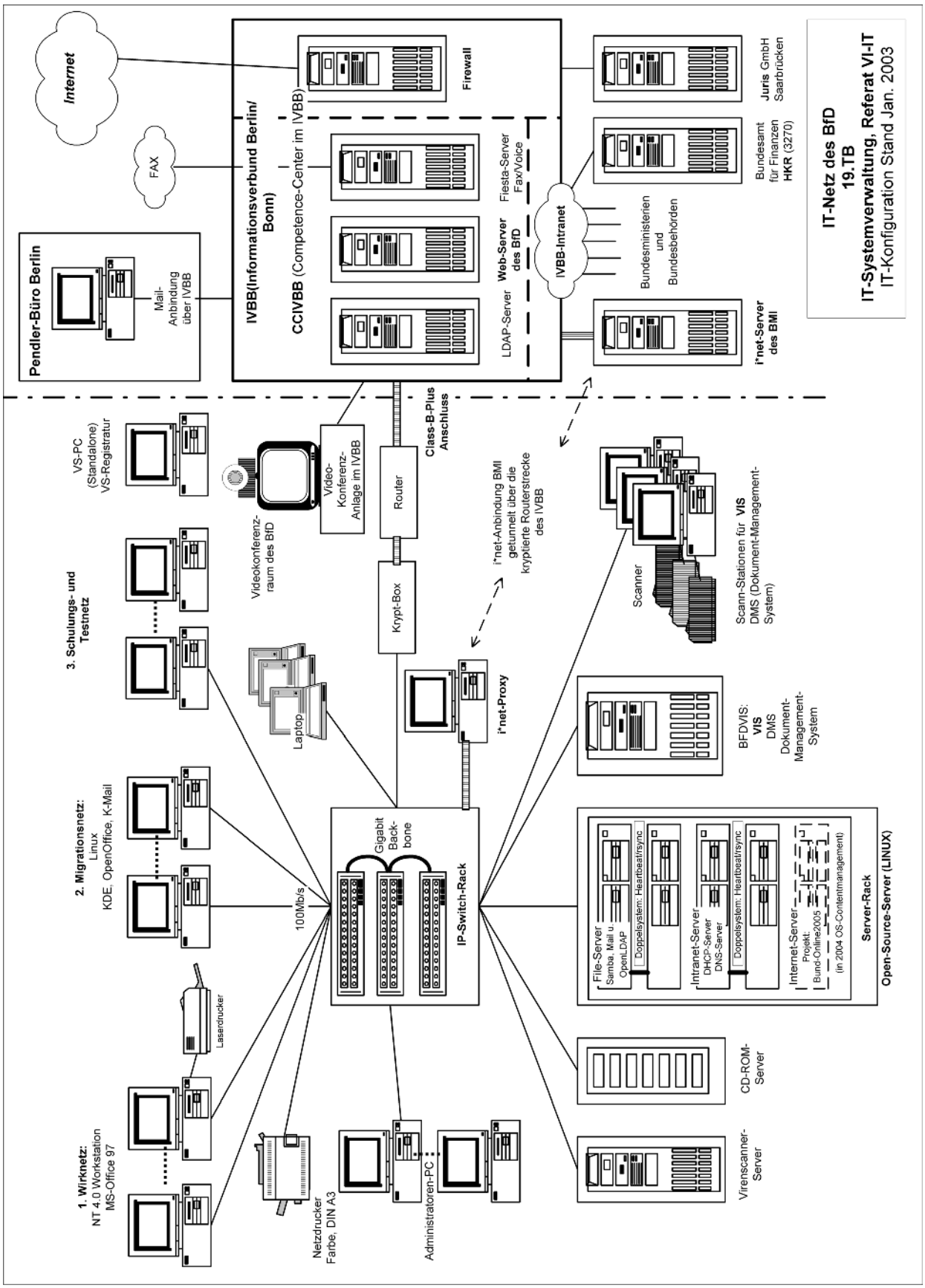
Für den Datenschutz sehe ich beim Einsatz von offener und freier Software einige Vorteile gegenüber proprietären Produkten; z. B. gibt es keinen „Zwang“ zur Personalisierung von Softwareprodukten. Die Transparenz der Software ist durch die Quellcodeoffenheit immer gegeben. Auch Probleme durch Marktveränderungen haben keine Auswirkungen mehr auf die Softwarelinie des BfD. Es ist damit eine gezielte Unterstützung bei der Weiterentwicklung des Datenschutzes zum erstenmal überhaupt möglich (z. B. Datenvermeidung, Datensparsamkeit, prüfbare Sicherheit bei Verfahren zur Pseudonymisierung, Authentisierung usw.).

33.9 Fortentwicklung der elektronischen Aktenführung

In meinem 18. TB (Nr. 33.4.1) habe ich von der Einführung der elektronischen Akte in meiner Dienststelle berichtet. Nach entsprechenden Vorbereitungsarbeiten im Laufe des Jahres 2000 konnte 2001 die flächendeckende Einführung begonnen und bis Ende des Jahres zügig abgeschlossen werden. Mit der Zielvorgabe, ein vollständig nach dem DOMEA-Konzept ausgerichtetes Verfahren in zwei Phasen zu implementieren, sollten die bei der Einführung eines Dokumentenmanagementsystems zu erwartenden Auswirkungen auf bisher gewohnte Arbeitsweisen zu keiner Beeinträchtigung der Arbeitsfähigkeit des Hauses führen, was im wesentlichen auch gelungen ist. Die im Vorfeld der Einführung von mir getroffene Entscheidung, das System entsprechend dem DOMEA-Stufenkonzept zunächst lediglich zum Aufbau eines elektronischen Aktenarchivs zu nutzen, hat sich rückblickend als richtig erwiesen und trug zu einer akzeptanzfördernden Arbeitsweise bei. Diese Vorgehensweise bietet den Vorteil, dass für alle Arbeitsbereiche vorerst weiterhin die gewohnte papiergebundene Bearbeitung erhalten

Abbildung 8 (zu Nr. 33.8)

BfD-Netz mit 107 IT-Arbeitsplätzen



bleibt; daneben wird aber durch den Aufbau der elektronischen Aktenablage die Möglichkeit geschaffen, von allen Arbeitsplätzen des Hauses aus auf alle aktenrelevanten Dokumente zuzugreifen. Die erhofften Zugewinne, wie verbesserte Informationsgewinnung durch den Bearbeiter unter gleichzeitiger Entlastung der Registratoren bei der Informationsbeschaffung und -aufbereitung, konnten erzielt werden.

Zugleich wurde der Personalrat zur Wahrung der berechtigten Interessen meiner Mitarbeiter und Mitarbeiterinnen frühzeitig in das Vorhaben einbezogen. Die datenschutzrechtliche Bedeutung des automatisierten Vorgangsbearbeitungssystems besteht darin, dass die elektronische Akte jeden Beitrag eines Bearbeiters ausweist und dies nach beinahe jedem beliebigen Kriterium auswertbar ist. Die elektronische Akte wäre deshalb für eine weitgehend lückenlose Leistungskontrolle geeignet, die weit über das hinausginge, was rechtlich und auch unter dem Aspekt moderner Personalführung akzeptabel wäre. Ein solches System kann nur mit Zustimmung des Personal- bzw. Betriebsrates eingeführt werden. Es wurden Vereinbarungen getroffen, wie mit diesen Daten und mit den Daten aus eventuellen Protokollierungen einzelner Arbeitsschritte umzugehen ist. Die im Vorfeld geäußerten Bedenken konnten hierdurch restlos ausgeräumt werden. Nach den bisherigen Erfahrungen gab und gibt es bei den Beschäftigten keine Veranlassung zu Misstrauen.

Über den Fortgang des Projekts werde ich auch künftig berichten.

34 Am Schluss noch einiges Wichtige aus zurückliegenden Tätigkeitsberichten

1. Über die Problematik **ausländerrechtlicher Vermerke in ausländischen Pässen** mithilfe von Kontrollstempeln habe ich in meinem 18. TB (Nr. 5.1.3) berichtet. In diesem Zusammenhang hatte ich angeregt, für die Vermerke „Ausgewiesen“ und „Abgeschoben“ im Ausländergesetz selbst eine Rechtsgrundlage zu schaffen. Dem ist das BMI nicht gefolgt. Es hatte lediglich in dem Entwurf einer Verordnung zur Durchführung des Zuwanderungsgesetzes in § 56 Nr. 8 eine Reglung vorgesehen, nach dem der Ausländer verpflichtet ist, „seinen Pass oder Passersatz zur Anbringung von Vermerken über Ort und Zeit der Ein- und Ausreise, des Antreffens im Bundesgebiet sowie über Maßnahmen und Entscheidungen nach dem Aufenthaltsgesetz in seinem Pass oder Passersatz durch die Ausländerbehörden oder die Polizeivollzugsbehörden des Bundes oder der Länder sowie die sonstigen mit der polizeilichen Kontrolle des grenzüberschreitenden Verkehrs beauftragten Behörden auf Verlangen vorzulegen“. Offen geblieben ist bislang noch das Ergebnis der vom BMI im Zusammenwirken mit dem AA zugesagten Prüfung der Frage, ob die deutsche Vorgehensweise den internationalen Gepflogenheiten entspricht. Nachdem das Bundesverfassungsgericht das Zuwanderungsgesetz für nichtig erklärt hat, werde ich in den anstehenden Erörterungen für ein neues Zuwanderungsgesetz versuchen nunmehr eine gesetzliche Regelung für das Problem „Kontrollstempel“ zu erreichen. Ich werde über das Ergebnis meiner Bemühungen erneut berichten.

2. Im November 1999 hatte sich die Ständige Konferenz der Innenminister und -senatoren der Länder (IMK) für einen Pilotversuch auf der Basis der „**Machbarkeitsstudie zum Einsatz einer Smart-Card im Asylverfahren**“ ausgesprochen (s. 18. TB Nr. 34.1). Dabei nahm das BMI als Rahmenbedingung an, dass bei Verzicht auf die Schaffung einer gesetzlichen Grundlage eine Karte nur auf freiwilliger Basis durch Einverständniserklärung des Asylbewerbers ausgegeben werden könne. Wie mich das BMI inzwischen informiert hat, habe sich aber nach Erörterungen mit den Ländern gezeigt, dass der Pilotversuch aus fachlichen Gründen so nicht umgesetzt werden konnte. Es habe daher im Mai 2000 eine geänderte Konzeption mit einem von der Bundesdruckerei entworfenen Muster der Asylcard zur Diskussion gestellt. Zu einem erneuten IMK-Beschluss ist es nicht gekommen. Das Terrorismusbekämpfungsgesetz (Aufenthaltsgestattung und Duldung dokumentiert durch einen selbstständigen fälschungssicheren Ausweis) und das Zuwanderungsgesetz (Speicherung der Nummern von Aufenthaltgestattungen im Ausländerzentralregister bzw. der Visadatei im Ausländerzentralregister) beschreiten inzwischen andere Wege. Die Asylcard ist aber nach Auskunft des BMI weiterhin Gegenstand von Diskussionen im Zusammenhang mit dem Einsatz biometrischer Daten. Ich werde die weitere Entwicklung sorgsam beobachten und sodann erneut berichten.

3. Über die datenschutzrechtlichen Probleme beim **Einsatz ausländischen Liaisonpersonals im Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl)** habe ich zuletzt in meinem 18. TB (Nr. 34.3) berichtet. Inzwischen hat mich das BMI darüber informiert, dass es derzeit, bedingt durch eine Schwerpunktverlagerung bei der Tätigkeit des ausländischen Liaisonpersonals, kein zwingendes Erfordernis mehr sieht, an der beabsichtigten Doppelfunktion dieses Personenkreises festzuhalten. Das BMI hat daher das BAFl gebeten, von der seinerzeit beabsichtigten Doppelfunktion beim Einsatz des ausländischen Liaisonpersonals Abstand zu nehmen. Ich betrachte die Angelegenheit damit als erledigt.

4. Nachdem die zuständigen europäischen Gremien, wie ich in meinem 18. TB (Nr. 5.2.1) berichtet habe, gegen einen Zugriff des Bundesamtes für die Anerkennung ausländischer Flüchtlinge (BAFl) auf das Schengener Informationssystem (SIS) keine Bedenken erhoben hatten, hat das BAFl seit Juli 2000 versuchsweise einen lesenden Direktzugriff im Dialogverfahren auf den beim Bundesverwaltungsamt geführten Datenbestand nach Artikel 96 SDÜ erhalten. Die Dauer des Probebetriebs war auf neun Monate beschränkt und endete am 31. März 2001. In seinem Abschlussbericht über die Erfahrungen des Probebetriebs hat mir das BMI mitgeteilt, dass der Direktzugriff auf das SIS in vielen Fällen ein wichtiges Hilfsmittel für die Feststellung der Zuständigkeit eines anderen Mitgliedstaates war. So hat das BAFl in 88 % der erzielten Treffer ein Übernahmeersuchen an den jeweiligen Mitgliedsstaat gestellt. Aufgrund der erzielten Treffer hat sich das BMI für eine Fortführung des Direktzugriffs des BAFl auf den Datenbestand des Artikel 96 des Schengener

Durchführungsübereinkommens ausgesprochen. Auch ich habe gegen die Fortsetzung des Verfahrens über die am 31. März 2001 ausgelaufene Probephase hinaus keine Einwendungen erhoben. Ich gehe dabei jedoch davon aus, dass der Zugriff auf das SIS nur bis zu der Aufnahme des Wirkbetriebs des Systems Eurodac (s. u. 7.1.1) erforderlich ist.

5. In meinem 18.TB (Nr. 5.1.4) habe ich über **Anfragen stellvertretender Behörden an das Ausländerzentralregister** berichtet. Ich habe mich, um den Belangen der Praxis gerecht zu werden, seinerzeit bereit erklärt, meine Bedenken gegen diese Verfahrensweise zurückzustellen, wenn zwischen Bund und Ländern entsprechende Vereinbarungen über die Behandlung dieser Stellvertreteranfragen getroffen werden. Das BMI hat mir inzwischen einen mit der Registerbehörde abgestimmten Vorschlag zugeleitet, dem ich zugestimmt habe. Er sieht vor, dass Vertreterabfragen bei Dienststellen innerhalb der gleichen Behördengruppe künftig nur dann hinzunehmen sind, wenn die anfragende Stelle durch Auswertung der Protokolldatei der Registerbehörde erkennbar ist. Um dies sicherzustellen, wird eine entsprechende Vereinbarung mit den Innenministern/-senatoren der Länder angestrebt, die bei Redaktionsschluss noch nicht vorlag. Ich werde erneut berichten.

6. Aufgrund einer mir von der Präsidentin des Europäischen Parlaments im Jahre 1999 übermittelten Petition habe ich die Frage geprüft, 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 verstößt. Ich bin zu dem Schluss gelangt, dass eine solche Speicherung lediglich im Einzelfall erforderlich sein kann, dass aber eine systematische Erfassung aller in Deutschland wohnenden Staatsangehörigen aus EU-Staaten nicht gerechtfertigt ist. Das BMI hat seinerzeit mitgeteilt, es prüfe, ob eine entsprechende Änderung des AZR-Gesetzes in das Zuwanderungsgesetz aufgenommen werden soll. Dazu ist es nicht gekommen. Ich bin der Ansicht, dass diese Problematik in der laufenden Legislaturperiode erneut diskutiert werden muss.

7. Die in der Wendezeit unter nicht geklärten Umständen in den Besitz der USA geratenen so genannten **Rosenholz-Unterlagen** mit Angaben über die Westagenten des Ministeriums für Staatssicherheit (s. 18. TB Nr. 5.8.2) sind im Berichtszeitraum von den USA als duplizierte CD-ROM der Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes weitgehend übergeben worden. Diese hat mir mitgeteilt, dass sie bisher 307 CD-ROM erhalten hat und noch 65 CD-ROM erwartet. Die von einigen Medien erwartete spektakuläre Enttarnung weiterer West-Agenten der Stasi ist bisher nicht eingetreten. Dies wohl auch deshalb, weil die Strafverfolgungsorgane im Rahmen der Rechtshilfe auch schon vorher Zugriffsmöglichkeiten auf diese Unterlagen hatten.

8. In meinem 18. TB (Nr. 6.8) habe ich ausführlich über die seinerzeit rege geführte öffentliche Diskussion zum Thema **„Elektronische Fußfessel“** berichtet. Dabei habe ich auf einen Gesetzesentwurf des Bundesrates (Bundestagsdrucksache 14/1519) hingewiesen, der vorsah, den Ländern durch eine Änderung des Strafvollzugsgesetzes befristet die Möglichkeit einzuräumen, Regelungen über die Einführung und Ausgestaltung eines elektronisch überwachten Hausarrestes zu schaffen. Hierzu habe ich die Auffassung vertreten, dass aus datenschutzrechtlicher Sicht keine grundsätzlichen Bedenken gegen die probeweise Einführung dieses Instrumentes bestünden, vielmehr die konkrete Ausgestaltung des Verfahrens entscheidend sei. Da der Entwurf im Parlament nicht weiter beraten wurde, war eine vertiefte Befassung mit diesem Thema für mich bisher nicht erforderlich. Ob es in diesem Bereich eine neue Gesetzesinitiative geben wird, bleibt abzuwarten. Ich werde mich in diesem Fall – wie bereits im 18. TB angekündigt – für eine die Persönlichkeitsrechte aller Betroffenen wahrende Regelung einsetzen und weiter über die Angelegenheit berichten.

9. Über die Praxis der Datenerhebung und Recherche im Zusammenhang mit der **Verleihung des Verdienstordens der Bundesrepublik Deutschland** habe ich zuletzt in meinem 18. TB (Nr. 34, dort Nr. 5) berichtet. Um eine Datenbeschaffung auf Vorrat durch die parallele Prüfung von „Verdiensten“ und „Würdigkeit“ zu unterbinden, habe ich dem BMI geraten, in Absprache mit dem Bundespräsidialamt und den Ländern eine abgestimmte und verbindliche Verfahrensregelung zu dem von mir vorgeschlagenen so genannten Zwei-Stufen Modell zu treffen. Danach werden zunächst die Verdienste des Auszuzeichnenden abschließend geprüft und erst bei einem positiven Ergebnis (die Verdienste reichen für eine Auszeichnung aus) die Ordenswürdigkeit. Dieses Modell wurde zwischenzeitlich von allen Ländern, mit Ausnahme von Sachsen und Thüringen, erprobt, wobei die Länder, die dem Bundespräsidenten die meisten Ordensvorschläge unterbreiten, ihre Prüfungen ohnehin schon vorher entsprechend dem so genannten Zwei-Stufen-Modell durchgeführt haben. Nach den bisherigen Erfahrungen der Länder hat sich dieses Modell bewährt und soll nunmehr auf Dauer umgesetzt werden. Die Länder Sachsen und Thüringen haben zugesagt, ihr Verfahren aufgrund der positiven Erfahrungen der anderen Länder nochmals zu überprüfen.

   Ich werde die Entwicklung weiterverfolgen. Ob auch vor dem Hintergrund der zweiten Stufe der Novellierung des Datenschutzrechts eine bereichsspezifische Regelung für das Ordensrecht erforderlich ist, wird zu gegebener Zeit zu entscheiden sein.

10. In meinem 18. TB (Nr .34, dort Nr.6) habe ich ausgeführt, dass sich der Erlass der **Steuerdaten-Abruf-Verordnung** (StDAV) nach Mitteilung des BMF weiterhin verzögert, da aufgrund eingegangener Stellungnahmen der Länder und Gemeinden eine Überarbeitung des Entwurfs erforderlich sei. Nach Auswertung der Stellungnahmen der Länder, Gemeinden, Verbände und anderer beteiligter Behörden wurden mir neue Entwürfe der StDAV zugesandt, die die wesentlichen datenschutzrechtlichen Aspekte berücksichtigen. Nach dem derzeitigen Sachstand gehe ich davon aus, dass die StDAV im Laufe des Jahres 2003 in Kraft treten wird.

11. Im 18. TB (Nr. 20.1) habe ich darüber berichtet, dass die **Musterprüfungsverfügung**, auf der die Prüfungsverfügungen der Arbeits- und Hauptzollämter beruhen, falls diese **Außenprüfungen** zur Aufdeckung von Leistungsmissbrauch – ausnahmsweise – ankündigen, den rechtstaatlichen Erfordernissen nicht entsprach. Insbesondere muss aus der Prüfungsverfügung für den Arbeitgeber erkennbar sein, welche Daten über seine Arbeitnehmer er an die prüfende Behörde übermitteln muss. Inzwischen konnte nach einem konstruktiven Dialog zwischen dem BMF, der Bundesanstalt für Arbeit und mir eine Musterprüfungsverfügung erarbeitet werden, die rechtstaatlichen Ansprüchen an die Bestimmtheit von Verwaltungsakten genügt.

12. Über die Notwendigkeit einer gesetzlichen Grundlage für die **Aufbewahrung von Akten und die Speicherung personenbezogener Daten in Dateien der Justiz** habe ich in den zurückliegenden Tätigkeitsberichten (18. TB Nr. 6, 17. TB Nr. 34, dort Nr. 7, und 16. TB Nr. 6.14) mehrfach berichtet und auf die Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom Frühjahr 1995 (16. TB Anlage 6) und vom Herbst 1999 (18. TB Anlage 16) hingewiesen. In der Zwischenzeit hat zwar eine Arbeitsgruppe der Konferenz der Justizministerinnen und -minister (Justizministerkonferenz) ebenfalls die Notwendigkeit bejaht, eine gesetzliche Regelung zu schaffen, sodass die 72. Justizministerkonferenz im Juni 2001 eine länderoffene Arbeitsgruppe beauftragt hat, einen Entwurf für ein Aufbewahrungsgesetz zu erarbeiten. Da zwischen den Justizministern des Bundes und der Länder aber Uneinigkeit über die Federführung besteht, hat diese Arbeitsgruppe ihre Arbeit bis heute noch nicht aufgenommen.

13. In meinem 18. TB (Nr. 34, dort Nr. 7) habe ich berichtet, dass hinsichtlich der Umsetzung der Verordnung (EG) Nr. 1469/95 des Rates vom 22. Juni 1995 über Vorkehrungen gegenüber bestimmten Begünstigten der vom Europäischen Ausrichtungs- und Garantiefond für die Landwirtschaft, Abteilung Garantie, finanzierten Maßnahmen, der so genannten „ **Schwarze-Liste-Verordnung**“, noch keine Einigung mit dem BMF in der Frage erzielt werden konnte, ob ein direkter Zugriff auf die Daten von Marktbeteiligten erforderlich ist, solange bei ihnen festgestellte Unregelmäßigkeiten nicht den Schwellenwert von 100 000 Euro überschritten haben. Insoweit konnte nunmehr eine abschließende Klärung erreicht werden. Aus Artikel 2 Abs. 1 der VO (EG) Nr. 745/96 der Kommission vom 24. April 1996 zur Durchführung der Verordnung Nr. 1469/95 i. V. m. Artikel 8 Abs. 1 der VO (EWG) Nr. 729/70 des Rates vom 21. April 1970 über die Finanzierung der gemeinsamen Agrarpolitik ergibt sich die Verpflichtung der Mitgliedsstaaten, Unregelmäßigkeiten vorzubeugen und zu verfolgen. Der zuständige Bearbeiter benötigt bereits vor Überschreiten des Schwellenwertes einen Überblick über den Sachstand, da ansonsten keine Möglichkeit gegeben ist, eventuellen Betrugspraktiken nachzugehen und finanziellen Schaden vom Gemeinschaftshaushalt abzuwenden. Rechtsgrundlage für die Aufnahme von Daten über Verdachtsfälle bilden Artikel 1 Abs. 1 der VO Nr. 1469/95 und Artikel 1 Abs. 2 der VO Nr. 745/96. Meine datenschutzrechtlichen Bedenken konnten somit ausgeräumt werden.

14. Über das **Scoring-Verfahren** der SCHUFA habe ich zuletzt in meinem 18. TB (Nr. 31.1.1, 31.1.2) berichtet und die bestehenden Probleme dargestellt.

    Ein Datenschutzproblem bei der Score-Wert Berechnung der SCHUFA konnte im Berichtszeitraum gelöst werden – die Einbeziehung der Selbstauskunft in den Score-Wert. Ein neues Verfahren, das die Selbstauskunft bei der Score-Berechnung nicht mehr berücksichtigt, steht den Vertragspartnern der SCHUFA seit Dezember 2001 zur Verfügung. Da – laut SCHUFA – bei vielen Vertragspartnern die Umstellung des hausinternen Verfahrens längere Zeit in Anspruch genommen hat, war zunächst noch eine Anpassungsphase notwendig. Mit Schreiben vom 4. September 2002 hat die SCHUFA die Datenschutzaufsichtsbehörden darüber informiert, dass die Selbstauskunft bei der Score-Berechnung ausnahmslos nicht mehr berücksichtigt würde.

    Hinsichtlich der Transparenz des Score-Wertes konnte seitens der Datenschutzaufsichtsbehörden leider noch immer kein befriedigendes Ergebnis erzielt werden. Die SCHUFA erklärt sich zwar mittlerweile bereit, den Betroffenen einen aktuellen Score-Wert mitzuteilen, ist aber noch immer nicht bereit, den an die Vertragspartner übermittelten Score-Wert bekannt zu geben. Nur letzterer Wert würde allerdings Transparenz für den Betroffenen bringen, da der Score-Wert kein statischer Wert ist, vielmehr sich fortlaufend ändern kann. Die SCHUFA begründet ihr Verhalten damit, dass sie selber den Wert nicht speichere und eine entsprechende Änderung der genutzten Software mit dem Ziel, den Score-Wert zu speichern, mit einem wirtschaftlich vertretbaren Aufwand nicht möglich sei. Frühestens Ende 2003/Anfang 2004 würde es eine neue Software-Generation erlauben, den übermittelten Score-Wert zu speichern und den Betroffenen mitzuteilen. Einer noch weitergehenden Forderung der Aufsichtsbehörden, den Betroffenen nicht nur den Score-Wert selbst, sondern auch die Parameter und deren Gewichtung bekannt zu geben, wird seitens der SCHUFA nach wie vor mit der Begründung der Wahrung des Geschäftgeheimnisses abgelehnt.

    Aus Anlass meines 18. Tätigkeitsberichtes hat der Deutsche Bundestag die Bundesregierung aufgefordert, eine gesetzliche Verpflichtung aller Auskunfteien zur Mitteilung der von ihnen erstellten Score-Werte, der zugrunde liegenden Parameter und ihrer Gewichtung an die jeweils Betroffenen zu prüfen. Ich hoffe, dass die Bundesregierung diesem Prüfauftrag alsbald nachkommt, damit der inakzeptable Zustand, dass dem Betroffenen selbst verschlossen bleibt, was bei Kreditinstituten etc. zur Entscheidungsgrundlage für eine kreditorische Leistung an ihn gemacht wird, bald ein Ende findet.

15. In meinem 18. TB (Nr. 31.5) habe ich ausführlich über das Konzept des Deutschen Pressera tes berichtet, im Rahmen des § 41 Abs. 1 BDSG durch Selbstregulierung und Selbstkontrolle einen wirksamen Datenschutz bei der redaktionellen Datenverarbeitung sicherzustellen.

Dieses Konzept ist im Berichtszeitraum weiter umgesetzt worden. Im November 2001 wurde der neue Pressekodex, der um eine Reihe von datenschutzrechtlichen Regelungen erweitert worden war , offiziell dem Bundespräsidenten überreicht und der Öffentlichkeit vorgestellt; der gesonderte Beschwerdeausschuss des Deutschen Presserates für Fragen des redaktionellen Datenschutzes hat im März 2002 seine Arbeit aufgenommen und schon eine Reihe von Fällen zu behandeln gehabt. Eine Vielzahl von Presseverlagen hat inzwischen die erforderlichen Selbstverpflichtungserklärungen abgegeben. Der Deutsche Presserat wird entsprechend seinen Statuten regelmäßig alle zw ei Jahre einen Tätigkeitsbericht zum **Redaktionsdatenschutz** veröffentlichen, der auch eine Darstellung der wesentlichen Entwicklung des Redaktionsdatenschutzes in der Presse enthalten soll.

In mehreren Gesprächen habe ich mich davon überzeugen können, dass es dem Deutschen Presserat mit der Sicherstellung eines wirksamen Redaktionsdatenschutzes ernst ist.

Die weitere Entwicklung werde ich aufmerksam verfolgen.

16. In meinem 18. TB (Nr. 31.8) habe ich über die Absicht der Bundesregierung berichtet, den Rechtsrahmen für das **private Sicherheitsgewerbe** neu zu regeln und in diesem Zusammenhang auch den datenschutzrechtlichen Aspekten der Tätigkeit Rechnung zu tragen. Das Gesetz zur Änderung des Bewachungsgewerberechts vom 23. Juli 2002 (BGBl. I S. 2724) sieht nunmehr in § 8 Bewachungsverordnung vor, dass die V orschriften des ersten und dritten Abschnitts des BDSG auch Anwendung finden, wenn der Gewerbetreibende in Ausübung seines Gewerbes Daten über Dritte verarbeitet, nutzt oder dafür erhebt und dies weder unter Einsatz von Datenverarbeitungsanlagen noch in oder aus nicht automatisierten Dateien erfolgt. Die Regelung geht auf eine Anregung von mir im Gesetzgebungsverfahren zurück. Sie führt dazu, dass nunmehr auch der dritte Abschnitt des BDSG für das private Sicherheitsgewerbe gilt, sofern personenbezogene Datenverarbeitung in nichtstrukturierten Akten und Aktensammlungen stattfindet. Ich halte die uneingeschränkte Anwendung dieser Vorschriften für geboten, weil personenbezogene Daten Dritter durch Unternehmen des privaten Sicherheitsgewerbes nach meiner Kenntnis häufig in Akten verarbeitet und genutzt werden. Gleichzeitig geraten im Rahmen der Tätigkeit privater Sicherheitsdienste nicht nur bescholtene, sondern auch unbeteiligte Bür ger in größerem Umfang in deren V isier, als dies im Zusammenhang mit der Tätigkeit anderer nicht öf fentlicher Stellen der Fall ist. Die Re gelung trägt auch dem Umstand Rechnung, dass zunehmend das private Sicherheitsgewerbe mit den Polizeibehörden der Länder im Rahmen von so genannten Sicherheitspartnerschaften zusammenarbeitet und sich hieraus auch neue datenschutzrechtliche Anforderungen ergeben.

17. Auch die **Regulierungsbehörde für Telekommunikation und Post** (RegTP) hat die Aufgabe, die Einhaltung der datenschutzrechtlichen Vorschriften des Telekommunikationsgesetzes sicherzustellen (s. 17. TB Nr . 10.1.7). Wie bereits früher berichtet, ist es deshalb notwendig, eng mit der RegTP zusammenzuarbeiten (s. 18. TB Nr. 10.15).

    Die Zusammenarbeit wurde au ch in den ver gangenen zwei Jahren weitergeführt und erfolgt u. a. im Rahmen eines regelmäßig stattfindenden Jour Fixe. Dadurch wird erreicht, dass die Auslegung der einschlägigen Vorschriften und die sich daraus er gebenden datenschutzrechtlichen Forderungen an die Telekommunikationsunternehmen übereinstimmend erfolgt. Auch im Rahmen der Bearbeitung von Bür gereingaben kann es notwendig sein, sich über Einzelfälle auszutauschen. Im Berichtszeitraum bestand für einen Mitarbeiter meines Hauses die Möglichkeit einer informellen Beteiligung an einer Kontrolle der Regulierungsbehörde.

18. In meinem 18. TB (Nr. 24.1.1) habe ich über die Entwürfe eines **Pflege-Qualitätssicherungsgesetz**es und eines Dritten Gesetzes zur **Änderung des Heimgesetzes** berichtet. In den parlamentarischen Beratungen sind die von mir bei der V orbereitung beider Gesetzentwürfe gegebenen Hinweise zum Datenschutz sowie weitere V orschläge während dieser Beratungen aufgegriffen worden. Beide Gesetze sind am 1. Januar 2002 (BGBl. I 2001 S. 2320; BGBl. I 2001 S. 2960) in Kraft getreten.

19. In meinem 18. TB (Nr. 29.2) habe ich angekündigt, die seit der Liberalisierung des Postmarktes zum 1. Januar 1998 gegründeten **neue**n **Postdienstunternehmen** weiter intensiv zu kontrollieren und zu beraten, um auf die Einhaltung des Datenschutzes hinzuwirken. Die Zahl der Unternehmen ist in den letzten beiden Jahren weiter gewachsen, wobei jedoch immer wieder Unternehmen mangels Konkurrenzfähigkeit ihre Tätigkeit vollständig einstellen mussten. Meine Kontrollen haben ein insgesamt sehr erfreuliches Ergebnis erbracht. In keinem Fall wurde der Datenschutz grob missachtet. Lediglich geringere Verstöße (wie z. B. fehlerhafte Benachrichtigungen bei Nichtantreffen eines Empfängers, nicht hinreichende Aufklärung innerhalb der Unternehmen bzw. bei Subunternehmen zum Thema Daten- und Postgeheimnis) waren zu bemängeln. Sie wurden jeweils nach meinen Besuchen bei den Unternehmen abgestellt. Die Unternehmen haben meine Anregungen und Hinweise dankbar zur Kenntnis genommen. Der Datenschutz bei den neuen Unternehmen am Postmarkt erreicht damit ein erfreulich hohes Niveau, wozu sicher auch die T atsache beiträgt, dass viele der Unternehmen V erbänden angeschlossen sind, die Informationen auch zum Datenschutz an ihre Mitglieder weiter geben. Ich werde auch weiterhin intensiv Kontrollen und Beratungen neuer Postdienstunternehmen durchführen, um dem Datenschutzaspekt von vornherein die notwendige Geltung zu verschaffen.

20. In meinem 18. TB (Nr . 16.4) habe ich mich, nicht zuletzt vor dem Hintergrund mangelnder Transparenz, besorgt über das **Abhörsystem ECHELON** geäußert und die Initiative des Europäisch en Parlaments (EP), einen nichtständigen Ausschuss einzusetzen, begrüßt. Dabei kam es vor allem auf eine Überprüfung des in der Öffentlichkeit erweckten Ei ndrucks an, mit ECHELON werde in elementare Bür gerrechte eingegriffen. Der

Ausschuss hat unter dem 11. Juni 2001 seinen umfangreichen Bericht abgegeben. Das EP hat dazu in seiner Sitzung am 5. September 2001 eine Entschließung gefasst (ABl. C 72 E/221 vom 21. März 2002). Danach steht die Frage der Existenz von ECHELON nicht mehr in Zweifel. Ob tatsächlich Wirtschaftsspionage mit dem System betrieben wird, konnte durch den Ausschuss nicht nachgewiesen werden. Die Gerüchte hierzu sind allerdings nicht verstummt, die Bedenken nach wie vor nicht ausgeräumt. Denn eine wirklich objektive Bestandsaufnahme des Systems, wie ich sie in meinem 18. TB gefordert hatte, konnte nicht durchgeführt werden. Dies wäre möglicherweise anders gewesen, wenn nicht die USA die Unterstützung durch Abweisung der untersuchenden Parlamentarier in Washington boykottiert hätten.

Ich begrüße vor allem, dass das EP die Datenschutzprobleme in Verbindung mit ECHELON deutlich angesprochen hat. Besonders bedenklich ist, dass ECHELON keinerlei rechtsstaatlichen Vorbehalten, wie sie z. B. in Deutschland das Artikel 10-Gesetz enthält, unterliegt. Eine Kontrolle findet ebenfalls nicht statt. Vor dem Hintergrund, dass jedes Abhören von Kommunikation einen tief greifenden Eingriff in die Privatsphäre des Einzelnen darstellt, stimme ich den Erwägungen in der o. a. Entschließung zu. Vor allem ein gemeinsames Schutzniveau gegenüber nachrichtendienstlicher Tätigkeit in allen EU-Mitgliedsstaaten und die Schaffung der Voraussetzungen durch das EP für ein gemeinsames Kontrollorgan zur Überwachung und Kontrolle in diesem hoch sensiblen Bereich sollten unterstützt werden. Zu begrüßen ist auch die Forderung an die Europäische Kommission, den Rat und die Mitgliedsstaaten, eine „wirksame und effektive Politik betreffend die Sicherheit in der Informationsgesellschaft zu entwickeln und umzusetzen"; diese Politik soll auch die stärkere Sensibilisierung aller Nutzer moderner Kommunikationssysteme für die Notwendigkeit und die Möglichkeit des Schutzes vertraulicher Informationen beinhalten, z. B. durch Schaffung benutzerfreundlicher Krypto-Software. Eine erste Maßnahme ist der Appell an die europäischen Institutionen sowie an die öffentlichen Verwaltungen der Mitgliedsstaaten, Verschlüsselung von E-Mails systematisch einzusetzen, um so langfristig die Verschlüsselung zum Normalfall werden zu lassen.

Der Innenausschuss des Deutschen Bundestages hat in seiner Sitzung am 5. Juni 2002 die Entschließung zur Kenntnis genommen. Ich werde mit Interesse die weitere Entwicklung verfolgen.

21. Der Entwurf einer Entschließung des Rates über die operativen Anforderungen der Strafverfolgung in Bezug auf öffentliche Telekommunikationsnetze und -dienste, der in den vergangenen Jahren als **ENFOPOL 55** auch zu datenschutzrechtlichen Bedenken Anlass gegeben hatte (s. 18. TB Nr. 16.3 und Anlg. 11), ist im Berichtszeitraum beim Rat nicht weiter verfolgt worden. Im Vorgriff auf eine zu erwartende Entscheidung hat allerdings die Bundesregierung ihre Haltung zu diesem Entwurf präzisiert. Dazu zählt, was von mir unterstützt wird, dass im Text nicht einseitig auf die Interessen der Bedarfsträger abgestellt wird, sondern auch das Grundrecht auf informationelle Selbstbestimmung angemessen berücksichtigt werden soll. Es bleibt abzuwarten, ob das Projekt im Rat nochmals aufgegriffen wird und wie dann die revidierte deutsche Position, die datenschutzrechtliche Verbesserungen enthält, durchgesetzt werden kann.

22. In meinem 18. TB (Nr. 18.2) habe ich über den Entwurf des Gesetzes zur Neuordnung des **Bundesdisziplinarrechts** (BDiszNOG) (BGBl. I 2001 S. 1510) berichtet. Meine Anregung, die Löschungsvorschriften in § 90e Abs. 1 Nr. 2 BBG an die Neuregelung im BDiszNOG anzupassen, hat das BMI leider nicht aufgenommen. Ich werde diese Angelegenheit bei der Beratung des Entwurfs des nächsten Gesetzes zur Änderung beamtenrechtlicher Vorschriften erneut aufgreifen.

23. Das Pilotprojekt für das **Umzugskostenverfahren bei der Bundeswehr,** über das ich in meinem 18. TB berichtet habe, wurde zum 31. Oktober 2000 beendet. Die mir vom BMVg im Berichtszeitraum angekündigte Folgeregelung ist noch nicht erlassen worden. Bis zu dieser Regelung soll wie vor der Aufnahme des Pilotprojektes verfahren werden. Vom Umziehenden werden nur die nach dem Bundesumzugskostengesetz erforderlichen Daten erhoben.

24. In meinem 18. TB (Nr. 27) habe ich über meine datenschutzrechtlichen Bedenken zum Entwurf des Bundesministeriums für Familie, Senioren, Frauen und Jugend (BMFSFJ) für eine **Personalaktenverordnung für Zivildienstleistende** (ZDPersAV) berichtet. Das BMFSFJ hat diesen Bedenken nunmehr Rechnung getragen. Inzwischen wurde die ZDPersAV verabschiedet (BGBl. 2002 I S. 4025). Damit besteht ein weitgehend einheitliches Personalaktenrecht für Zivildienstleistende, Beamte, Soldaten und ungediente Wehrpflichtige.

25. Im Zusammenhang mit der Problematik der **Vernichtung von** personenbezogenen Daten in Personen- und Sachakten des BfV (s. o. Nr. 17.2) habe ich auch die Frage der **Sonderakten** (s. 16. TB Nr. 14.5) erneut aufgegriffen. Bis auf zwei Fälle, die als „zeitgeschichtlich bedeutsam" eingestuft wurden, sind nach Auskunft des BMI inzwischen die übrigen Personenakten als nicht mehr erforderlich für die Tätigkeit des BfV vernichtet worden.

26. Ich habe die **Deutsche Post AG** bereits in meinem 18. TB (Nr. 29.6) auf die Bedeutung einer eigenen Datenschutzseite für ihren Internetauftritt hingewiesen. Für den Nutzer wäre es eine willkommene Hilfe, wenn er bereits beim ersten „Betreten" des Internetangebotes der Deutschen Post AG auf umfassende Informationen zum Datenschutz hingewiesen würde. Eine gelungene Präsentation dieses Themas findet sich z. B. beim Internetmarktplatz eVITA, einem Geschäftsfeld der Deutschen Post AG.

Trotz mehrerer Erinnerungen sah sich die Deutsche Post AG bisher nicht in der Lage, meine Empfehlung umzusetzen. Bei Eingabe des Suchbegriffs „Datenschutz" in der Homepage der Deutschen Post AG öffnet sich zwar eine Liste mit Links zu verschiedenen Webseiten, die das Wort beinhalten, allerdings finden sich nur unter dem Stichwort „In Haus Service" tatsächlich einige wenige, allgemein gehaltene Informationen zu diesem Thema. Diese Informationen sind jedoch nicht

ausreichend. Bei „In Haus Service“ handelt es sich im Übrigen um einen Service der Deutschen Post AG für Unternehmen. Ausführungen zum Datenschutz im privaten Bereich finden sich auf der W ebseite nicht. Ein weiterer Link verweist in einer allgemein gehaltenen Information auf die Absicht der Bundesregierung, das Datenschutzrecht zwecks Harmonisierung mit dem europäischen Recht zu novellieren. Der Kunde der Deutschen Post AG erfährt darüber hinaus nichts Interessantes oder Hilfreiches zum Thema Datenschutz. Soweit mir bekannt ist, wurde inzwischen wenigstens mit vorbereitenden Arbeiten zu einer umfassenden Lösung dieses Problems für alle Gesc häftsfelder der Deutschen Post AG begonnen, sodass dieser Missstand hoffentlich bald beendet sein wird.

Ich werde darauf achten, dass die Deutsche Post AG die erforderlichen Maßnahmen nunmehr schnellstmöglich umsetzt und hierbei der besonderen Stellung des Datenschutzes durch einen direkten V erweis auf der ersten Seite der Homepage Rechnung trägt.

Anlage 1 (zu Nr. 1.15)

Hinweis für die Ausschüsse des Deutschen Bundestages

Nachfolgend habe ich dargestellt, welche Beiträge dieses Berichtes für welchen Ausschuss von besonderem Interesse sein könnten:

Ausschuss für Wahlordnung, Immunität und Geschäftsordnung	5
Auswärtiger Ausschuss	3.2.4; 3.6 bis 3.10; 6; 8.5; 32
Innenausschuss	1; 2; 3; 4; 7; 8.1 bis 8.9; 8.10.2; 10.5 bis 10.5.3; 10.6 bis 10.9; 11.3; 13; 14; 16; 17; 18; 19; 20; 21; 33.3; 33.6 bis 33.9; 34.1 bis 34.7; 34.9; 34.14; 34.15; 34.20; 34.21; 34.22; 34.25
Rechtsausschuss	1; 2; 4.2; 7.6.1; 8.1 bis 8.9; 8.10.1; 8.11; 10.7; 11.3; 11.4; 32; 34.8; 34.12
Finanzausschuss	4.3; 4.4; 9; 10.2; 10.4; 14.3; 15; 16.3; 16.4; 34.10; 34.11; 34.13
Ausschuss für Wirtschaft und Arbeit	4.1; 10.1; 10.3; 10.5 bis 10.9; 11; 12; 20.3.5; 21.1; 23; 34.11; 34.14; 34.16; 34.17; 34.19; 34.26
Ausschuss für Verbraucherschutz, Ernährung und Landwirtschaft	3.5; 4.2; 10.5.4; 10.5.5; 10.9; 11.2; 11.4 bis 11.14
Verteidigungsausschuss	18; 20.3.2; 30; 34.23
Ausschuss für Familie, Senioren, Frauen und Jugend	31; 34.24
Ausschuss für Gesundheit und Soziale Sicherung	4.3; 22; 24; 25; 26; 27; 28; 34.18
Ausschuss für Verkehr, Bau- und Wohnungswesen	29
Ausschuss für Bildung, Forschung und Technikfolgenabschätzung	4; 11.2; 28.5
Ausschuss für die Angelegenheiten der Europäischen Union	3.2.4; 3.6 bis 3.10; 4.4; 8.9; 11.1; 16; 32; 34.20; 34.21
Ausschuss für Kultur und Medien	4.1; 4.4; 11.1; 11.2; 11.6; 34.15

Anlage 2 (zu Nr. 1.15)

Übersicht über die durchgeführten Kontrollen, Beratungen und Informationsbesuche

Deutscher Bundestag

- SPD-Fraktion des Deutschen Bundestages
- Verwaltung des Deutschen Bundestages

Bundeskanzleramt

- Bundesnachrichtendienst

Auswärtiges Amt

- Auswärtiges Amt (Telekommunikationsanlage/Zentrale)
- eine Ständige Vertretung
- ein Generalkonsulat

Bundesministerium des Innern

- Bundesamt für die Anerkennung ausländischer Flüchtlinge:
  Zentrale und drei Außenstellen
- Bundesamt für Verfassungsschutz
- Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR:
  Zentrale und zwei Außenstellen
- Bundesgrenzschutz mit Grenzschutzdirektion, mehreren Grenzschutzämtern und der Zentralstelle für Information und Kommunikation
- Bundeskriminalamt
- Bundesverwaltungsamt
- Geschäftsstelle des Bundespersonalausschusses
- Bundesakademie für öffentliche Verwaltung
- Bundesbeauftragter für Asylangelegenheiten
- Gemeinsames Zentrum der deutsch-französischen Polizei- und Zollzusammenarbeit in den Grenzgebieten
- Statistisches Bundesamt
- Competence Center IVBB, Berlin

Bundesministerium der Justiz

- Generalbundesanwalt beim Bundesgerichtshof:
  Dienststelle Bundeszentralregister
- Bundesgerichtshof
- Deutsches Patent- und Markenamt
  Zentrale und Außenstellen Berlin und Jena

Bundesministerium der Finanzen

- ein Hauptzollamt
- ein Bundesvermögensamt
- Zollkriminalamt
- Bundesanstalt für Finanzdienstleistungsaufsicht
- Zentrum für Informations- und Datentechnik der Bundesfinanzverwaltung, Bonn und Frankfurt

Bundesministerium für Wirtschaft und Arbeit

- Hauptstelle der Bundesanstalt für Arbeit
- zwei Arbeitsämter
- Telekommunikationsanlage

Bundesministerium der Verteidigung

- zwei Wehrbereichsverwaltungen
- Militärischer Abschirmdienst
- Heeresführungskommando
- Luftwaffenamt
- Amt für Fernmelde- und Informationssysteme der Bundeswehr
- ein Kreiswehrersatzamt

Bundesministerium für Familie, Senioren, Frauen und Jugend

- Bundesamt für den Zivildienst
- eine Zivildienstgruppe
- eine Zivildienststelle

Bundesministerium für Gesundheit und Soziale Sicherung

- Bundesversicherungsamt
- Bundesarbeitsgemeinschaft für Rehabilitation
- Gemeinsame Servicestellen (SGB IX)

Bundesministerium für Verkehr, Bau- und Wohnungswesen

- Luftfahrt-Bundesamt
- Kraftfahrt-Bundesamt
- Bundesamt für Güterverkehr
- Bundesanstalt für Straßenwesen

Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit

- Telekommunikationsanlage

Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung

- Telekommunikationsanlage
- Dienststelle Bonn

noch Anlage 2

Presse- und Informationsamt der Bundesregierung

– Gesamtpersonalrat beim Presse- und Informationsamt der Bundesregierung, Berlin

Deutsche Post AG

– Zentrale
– Niederlassung Wuppertal
– Deutsche Post AG, Bonn, München, Frankfurt/Main Flughafen

Neue Postdienstunternehmen

– AiVOS Brief & Paket Post GmbH, Bamberg
– ALPHA TRANS GmbH & Co. KG, Berlin
– DPD Deutscher Paket Dienst GmbH & Co. KG, Aschaffenburg
– Federal Express Europe Inc. Deutsche Niederlassung, Neu-Isenburg
– General Logistics Systems Germany vormals German Parcel, Neuenstein
– GO! General Overnight, Frankfurt/Main
– Messenger Transport Logistik GmbH, Berlin
– Morgenpost Briefservice GmbH, Mannheim
– OPC Berlin GmbH, Berlin
– TNT Holdings (Deutschland) GmbH, Troisdorf
– trans-o-flex Schnell-Lieferdienst GmbH, Weinheim

Telekommunikationsunternehmen

– 01051 Telecom GmbH
– accom Gesellschaft für Telekommunikationsnetze und -dienstleistungen mbH & Co. KG
– Arcor AG & Co.
– BreisNet Telekommunikations- und Carrier-Dienste GmbH
– Cellway Kommunikationsdienste GmbH
– Deutsche Telekom AG
– dtms AG
– E-Plus Mobilfunk GmbH
– Hutchison Telecom GmbH

Bundesversicherungsanstalt für Angestellte

– Hauptstelle
– zwei Rehabilitationskliniken

Berufsgenossenschaften und Krankenkassen

– Hauptverband der gewerblichen Berufsgenossenschaften
– Bau-Berufsgenossenschaft Frankfurt (Hauptverwaltung)
– Berufsgenossenschaft für den Einzelhandel (Bezirksstelle Bonn)
– Berufsgenossenschaft für Gesundheitsdienst und W ohlfahrtspflege (Hauptverwaltung und Bezirksverwaltung Berlin)
– Berufsgenossenschaft der Feinmechanik und Elektrotechnik (Bezirksverwaltung Köln)
– Berufsgenossenschaft der chemischen Industrie (Bezirksverwaltung Köln)
– Rechenzentrum für das Projekt Phoenics
– AOK-Bundesverband
– Barmer Ersatzkasse – Zentrale Wuppertal
– Karstadt + Quelle BKK

Sonstige

– Otto von Bismarck-Stiftung
– ein überregionales Corporate Network, Bayer AG
– Wirtschaftsunternehmen wegen V erfahren zur Sicherheitsüberprüfung
– Stiftung „Erinnerung, Verantwortung und Zukunft“
– Projekt „Nachweisbeschaffung für ehemalige NS-Zwangsarbeiter/-innen“
– Bundesdruckerei GmbH, Berlin

Anlage 3 (zu Nr. 1.15)

Übersicht über Beanstandungen nach § 25 BDSG

Bundesministerium des Innern

- Verstoß der Bundesgrenzschutzdirektion gegen § 90a Bundesbeamtengesetz beim Umgang mit Beihilfeakten (s. Nr. 21.4)
- Verstoß eines Bundesgrenzschutzamtes gegen die Regelungen der §§ 90 ff. Bundesbeamtengesetz beim Umgang mit Personalaktendaten (s. Nr. 21.3.4)
- Verstoß des BKA gegen §§ 3 DNA-Identitätsfeststellungsgesetz, 11 Abs. 2, 34 BKA-Gesetz i.V .m. der Errichtungsanordnung zur DNA-Analyse-Datei wegen des Speicherns von Datensätzen des Bundesgrenzschutzes und des Zollfahndungsdienstes in der DNA-Analyse-Datei (s. Nr. 13.3)
- Verstoß des BKA gegen § 3 DNA-Identitätsfeststellungsgesetz i.V.m. §§ 81g Strafprozessordnung, 12 Abs. 2 BKA-Gesetz wegen des Speicherns unrechtmäßig vom BGS erhobener DNA-Identifizierungsmuster in der DNA-Analyse-Datei (s. Nr. 13.3)
- Verstoß des BGS gegen §§ 81g, f Strafprozessordnung wegen der Erhebung von DNA-Identifizierungsmustern zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren ohne vorherige richterliche Anordnung (s. Nr. 13.3)
- Verstoß des BGS gegen § 35 Abs. 2 Nr . 2 und Abs. 5 Satz 2 BDSG wegen unterlassener Löschung von beim BGS gespeicherten personenbezogenen Daten und unterlassener Vernichtung der entsprechenden Aktenvorgänge (s. Nr. 14.1)
- Verstoß des BGS gegen § 32 Abs. 1 BDSG wegen unzulässiger Übermittlung personenbezogener Daten an eine Landespolizeibehörde (s. Nr. 14.1)
- Verstoß des BfV gegen innerdienstliche Vorschriften wegen unterlassener V ernichtung von Akten nach Löschung personenbezogener Daten in NADIS-PZD (s. Nr. 17.3)

Bundesministerium der Finanzen

- Verstoß einer Familienkasse gegen § 30 Abgabenordnung wegen unzulässiger Datenübermittlung an die Personalverwaltung eines öffentlich-rechtlichen Kreditinstituts (s. Nr. 9.5)
- Verstoß einer Familienkasse gegen § 93 Abgabenordnung wegen unzulässiger Datenerhebung bei einem privaten Arbeitgeber, anstatt beim Betroffenen (s. Nr. 9.6)
- Verstoß gegen § 89 Abs. 6 T elekommunikationsgesetz wegen Unvereinbarkeit eines BMF-Schreibens mit dieser Vorschrift (s. Nr. 9.8)
- Verstoß der Staatlichen V ersicherung der DDR in Abwicklung gegen das Auskunftsrecht des Betrof fenen gem. § 19 BDSG (s. Nr. 10.4)
- Verstoß des BMF gegen § 24 Abs. 4 Satz 1 Nr. 1 BDSG wegen mangelnder Mitwirkung auf ein Auskunftsersuchen des BfD bezüglich der Dateianwendung „ZAUBER“ beim Bundesamt für Finanzen (vgl. Nr. 15.3)

Bundesministerium der Verteidigung

- Verstoß eines Kreiswehrersatzamtes gegen § 17 Abs. 8 Wehrpflichtgesetz wegen routinemäßiger Erhebung sensibler Daten Wehrpflichtiger im Rahmen der Eignungsuntersuchung und Eignungsfeststellung zum T eil bereits vor der Feststellung, ob der Betrof fene wehrdienstfähig ist (s. Nr. 30.3.1)
- Zahlreiche Verstöße gegen die Regelungen der §§ 90 ff. Bundesbeamtengesetz beim Umgang mit Personalakten (s. Nr. 21.2.3.2)

Bundesministerium für Familie, Senioren, Frauen und Jugend

- Verstoß des Bundesamtes für den Zivildienst gegen § 36 Zivildienstgesetz wegen Speicherung nicht erforderlicher Daten in der Personalakte eines Zivildienstleistenden (s. Nr. 31.1)

Bundesministerium für Verkehr, Bau- und Wohnungswesen

- Zwei Beanstandungen wegen V erstößen des Kraftfahrt-Bundesamtes gegen die Regelungen der §§ 90 ff. Beamtengesetz beim Umgang mit Personalaktendaten (automatisiert und manuell) sowie hierbei eine Beanstandung wegen eines Verstoßes gegen § 9 BDSG nebst Anlage wegen Mängeln im Bereich der Datensicherheit beim Umgang mit Personalaktendaten (s. Nr. 21.3.4)

Bundesanstalt für Arbeit

- Verstoß eines Arbeitsamtes gegen §§ 67a Abs. 2 und 69 Abs. 1 Nr. 2 SGB X wegen rechtswidriger Erhebung von Daten bei einem ehemaligen Arbeitgeber und Übermittlung der Daten an das Sozialgericht (s. Nr. 23.5.1)
- Verstoß eines Arbeitsamtes gegen § 69 Abs. 1 Nr. 1 SGB X wegen rechtswidriger Übermittlung von Daten an eine Krankenkasse (s. Nr. 23.5.2)
- Verstoß eines Mitarbeiters eines Arbeitsamtes gegen § 402 Abs. 1 SGB III wegen rechtswidriger Erhebung und Nutzung von Daten zu privaten Zwecken (s. Nr. 23.5.3)
- Verstoß eines Arbeitsamtes gegen § 35 SGB I i. V. m. § 67d Abs. 1 SGB X wegen rechtswidriger Übermittlung von Daten an private Dritte (s. Nr. 23.5.4)

Deutsche Post AG

- Verstoß gegen § 90 Abs. 3 und 4 Bundesbeamtengesetz (Beamte) und § 12 Abs. 4, § 28 Abs. 1 Satz 1 Nr. 1 und Satz 2 BDSG (Arbeitnehmer) wegen der Erhebung und

noch Anlage 3

Speicherung von Krankheitsdaten in der Personalakte, Verstoß gegen § 90 Abs. 3 Bundesbeamtengesetz wegen des uneingeschränkten Zugangs zu Personalakten durch Fachvorgesetzte und Verstoß gegen § 90 Abs. 4 Bundesbeamtengesetz i. V. m. §§ 46a, 42 Abs. 1 Satz 3 Bundesbeamtengesetz (Beamte) und gegen §§ 13 Abs. 1, 12 Abs. 4 i. V. m. § 28 Abs. 1 Satz 2 BDSG (Arbeitnehmer) bei der Erhebung von Krankheitsdaten bei den Ärzten von Mitarbeitern, von denen hierfür eine „Schweigepflichtentbindungserklärung“ verlangt wurde (s. Nr. 21.2.3.1)

Anlage 4 (zu Nrn. 11.3.3 und 32.5)

24. Internationale Datenschutzkonferenz vom 9. bis 11. September 2002: Statement of the European Data Protection Commissioners at the International Conference on mandatory systematic retention of telecommunication traffic data

The European Data Protection Commissioners have noted with concern that in the third pillar of the EU, proposals are considered which would result in the mandatory systematic retention of traffic data concerning all kinds of telecommunication (i.e. details about time, place and numbers used for phone, fax, e-mail and other use of the internet) for a period of one year or more, in order to permit possible access by law enforcement and security bodies.

The European Data Protecti on Commissioners have grave doubt as to the legitimacy and legality of such broad measures. They also want to draw attention to the excessive costs that would be involved for the telecommunication and internet industry, as well as to the absence of such measures in the United States.

The European Data Protection Commissioners have repeatedly emphasized 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, as further elaborated by the European Court of Human Rights (see Opinion 4/2001 of the Article 29 Working Party established by Directive 95/46/EC, and Declaration of Stockholm, April 2000).

The protection of telecommunication traffic data is now also provided by Directive 2002/58/EC of the European Parliament and the Council concerning privacy and electronic communications (Official Journal L 201/37), under which processing of traffic data is in principle allowed for billing and interconnection payments. After lengthy and explicit debate, retention of traffic data for purposes of law enforcement should meet strict condi tions under Article 15 (1) of the Directive: i.e. in each case only for a limited period and where necessary, appropriate and proportionate in a democratic society.

Where traffic data are to be reta ined in specific cases, there must therefore be a demonstrable need, the period of retention must be as short as possible and the practice must be clearly regulated by law, in a way that provides suf ficient safeguards against unlawful access and any other abuse. Systematic retention of all kinds of traffic data for a period of one year or more would be clearly disproportionate and therefore unacceptable in any case.

The European Data Protection Commissioners expect that the Article 29 Working Party will be consulted on measures that may emer ge from the third pillar discussions before they are adopted.

Anlage 5 (zu Nr. 32.5)

24. Internationale Datenschutzkonferenz vom 9. bis 11. September 2002: Communiqué from Closed Session 9/9/02

Representatives from over 50 Data Protection Authorities and Privacy Commissioners attended the 24 th International Data Protection and Privacy Commissioners Conference held in Cardiff, Wales. The Conference was jointly hosted by the Commissioners from Republic of Ireland, Jersey , Guernsey, Isle of Man and the United Kingdom.

The assembled Commissioners and their representatives discussed many matters of common concern ranging from privacy issues in relation to websites through to video surveillance of the population in public and private places. However, the Commissioners devoted a substantial amount of time to considering the va rious national responses to the terrorist attacks on 11th September 2001.

The Commissioners agreed that whilst there is the need to protect society from such ou trages the reaction in many countries may have gone beyond a measured response to the terrorist threat with serious implications for personal privacy. The Commissioners agreed that the need to safeguard personal privacy in such developments remains an essential task for the world wide data protection community . Unless an approach is taken by Governments which correctly weighs data protection and privacy concerns there is a real danger that they will start to undermine the very fundamental freedoms they are seeking to protect.

Anlage 6 (zu Nr. 3.9)

Konferenz der Europäischen Datenschutzbeauftragten vom 10. bis 11. Mai 2001: Retention of traffic data by Internet Service Providers (ISP's)

The Spring 2001 Conference of European Data Protection Commissioners notes with continuing concern proposals that IPS's should routinely retain traffic data beyond the requirements of billing purposes in order to permit possible access by law enforcement bodies.

The Conference emphasises its view expressed in Stockholm 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 and in relation to the processing of personal data by the 1981 Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108). The Conference points out that such retention would also invade the rights to privacy and data protection specified by Articles 7 and 8 of the recently adopted Charter of Fundamental Rights of the European Union. 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 7 (zu Nr. 3.9)

Konferenz der Europäischen Datenschutzbeauftragten vom 10. bis 11. Mai 2001: Declaration on Article 8 of the EU Charter of Fundamental Rights

The Spring Conference of European Data Protection Commissioners notes with satisfaction that Article 8 of the Charter of Fundamental Rights of the European Union strengthens the provisions on data protection that have been issued in the past few years so that the right to data protection is finally recognised as a fundamental human right.

A veritable „European model“ has been established for data protection. This model is shaping discussions in the international community and should positively influence the dif fusion of an approach considering data protection as a fundamental human right and a basic component of e-citizenship.

This personal data protection model should serve as a guideline for all European Union’s institutions in revising the existing legislation and developi ng new rules as well as in shaping their relationships with third countries. The Conference would like to draw the Commission’s and Parliament’s attention to this important requirement.

Anlage 8 (zu Nr. 3.6)

Von der Arbeitsgruppe nach Artikel 29 der EG-Datenschutzrichtlinie angenommene Dokumente

WP 38 (5102/00)	Stellungnahme 1/2001 zum Entwurf einer Entscheidung der Kommission betreffend die Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach Artikel 26 Absatz 4 der Richtlinie 95/46 Angenommen am 26. Januar 2001
WP 39 (5109/00)	Stellungnahme 2/2001 zum Datenschutzniveau des kanadischen „Personal Information and Electronic Documents Act“ Angenommen am 26. Januar 2001
WP 40 (5095/00)	Stellungnahme 3/2001 zum Datenschutzniveau des australischen „Privacy Amendment (Private Sector) Act 2000“ Angenommen am 26. Januar 2001
WP 41 (5001/01)	Stellungnahme 4/2001 zum Entwurf einer Konvention des Europarats über Cyberkriminalität Angenommen am 22. März 2001
WP 42 (5008/01)	Empfehlung 1/2001 hinsichtlich Daten in Beurteilungen von Arbeitnehmern Angenommen am 22. März 2001
WP 43 (5020/01)	Empfehlung 2/2001 zu einigen Mindestanforderungen für die Online-Erhebung personenbezogener Daten in der Europäischen Union Angenommen am 17. Mai 2001
WP 44 (5003/00)	Stellungnahme 5/2001 zum Sonderbericht des Europäischen Bürgerbeauftragten an das Europäische Parlament im Anschluss an den Empfehlungsentwurf an die Europäische Kommission in der Beschwerde 713/98/IJH Angenommen am 17. Mai 2001
WP 46 (5019/01)	Vierter 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 1999 Angenommen am 17. Mai 2001
WP 47 (5061/01)	Stellungnahme 7/2001 zum Entwurf der Entscheidung der Kommission in der Fassung vom 31. August 2001 über Standardvertragsklauseln zur Übermittlung personenbezogener Daten an Datenverarbeiter in Drittländer nach Artikel 26 Absatz 4 der Richtlinie 95/46 Angenommen am 13. September 2001
WP 48 (5062/01)	Stellungnahme 8/2001 bezüglich der Verarbeitung personenbezogener Daten in Arbeitgeber/ Arbeitnehmer-Beziehungen Angenommen am 13. September 2001
WP 49 (5032/01)	Arbeitspapier zur empfohlenen Praktik 1774 der IATA Angenommen am13. September 2001
WP 51 (5074/01)	Stellungnahme 9/2001zur Mitteilung der Kommission über die „Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität“ Angenommen am 5. November 2001

noch Anlage 8

WP 52 (5080/01)	Beschluss 1/2001 über die Teilnahme von Vertretern der Kontrollstellen in den Beitrittsländern an Sitzungen der Artikel 29-Datenschutzgruppe Angenommen am 13. Dezember 2001
WP 53 (5403/01)	Stellungnahme 10/2001 zur Notwendigkeit eines ausgewogenen Vorgehens im Kampf gegen den Terrorismus Angenommen am 14. Dezember 2001
WP 54 (10557/02)	Fünfter Jahresbericht über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten und des Schutzes der Privatsphäre in der Europäischen Union und in Drittländern, Berichtsjahr 2000Angenommen am 6. März 2002
WP 55 (5401/01)	Arbeitsdokument zur Überwachung der elektronischen Kommunikation von Beschäftigten Angenommen am 29. Mai 2002
WP 56 (5035/01)	Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU Angenommen am 30. Mai 2002
WP 57 (10761/02)	Hintergrundinformationen zum Bericht von CEN/ISSS über Standardisierung und Normung im Bereich des Datenschutzes in Europa (CEN, Comité Européen de Normalisation) Angenommen am 30. Mai 2002
WP 58 (10750/02)	Stellungnahme über die Verwendung von eindeutigen Kennungen bei Telekommunikations-endeinrichtungen: das Beispiel IPv6 Angenommen am 30. Mai 2002
WP 60 (11203/02)	Arbeitsdokument Erste Orientierungen der Artikel 29 Datenschutzgruppe zu on-line Authentifizierungsdiensten Angenommen am 2. Juli 2002
WP 61 (11190/02)	Stellungnahme 3/2002 über die Datenschutzbestimmungen eines Richtlinienvorschlags der Kommission zur Harmonisierung der Rechte, Regelungen und Verwaltungsbestimmungen der Mitgliedstaaten zum Konsumentenkredit Angenommen am 2. Juli 2002
WP 62 (11194/02)	Arbeitsdokument zur Funktionsweise des Safe Harbor-Abkommens Angenommen am 2. Juli 2002
WP 63 (11081/02)	Stellungnahme 4/2002 zum Niveau des Schutzes personenbezogener Daten in Argentinien Angenommen am 3. Oktober 2002
WP 64 (11818/02)	Stellungnahme 5/2002 zur Erklärung der europäischen Datenschutzkommissare anlässlich der Internationalen Konferenz in Cardiff (9. bis 11. September 2002) bezüglich der verbindlichen systematischen Aufbewahrung von Verkehrsdaten im Telekommunikationssektor Angenommen am 11. Oktober 2002
WP 65 (11118/02)	Arbeitsdokument über Schwarze Listen Angenommen am 3. Oktober 2002
WP 66 (11647/02)	Stellungnahme 6/2002 betreffend der Übermittlung von Informationen, die Passagiere betreffen sowie andere Flugliniendaten an die USA Angenommen am 24. Oktober 2002

Anlage 9 (zu Nr. 3.4)

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2001: Informationsgesetze

Die Konferenz verfolgt mit Interesse die Bestrebungen des Bundes, ein Informationszugangsgesetz zu schaffen und dem Bundesbeauftragten für den Datenschutz die Aufgaben zur Sicherung des Informationszugangs zu übertragen. Die Bundesregierung nimmt damit die Überlegungen auf, die in Artikel 255 EU-Vertrag und Artikel 42 EU-Grundrechte-Charta zum Ausdruck kommen. Die Konferenz betont, dass das Recht auf informationelle Selbstbestimmung der Einzelnen dem freien Zugang zu behördeninternen, amtlichen Informationen nicht entgegen steht, wenn die Privatsphäre der Betroffenen sowie Betriebsgeheimnisse gesetzlich geschützt bleiben. Die Berichte aus den Ländern Berlin, Brandenburg und Schleswig-Holstein zeigen, dass die datenschutzrechtlichen Gewährleistungen für die informationelle Selbstbestimmung sich mit dem erweiterten Zugangsrecht zu den Informationen öffentlicher Stellen unter der Voraussetzung entsprechender Schutzmechanismen vereinbaren lassen. Die Zusammenführung von Datenschutz- und Informationszugangskontrolle kann diese Gewährleistung institutionell absichern.

Anlage 10 (zu Nr. 7.3)

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2001:
Novellierung des Melderechtsrahmengesetzes

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Absicht der Bundesregierung, das Melderechtsrahmengesetz im Hinblick auf die neuen Informations- und Kommunikationstechnologien zu modernisieren und einzelne unnötige Meldepflichten abzuschaffen.

1. Allerdings sind aus dem vorliegenden Gesetzentwurf Tendenzen zu erkennen, dass durch den Zusammenschluss mehrerer Melderegis ter übergreifende Dateien entstehen können, die letztlich sogar zu einem zentralen Melderegister führen würden. Eine solche Entwicklung wäre aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil damit das Recht auf info rmationelle Selbstbestimmung der Bür gerinnen und Bür ger unverhältnismäßig eingeschränkt werden würde.

2. Bereits die bisherige Rechtslage, nach der nahezu jedermann eine einfache Melderegisterauskunft von der Meldebehörde erhalten kann, ist äußerst unbefriedigend. Dies wird dadurch verschärft, dass der Gesetzentwurf – wie in seiner Begründung ausdrücklich betont wird – nunmehr vorsieht, einfache Melderegisterauskünfte mithilfe des Internet durch jedermann auch elektronisch abrufen zu können. Um sich gegen eine unkontrollierte Weitergabe solcher über das Internet zum Abruf bereitgehaltener Daten schützen zu können und weil beim internetgestützten Abruf die gesetzlich vor geschriebene Berücksichtigung der schutzwürdigen Belange Betroffener nicht möglich ist, sollte für die Bür gerin oder den Bürger in diesen Fällen ei n ausdrückliches Einwilligungsrecht oder mindestens ein W iderspruchsrecht geschaffen werden. Es handelt sich hier um personenbezogene Daten, die auf der Grundlage einer gesetzlichen Auskunftspflicht erhoben wurden.

3. Auch für öffentliche Stellen sollte in das Gesetz eine Bestimmung aufgenommen werden, wonach bei elektronischen Abrufverfahren über das Internet zur Wahrung der schutzwürdigen Interessen der Betrof fenen zumindest Verfahren der fortgeschrittenen elektronischen Signatur gemäß den Regelungen des Signaturgesetzes einzusetzen sind.

4. Nach geltendem Recht ist jede Melderegisterauskunft unzulässig, wenn eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange glaubhaft gemacht wird. Diese Regelung hat sich bewährt. Die Datenschutzbea uftragten treten angesichts des in diesen Fällen best ehenden hohen Schutzbedarfs dem Vorhaben entschieden entgegen, diese Regelung durch eine Risikoabwägung im Einzelfall aufzuweichen.

5. Bislang dürfen Meldebehörden an Parteien, Wählergruppen und andere T räger von W ahlvorschlägen Auskunft über Daten von Gruppen von W ahlberechtigten erteilen, sofern die W ahlberechtigten dieser Auskunftserteilung nicht widersprochen haben. Die Datenschutzbeauftragten bekräftigen ihre bereits in der V ergangenheit erhobene Forderung, gesetzlich zu regeln, dass eine Einwilligung der Betrof fenen Voraussetzung für solche Datenweitergaben sein muss. Die bisherige W iderspruchslösung ist in weiten Kreisen der Bevölkerung unbekannt.

6. Außerdem fordern die Datenschutzbeauftragten, die Hotelmeldepflicht abzuschaffen, da die hiermit verbundene millionenfache Datenerhebung auf V orrat unverhältnismäßig ist.

Bei Enthaltung Thüringens zu Ziffer 6.

Anlage 11 (zu Nr. 8.5)

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2001: Datenschutz bei der Bekämpfung von Datennetzkriminalität

Der Europarat entwirft gegenwärtig zusammen mit anderen Staaten, insbesondere den USA und Japan, eine Konvention über Datennetzkriminalität (Cyber-crime-Konvention), die über ihren Titel hinaus auch die automatisierte Speicherung von Daten im Zusammenhang mit anderen Straftaten regeln soll.[1)]

Die Datenschutzbeauftragten des Bundes und der Länder verkennen nicht, dass das Internet – ebenso wie andere technische Hilfsmittel – für Straftaten missbraucht wird. Sie teilen daher die Auffassung des Europarats, dass der Kriminalität auch im Internet wirksam begegnet werden muss. Allerdings ist zu beachten, dass sich die weit überwiegende Anzahl der Nutzenden an die gesetzlichen Vorgaben hält. Insoweit stellt sich die Frage der Verhältnismäßigkeit von Maßnahmen, die alle Nutzenden betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder teilen die Auffassung der Europäischen Kommission, dass zur Schaffung einer sichereren Informationsgesellschaft in erster Linie die Sicherheit der Informationsinfrastruktur verbessert werden und anonyme wie pseudonyme Nutzungsmöglichkeiten erhalten bleiben müssen; über Fragen der Bekämpfung der Datennetzkriminalität sollte ein offener Diskussionsprozess unter Einbeziehung der Betreiberinnen und Betreiber, Bürgerrechtsorganisationen, Verbraucherverbände und Datenschutzbeauftragten geführt werden.[2)]

Die Konferenz regt eine entsprechende Debatte auch auf nationaler Ebene an und bittet die Bundesregierung, hierfür den erforderlichen Rahmen zu schaffen.

Die Konferenz der Datenschutzbeauftragten fordert die Bundesregierung auf, sich bei der Schaffung von nationalen und internationalen Regelungen zur Bekämpfung von Datennetzkriminalität dafür einzusetzen, dass

- Maßnahmen zur Identifikation von Internetnutzenden, zur Registrierung des Nutzungsverhaltens und Übermittlung der dabei gewonnenen Daten für Zwecke der Strafverfolgung erst dann erfolgen dürfen, wenn ein konkreter Verdacht besteht,
- der Datenschutz und das Fernmeldegeheimnis gewährleistet und Grundrechtseingriffe auf das unabdingbare Maß begrenzt werden,
- der Zugriff und die Nutzung personenbezogener Daten einer strikten und eindeutigen Zweckbindung unterworfen werden,
- Daten von Internetnutzenden nur in Länder übermittelt werden dürfen, in denen ein angemessenes Niveau des Datenschutzes, des Fernmeldegeheimnisses und der Informationsfreiheit gewährleistet ist sowie verfahrensmäßige Garantien bei entsprechenden Eingriffen bestehen.

---

1) European Committee on Crimes Problems (CDPC), Committee of Experts on Crime in Cyber-Space (PC-CY), Draft Convention on Cyber-crime (PC-CY (2000) Draft No. 25)

2) Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 26.01.2001 – KOM (2000) 890 endgültig

Anlage 12 (zu Nr. 19.2)

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2001: Novellierung des G10-Gesetzes

Die Datenschutzbeauftragten des Bundes und der Länder sehen mit großer Sorge, dass die Empfehlungen des Rechts- und des Innenausschusses des Bundesrates erhebliche Einschränkungen der Persönlichkeitsrechte der Bürgerinnen und Bürger zur Folge hätten, die über den Gesetzentwurf der Bundesregierung teilweise weit hinausgehen. Die Datenschutzbeauftragten wenden sich insbesondere entschieden dagegen, dass

- die Befugnisse der Nachrichtendienste zur Übermittlung und Verwendung von G10-Daten an Strafverfolgungsbehörden gegenüber dem Gesetzentwurf noch deutlich erweitert werden sollen, indem Erkenntnisse der Nachrichtendienste u. a. zur Strafverfolgung weit über die Schwerkriminalität hinaus genutzt werden dürften;
- der Verzicht auf die Kennzeichnung von G10-Daten sogar ohne vorherige Zustimmung der G10-Kommission zulässig sein und
- die Schwelle dafür, endgültig von der Benachrichtigung Betroffener abzusehen, deutlich herabgesetzt werden soll.

Darüber hinaus kritisieren die Datenschutzbeauftragten des Bundes und der Länder, dass die Bundesregierung mit der Gesetzesnovelle über die Vorgaben des BVerfG hinaus weitere Änderungen im G10-Bereich erreichen will, die neue grundrechtliche Beschränkungen vorsehen:

- Die Anforderungen an die halbjährlichen Berichte des zuständigen Bundesministers an die PKG müssen so gefasst werden, dass eine wirksame parlamentarische Kontrolle erreicht wird. Dies ist derzeit nicht gewährleistet. Deshalb muss über Anlass, Umfang, Dauer, Ergebnis und Kosten aller Maßnahmen nach dem G10-Gesetz sowie über die Benachrichtigung der Beteiligten berichtet werden. Die gleichen Anforderungen müssen auch für die Berichte der PKG an den Bundestag gelten.
- Die Neuregelung, nach der auch außerhalb der Staatsschutzdelikte mutmaßliche Einzeltäter und lose Gruppierungen den Maßnahmen nach dem G10-Gesetz unterliegen sollen, stellt das Trennungsgebot nach Artikel 87 Abs. 1 Satz 2 GG weiter infrage. Ermittlungen von der Eingriffsschwelle eines konkreten Anfangsverdachts zu lösen und nach nachrichtendienstlicher Art schon im Vorfeld zur Verdachtsgewinnung durchzuführen, weitet die Gefahr unverhältnismäßig aus, dass auch gegen Unbescholtene strafrechtlich ermittelt wird.
- Alle Neuregelungen wie z. B. zum Parteienverbotsverfahren, zur Verwendung von G10-Erkenntnissen bei Gefahren für Leib oder Leben einer Person im Ausland und zu Spontanübermittlungen an den BND müssen befristet und einer effizienten Erfolgskontrolle unterzogen werden.
- Bei der internen Datenverarbeitung durch die Nachrichtendienste ist die Zweckbindung so zu formulieren, dass die erhobenen Daten nicht zur Erforschung und Verfolgung anderer als der in § 3 und § 5 G10-E genannten Straftaten genutzt werden dürfen.
- Die vorgesehenen Ausnahmen von der vom BVerfG geforderten Kennzeichnungspflicht bei der Übermittlung von Daten, die aus G10-Maßnahmen stammen, begegnen schwerwiegenden datenschutzrechtlichen Bedenken.
- Im Gesetzentwurf fehlt die Regelung, dass eine Weiterübermittlung an andere Stellen und Dritte nicht zulässig ist. Sie darf nur durch die erhebende Stelle erfolgen. Die Weitergabe von G10-Daten an andere Dienststellen ist bei der übermittelnden Stelle stets zu dokumentieren und zu kennzeichnen.
- Eine dauerhafte Ausnahme von der Benachrichtigungspflicht ist abzulehnen. Sie würde für die Betroffenen zu einem Ausschluss des Rechtsweges führen.
- Dem BND wird nicht mehr nur die „strategische Überwachung“ des nicht leitungsgebundenen, sondern künftig des gesamten internationalen Telekommunikationsverkehrs ermöglicht. Dies setzt den Zugriff deutscher Stellen auf Telekommunikationssysteme in fremden Hoheitsbereichen voraus. Dabei muss sichergestellt werden, dass die Anforderungen des Völkerrechts eingehalten werden.
- Die Überwachung internationaler Telekommunikationsbeziehungen im Falle einer Gefahr für Leib oder Leben einer Person im Ausland (§ 8 G10-E) ermöglicht sehr intensive Grundrechtseingriffe in großer Zahl und mit einer hohen Dichte, die höher sein kann als bei „strategischen Überwachung“ nach § 5 G10-E. Dies setzt eine hohe Eingriffsschwelle und enge zeitliche Befristungen voraus, die der Entwurf nicht hinreichend vorsieht.

Anlage 13 (zu Nr. 24.1.1)

Beschluss der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2001 zum Arbeitsentwurf des Bundesministeriums für Gesundheit für ein Gesetz zur Verbesserung der Datentransparenz und des Datenschutzes in der gesetzlichen Krankenversicherung (Transparenzgesetz – GKV – TG)

Die Datenschutzkonferenz begrüßt es, dass mit dem Arbeitsentwurf die Forderung der Konferenz wieder aufgegriffen wird, durch Pseudonymisierung des Abrechnungsverfahrens die Belange des Patientengeheimnisses und des Datenschutzes zu wahren. Ziel muss sein, den „gläsernen Patienten“ bei den gesetzlichen Krankenkassen zu vermeiden. Mit Pseudonymisierungsverfahren lässt sich dieses Ziel erreichen, ohne dass beispielsweise die Kostenkontrolle oder Qualitätssicherung durch eine Krankenkasse beeinträchtigt wäre. Der Deutsche Bundestag hat die Realisierbarkeit dieses Ansatzes mit seinem Beschluss eines Gesundheitsreformgesetzes vom 4. November 1999, der nach einem Vermittlungsverfahren aus anderen als datenschutzrechtlichen Gründen nicht in vollem Umfang in Kraft getreten ist, bereits bejaht.

Die Datenschutzkonferenz begrüßt es weiterhin, dass in dem Arbeitsentwurf im Rahmen einer Klausel „Modellvorhaben Telematik“ die Weiterentwicklung des Datenschutzes als Ziel vorgegeben und dazu gefordert wird, die Modellvorhaben im Benehmen mit den Datenschutzbehörden durchzuführen. Die Konferenz geht dabei davon aus, dass unter „Weiterentwicklung“ die Sicherung der Patientenrechte auf Wahrung des Arztgeheimnisses und des Datenschutzes auch unter den Randbedingungen der Telematikanwendungen im medizinischen Bereich zu verstehen ist. Sie weist dazu besonders auf ihre Beschlüsse von der 47. und der 50. Konferenz zu Chipkarten im Gesundheitswesen hin, mit denen die Sicherung von Patientenautonomie und Transparenz sowie die Sicherheit der Datenverarbeitung gefordert wurde.

Die Konferenz nimmt auch zustimmend zur Kenntnis, dass durch die Begrenzung auf die Verarbeitung von höchstens 20 % der Versichertendaten in den Datenannahme- und -weiterleitungsstellen der Gefahr der Bildung mehr oder weniger bundesweiter Dateien mit sensiblen medizinischen Daten der Krankenversicherten begegnet werden soll.

Die Konferenz hält zu nachstehenden Punkten ergänzende Regelungen bzw. nähere Darlegungen für erforderlich:

– Die Effektivität eines Pseudonymisierungsverfahrens zum Schutz der sensiblen Versichertendaten steht und fällt mit sicheren Pseudonymen, mit der klaren Begrenzung von Reidentifikationen auf im überwiegenden öffentlichen Interesse absolut notwendige Fälle und der Vermeidung des Abgleichs mit identifizierenden Klardaten.

  Unter diesen Aspekten hält die Datenschutzkonferenz den Katalog der Reidentifikationsfälle für bedenklich: So ist nicht ersichtlich, in wieweit die Krankenkassen zur Durchführung des Risikostrukturausgleichs versichertenbezogene Detailangaben über Diagnosen und Leistungen benötigen. Das gilt auch im Hinblick auf in jüngsten Pressemeldungen berichtete Absichten, im Rahmen des Risikostrukturausgleichs einen so genannten Risikopool einzuführen, über den Kassen mit so genannten schlechten Risiken verstärkte Ausgleichsmittel erhalten sollen. Die Feststellung derartiger „schlechter Risiken“ kann auch über Pseudonyme und die ihnen zugeordneten Leistungszahlen erfolgen. Im Falle der Unterstützung der Versicherten bei Verdacht auf Behandlungsfehler sollte die Einwilligung der Versicherten in die Reidentifikation, die durch die Vertrauensstelle eingeholt werden könnte, angestrebt werden. Auch weitere Katalogfälle von Reidentifikationen sind kritisch zu hinterfragen, so insbesondere die Reidentifikation von Versicherten unter Bekanntgabe des Pseudonyms gegenüber den Kassen(zahn)ärztlichen Vereinigungen.

  Es muss verhindert werden, dass über einen zu weit gefassten Katalog von Reidentifikationsfällen ohne Zustimmung der Versicherten das Ziel der Pseudonymisierung praktisch verfehlt wird. Es ist zu gewährleisten, dass keine personenbezogenen Krankheitsdatenkonten bei den gesetzlichen Krankenversicherungen, oder kurz gesagt, dass keine gläsernen Patienten entstehen.

  In gleicher Weise ist zuverlässig zu vermeiden, dass durch Abgleich mit zeitweilig vorhandenen Klardaten Pseudonyme aufgelöst werden. Hierfür ist eine gesetzliche Sicherstellung erforderlich.

  Schließlich ist die Begrenzung der Speicherung und die Zweckbindung aufgelöster Pseudonyme nicht ausreichend klar. Über eine Verweisung in § 284 SGB V würden die dortigen erweiterten Zweckänderungs- und Verarbeitungsregelungen auch auf die Speicherungen von aufgelösten Pseudonymen angewandt und damit die anscheinend strengen Speicherungs- und Zweckbindungsregelungen des Arbeitsentwurfs für die genannten Daten ausgehöhlt. Es müsste klargestellt werden, dass die speziellen Speicher- und Zweckbindungsregelungen der allgemeinen Regel des § 284 SGB V vorgehen.

– Die oben erwähnte, nicht in Kraft getretene Fassung der GKV-Gesundheitsreform 2000 sah die alsbaldige Pseudonymisierung der Versichertendaten in allen Abrechnungen der Leistungserbringer vor, und zwar vor Kenntnisnahme durch die Krankenkassen. Der jetzige Arbeitsentwurf sieht die Pseudonymisierung der Versichertendaten in den Abrechnungen aller nichtvertragsärztlichen Leistungserbringer erst nach Überprüfung durch die Krankenkassen vor. Dies wäre ein datenschutzrechtlicher Rückschritt gegenüber dem Gesetzesbeschluss vom 4. November 1999. Die fachliche Erforderlichkeit dieses Rückschritts sollte, nicht zuletzt auch angesichts des o. g. Bundestagsbeschlusses, näher begründet werden. Zumindest sollte über eine Weiterent-

wicklungsklausel die Nutzung von Pseudonymen auch für diese Leistungsabrechnungen angestrebt werden. Dazu sollte auch geprüft werden, in wieweit die Krankenversichertenkarte als Mittel zur Pseudonymisierung verwendet werden kann.

– Die Konferenz fordert im Sinn von Lösungen, die dem Datensparsamkeitsprinzip genügen, auch eine Pseudonymisierung der Daten der Vertragsärztinnen und -ärzte. Angesichts der Deckelung der vertragsärztlichen Leistungen und der Verordnungen ist nicht ersichtlich, inwiefern für die GKV personenbezogene Daten dieser Leistungserbringer erforderlich sind. Es müsste ausreichen, wie bei den Versicherten die Reidentifikation nur in gesetzlich festgelegten Ausnahmefällen vorzusehen. Die regionalen Datenauswertungsstellen sollen die Daten auch der sonstigen Leistungserbringer nur pseudonymisiert erhalten.

– Die Konferenz würde es generell begrüßen, wenn im Rahmen der Reformüberlegungen zur Gesundheitsversorgung nach Systemen gesucht würde, die mit möglichst wenig personenbezogenen Daten auskommen. Dies würde dem Gebot der Datensparsamkeit entsprechen.

– Wesentliche Grundlage eines sicheren Pseudonymisierungskonzepts ist die Trennung der die Pseudonymisierung durchführenden Vertrauensstellen von den übrigen Datenverarbeitungsstellen des Systems. Für die Trennung von Datenaufbereitungs- und Vertrauensstellen ist das explizit im Arbeitsentwurf festgelegt, es fehlt aber eine entsprechende Regelung für das Verhältnis der Vertrauensstellen zu den übrigen Verarbeitungsstellen. Ungeachtet, dass diese Trennung selbstverständlich sein sollte, wird angeregt, das auch gesetzlich sicherzustellen. Das gleiche gilt für die Trennung der übrigen Stellen voneinander. Für die datenverarbeitenden Stellen ist der Schutz des Sozialgeheimnisses zu gewährleisten.

– Die vorgesehene „Arbeitsgemeinschaft auf Bundesebene“, deren Mitglieder und das BMG dürfen keine personenbezogenen Versicherten- und Leistungserbringerdaten erhalten. Es ist kein zureichender Grund ersichtlich, warum diese auf Bundesebene angesiedelte Arbeitsgemeinschaft, deren Aufgabe die Festlegung einheitlicher Standards für die Datenverarbeitung bei den Datenaufbereitungsstellen sein soll, derartige Daten benötigt. Das Gleiche gilt für die Vertragspartner auf Bundesebene und das Bundesministerium für Gesundheit. Die Datenschutzkonferenz geht davon aus, dass die Übermittlung personenbezogener Daten an diese Stellen nicht beabsichtigt ist. Die Entwurfsformulierung ist insoweit aber unklar. Ebenso ist sicherzustellen, dass die Arbeitsgemeinschaften auf Landesebene über ihren Sicherstellungsauftrag für die Vertrauensstellen keine Pseudonymisierungsparameter erhalten.

– Die Konferenz sieht keinen zureichenden Grund dafür, dass das datenschutzrechtlich begründete Verbot einer personenbezogenen Datei beim MDK mit medizinischen Daten aufgehoben wird. Die dann entstehende landesweite, einzelne Versicherte aller GKV umfassende Datei mit medizinischen Angaben birgt wegen der einfachen Auswertbarkeit in Bezug auf einzelne Personen ein hohes datenschutzrechtliches Risiko, dessen Eingehung damals wie heute nicht durch die „Medienbruchfreiheit“ zu rechtfertigen ist.

– Die Konferenz hat Bedenken gegen weitgehende Richtlinienermächtigungen zugunsten der Spitzenverbände der Krankenkassen. Der Gesetzgeber müsste die wesentlichen Inhalte eingreifender Regelungen selbst bestimmen.

Die Konferenz begrüßt nochmals die in dem Arbeitsentwurf zum Ausdruck kommende Bereitschaft zur Zusammenarbeit mit den Datenschutzstellen und bietet ihrerseits eine enge Zusammenarbeit für die zukünftigen Verhandlungen an, in denen diverseweitere Unklarheiten und Widersprüchlichkeiten des Entwurf auszuräumen sein werden.

Sie richtet zu diesem Zweck eine ad-hoc-Arbeitsgruppe des AK Gesundheit und Soziales ein, die auch vom BfD jeweils für die Verhandlungen einberufen werden kann.

Anlage 14 (zu Nr. 8.2.3.4)

Entschließung zwischen der 61. und 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder:
Anlasslose DNA-Analyse aller Männer verfassungswidrig

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist entschieden den V orschlag zurück, den „genetischen Fingerabdruck“ aller Männer zu erheben und rein vorsorglich zu speichern. Die Erhebung personenbezogener Daten ist auch im Rahmen der Strafverfolgung an rechtsstaatliche Grundsätze gebunden. Eine Datenerhebung auf Vorrat, die die Hälfte der Bevölkerung als potenzielle Straftäter behandelt, ist ve rfassungsrechtlich unzulässig. Darüber hinaus erscheint der erwartete Abschreckungseffekt äußerst fragwürdig.

Anlage 15 (zu Nr. 10.7)

Entschließung zwischen der 61. und 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. April 2001:
Veröffentlichung von Insolvenzinformationen im Internet

Dem Bundestag liegt ein Gesetzentwurf der Bundesregierung zur Änderung der Insolvenzordnung (Bundestagsdrucksache 14/5680) vor. Danach sollen gerichtliche Entscheidungen – vor allem in Verbraucherinsolvenzverfahren – künftig auch über das Internet veröf fentlicht werden können, um Kosten für Bekanntmachungen in Printmedien zu sparen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Informationen aus Insolvenzverfahren, die in das Internet eingestellt sind, durch die Justiz nicht räumlich begrenzt werden können. Darüber hinaus ist deren Speicherung zeitlich nicht beherrschbar und die Daten können vielfältig ausgewertet werden. Dies kann dazu führen, dass Dritte, etwa Auskunfteie n oder W irtschaftsinformationsdienste, die Daten auch nach Abschluss eines Insolvenzverfahrens speichern und diese über längere Zeit im Internet verfügbar sind. Die mit der Insolvenzordnung bezweckte Chance der Schuldner auf einen wirtschaftlichen Neubeginn würde letztlich auf Dauer beeinträchtigt, wenn sie zeitlebens weltweit abrufbar am Schulden-Pranger stehen.

Der Gesetzgeber muss das Ri siko für die betrof fenen Verbraucherinnen und Verbraucher, aufgrund einer möglichen Auswertung justizieller Veröffentlichungen im Internet dauerhaft Einbußen bei der Teilnahme am Wirtschaftsverkehr zu erleiden, sorgfältig mit dem Interesse an der beabsichtigten Senkung von Bekanntmachungskosten abwägen. Hierbei ist auch die gesetzgeberische Wertung zu berücksichtigen, dass Personen, für die ein Insolvenzverfahren eröffnet wurde, gerade nicht in das Schuldnerverzeichnis beim Amtsgericht aufgenommen werden. Das Internet bietet im Gegensatz zu einem gerichtlichen Verzeichnis letztlich keine Gewähr, die ordnungsgemäße Pflege und die Löschung personenbezogener Daten sicherzustellen, die für die Betrof fenen von entscheidender wirtschaftlicher Bedeutung sein können. Die Datenschutzbeauftragten appellieren daher an den Gesetzgeber und an die Justizverwaltungen der Länder, die aufgezeigten Risiken insbesondere für Verbraucherinsolvenzen neu zu bewerten. Die vorgenannten Überlegungen sind im Gesetzgebungsverfahren bisher nicht in ausreichendem Maße berücksichtigt worden. Dabei sollten die Erwägungen des Bundesverfassungsgerichts im Be schluss vom 9. März 1988 – 1 BvL 49/86 – zu einem ver gleichbaren Sachverhalt einbezogen werden.

Es erscheint zu einfach, die Informationen im Internet in gleicher Weise abzubilden wie in der Zeitung. Gerade das Internet bietet neue Chancen und Möglichkeiten, Informationen gezielt nur denen zugänglich zu machen, die es angeht. Gerade hier sind neue W ege möglich, die mit herkömmlichen Medien nicht erreicht werden konnten. Es gilt deshalb, insbesondere zu untersuchen, ob dem Prinzip der Publizität bei Veröffentlichungen im Internet nicht ein anderer Stellenwert zukommt und wie gravierende Nachteile für die Betroffenen vermieden werden können.

Bevor die geplante Änderung des § 9 InsO verabschiedet wird, ist daher vorrangig zu klären, wie das Recht auf informationelle Selbstbestimmung de r Betroffenen besser geschützt werden kann.

Auch in anderen Bereichen wird das Internet bereits genutzt, erprobt oder die Nutzung erwogen, um justizielle Informationen bereitzustellen, z. B. die Handels-, Vereins-, Genossenschafts- und Partnerschaftsregister oder in Zwangsvollstreckungsverfahren. Inwieweit das Internet als Medium der im Ergebnis unbegrenzbaren Informationsverarbeitung datenschutzrechtlich angemessen ist und welches Datenprofil ins Internet eingestellt werden darf, muss differenziert in Übereinstimmung mit dem gesetzlich bezweckten Grad der Publizität der jeweiligen Daten entschieden werden. Jede gesetzgeberische Entscheidung für eine Veröffentlichung über das Internet sollte aber im Hinblick auf deren besondere Risiken regeln, dass Veröffentlichungen befristet sind und dass spezielle Vorkehrungen getroffen werden, um die Identität und die Authentizität zu sichern sowie eine automatische Übernahme der Daten zu verhindern (Kopierschutz).

Sollte sich der Gesetzgeber nach sorgfältiger Abwägung für eine Veröffentlichung über das Internet entscheiden, so muss er die Auswirkungen der Regelung aufgrund aussagefähiger Berichte der Landesjustizverwaltungen überprüfen. Gegenstand dieser Überprüfung muss auch sein, ob die eingetretene Kostensenkung tatsächlich, wie von der Bundesregierung erwartet, einer größeren Anzahl von Schuldnerinnen und Schuldnern den W eg zur Restschuldbefreiung eröffnet hat.

Anlage 16 (zu Nr. 11.3.2)

Entschließung zwischen der 61. und 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 10. Mai 2001 zum Entwurf der Telekommunikations-Überwachungsverordnung

Das Bundesministerium für Wirtschaft hat Ende Januar 2001 den Entwurf für eine Telekommunikations-Überwachungsverordnung (TKÜV) vorgelegt, der in Kürze dem Bundeskabinett zugeleitet wird. Der Entwurf basiert auf dem Telekommunikationsgesetz, das den Begriff der Telekommunikation weit fasst. Da er technikneutral formuliert ist, werden von den Überwachungsmaßnahmen nicht nur die Sprachtelefonie und der Telefaxverkehr, sondern auch alle anderen elektronischen Kommunikationsplattformen und damit insbesondere auch das Internet erfasst.

Sobald ein Internetprovider einen E-Mail-Dienst anbietet, muss er technische Einrichtungen zur Umsetzung der Überwachungsmaßnahmen vorhalten, obwohl die Vermittlung des Zugangs zum Internet als anmelde- und zulassungsfreier Teledienst nicht zu den Telekommunikationsdiensten gehört. Diese Verpflichtung der Internetprovider macht es technisch möglich, künftig den gesamten Internetverkehr, also auch das bloße „Surfen“ zu überwachen. Dies ist aber nach deutschem Recht so nicht vorgesehen. Bedenklich ist in diesem Zusammenhang, dass das European Telecommunications Standards Institute (ETSI) gegenwärtig an einem technischen Standard arbeitet, der den Lauschangriff auf IP-Netze (Internet) und die Überwachung des gesamten Internetverkehrs europaweit vereinheitlichen soll.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden dagegen, eine technische Infrastruktur zu schaffen, die jederzeit eine umfassende Überwachung des Internetverkehrs möglich macht. Eine derartige Überwachung würde einen unverhältnismäßigen Eingriff in das Grundrecht auf Persönlichkeitsschutz darstellen und darüber hinaus den im Teledienstedatenschutzgesetz und im Mediendienstestaatsvertrag normierten Grundsätzen der Datenvermeidung und der Datensparsamkeit zuwiderlaufen.

Es muss sichergestellt werden, dass die zunehmende Nutzung von Telediensten zu Alltagsgeschäften auch künftig generell überwachungsfrei bleibt. Die bestehenden materiellen Befugnisse zur Telekommunikationsüberwachung im Strafprozessrecht, G 10-Gesetz und im Außenwirtschaftsgesetz bedürfen zudem insgesamt dringend einer kritischen Evaluation und Bereinigung, die die Bundesregierung durch eine wissenschaftliche Untersuchung der Effektivität bisheriger Überwachungsanordnungen bereits eingeleitet hat.

Die Datenschutzbeauftragten des Bundes und der Länder fordern ebenso eine Evaluation der Telekommunikations-Überwachungsverordnung, die im Lichte der Ergebnisse der Untersuchung über die Effektivität von Telekommunikations-Überwachungsmaßnahmen vorzunehmen ist.

Anlage 17 (zu Nr. 2.1)

Entschließung zwischen der 61. und 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. Oktober 2001 zur Terrorismusbekämpfung

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen mit Nachdruck den Kampf des demokratischen Rechtsstaates gegen Terrorismus und organisierte Kriminalität. Sie sind heute zu einem Sondertref fen in Bonn zusammengekommen, um die aktuelle Situation nach den Terroranschlägen zu erörtern. Im politischen Raum werden zahlreiche Forderungen und Vorschläge zur Verbesserung der inneren Sicherheit diskutiert, die auch Auswirkungen auf den Datenschutz haben.

Die Datenschutzbeauftragten weisen darauf hin, dass die Sicherheits- und Strafverfolgungs behörden zur T errorismusbekämpfung bereits über weitreichende Befugnisse zur Datenverarbeitung verfügen. So ist z. B. die Rasterfahndung zu Strafverfolgungszwecken generell möglich, in den meisten Ländern auch zur Gefahrenab wehr durch die Polizei. Das Bundesamt für die Anerkennung ausländischer Flüchtlinge kann bereits heute Erkenntnisse über terroristische Aktivitäten an den V erfassungsschutz und die Polizei übermitteln. Auch ist eine ef fektive Zusammenarbeit zwischen Polizei und Verfassungsschutz durch di e geltende Rechtslage gewährleistet; Vollzugsdefizite sind kein Datenschutzproblem. Zu pauschalen Forderungen nach Einschränkung des Bürgerrechts auf Datenschutz besteht deshalb kein Anlass. Die Datenschutzbeauftragten betonen, dass Datenschutz nie Täterschutz war und auch in Zukunft nicht sein wird.

Die Datenschutzbeauftragten sind zu einem ofenen und konstruktiven Dialog über etwa notwendige Anpassungen an die neue Bedrohungslage bereit. Sie erwarten, dass sie rechtzeitig beteiligt werden. Die Da tenschutzbeauftragten warnen vor übereilten Maßnahmen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger einschränken. Sie sprechen sich dafür aus, alle neu beschlossenen Eingriffsbefugnisse zu befristen und tief greifende Eingriffsbefugnisse, damit auch die laufende Rasterfahndung, einer ergebnisoffenen Erfolgskontrolle zu unterziehen.

Bei der künftigen Gesetzgebung sind die grundlegenden Rechtsstaatsprinzipien, das Grundrecht der freien Entfaltung der Persönlichkeit, das Verhältnismäßigkeitsprinzip, die Unschuldsvermutung und das Gebot besonderer gesetzlicher Verwendungsregelungen für sensible Daten selbstverständlich zu beachten. Diese verfassungsrechtlichen Garantien prägen den Rechtsstaat, den wir gemeinsam zu verteidigen haben.

Anlage 18 (zu Nr. 2.1)

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. bis 26. Oktober 2001: Freiheits- und Persönlichkeitsrechte dürfen bei der Terrorismusbekämpfung nicht verloren gehen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass zahlreiche Vorschläge in der gegenwärtigen Debatte um notwendige Konsequenzen aus den Terroranschlägen vom 11. September 2001 die erforderliche sachliche und verantwortungsbewusste Abwägung mit den grundgesetzlich geschützten Freiheits- und Persönlichkeitsrechten der Einzelnen vermissen lassen.

Der Entwurf eines Terrorismusbekämpfungsgesetzes und der Antrag der Länder Baden-Württemberg, Bayern und Hessen im Bundesrat zur wirksamen Bekämpfung des internationalen Terrorismus und Extremismus (Bundesratsdrucksache 807/01) übertreffen die in der Entschließung der Konferenz vom 1. Oktober 2001 geäußerte Befürchtung, dass übereilt Maßnahmen ergriffen werden sollen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger unangemessen einschränken.

Gegenwärtig wird ohne Rücksicht auf das grundrechtliche Übermaßverbot vorgeschlagen, was technisch möglich erscheint, anstatt zu prüfen, was wirklich geeignet und erforderlich ist. Außerdem müsste der Frage nachgegangen werden, ob es nicht in den Geheimdiensten und in der Strafverfolgung Vollzugsdefizite gibt. Dabei müsste auch untersucht werden, welche Resultate die vielen Gesetzesverschärfungen der letzten Jahre gebracht haben.

Persönlichkeitsrechte haben über ihre grundrechtssichernde Wirkung hinaus – mit den Worten des Bundesverfassungsgerichts – auch Bedeutung als „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens“.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert daher sehr eindringlich an alle Beteiligten, nicht Persönlichkeitsrechte vorschnell und ohne die gebotene sorgsam abwägende Prüfung über die bereits bestehenden Eingriffsmöglichkeiten hinaus dauerhaft einzuschränken und so den Ausnahmezustand zur Norm zu erheben.

Alle neu erwogenen Maßnahmen müssen sich daran messen lassen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte so überlagern, dass es in unserem Land zu einer langwirkenden Verschiebung zugunsten staatlicher Überwachung und zulasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommt.

Wesentliche im BMI-Entwurf eines Terrorismusbekämpfungsgesetzes enthaltene Eingriffsmöglichkeiten führen zwangsläufig dazu, dass eine Vielzahl völlig unbescholtener Einzelpersonen zentral erfasst oder verdeckt in Datenerhebungen einbezogen werden, ohne dass eine konkrete Verdachts- oder Gefahrenlage verlangt wird. Zugleich werden Auskunftspflichten und Ermittlungskompetenzen in einer Weise ausgedehnt, dass Eingrenzungen verloren gehen, die aus rechtsstaatlichen Gründen unverzichtbar sind.

Der Verfassungsschutz soll künftig zur Erfüllung aller seiner Aufgaben von den Banken die Kontenbewegungen, von den Luftverkehrsunternehmen alle Reisedaten und von den Post- und Telekommunikationsunternehmen alle Informationen darüber erhalten können, wer von wem Post erhalten und wann mit wem telefoniert hat. All dies soll ohne Wissen der Betroffenen erfolgen und bis zu 15 Jahren gespeichert werden.

Die geplante Befugnis des BKA, Vorermittlungen ohne Anfangsverdacht im Sinne der StPO zu ergreifen, führt zu Eingriffen in das Persönlichkeitsrecht, die weit über das verfassungsrechtlich Zulässige hinausreichen und das tradierte System der Strafverfolgung sprengen. Dies verschiebt die bisher klaren Grenzen zwischen BKA und Verfassungsschutz sowie zwischen Gefahrenabwehr und Strafverfolgung. Ohne jeden Anfangsverdacht soll das BKA künftig Daten über nicht näher eingegrenzte Personenkreise erheben dürfen. Dies kann im Prinzip jede Bürgerin und jeden Bürger betreffen, ohne dass sie sich auf die Schutzmechanismen der Strafprozessordnung verlassen können.

Auch die Vorschläge der Länder enthalten unvertretbare Einschränkungen von grundgesetzlich geschützten Rechtspositionen. So soll die Gefahrenschwelle für den verdeckten Einsatz technischer Mittel in Wohnungen übermäßig abgesenkt werden. Telekommunikationsunternehmen und Internetprovider sollen gesetzlich verpflichtet werden, Verbindungsdaten (zum Beispiel über den Besuch einer Website oder einer Newsgroup) länger zu speichern, als diese zu Abrechnungszwecken benötigt werden, um sie Sicherheitsbehörden zur Verfügung zu stellen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, dass neue Eingriffsbefugnisse nicht pauschal ausgerichtet, sondern zielgenau auf konkrete Gefährdungssituationen im terroristischen Bereich zugeschnitten und von vornherein befristet werden. Eine unabhängige Evaluierung nach festgelegten Fristen ist unerlässlich, um Geeignetheit und Erforderlichkeit für die Zukunft sachgerecht beurteilen zu können.

Anlage 19 (zu Nrn. 8.1 und 28.5)

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. bis 26. Oktober 2001:
Gesetzliche Regelung von genetischen Untersuchungen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder konkretisiert ihre Forderungen an Bundestag und Bundesrat, genetische Untersuchungen am Menschen gesetzlich zu regeln. Geboten sind besondere Regelungen für genetische Untersuchungen zu medizinischen Zwecken, zur Klärung von Identität und Abstammung, im Zusammenhang mit Arbeits- und Versicherungsverhältnissen sowie zu Forschungszwecken. Außer dem „genetischen Fingerabdruck" für Zwecke der Strafverfolgung – in der Strafprozessordnung bereits normiert – sind typische Anwendungsfelder für genetische Untersuchungen zu regeln. Von besonderer Bedeutung sind das Informations- und Entscheidungsrecht der betroffenen Personen. Die Kernanliegen der Datenschutzbeauftragten sind:

- Stärkung des Selbstbestimmungsrechts durch einen grundsätzlichen Einwilligungsvorbehalt für die Durchführung genetischer Untersuchungen;
- Information und Transparenz für die betroffene Person durch Umschreibung des notwendigen Aufklärungsumfangs;
- Qualität und Sicherheit genetischer Tests durch Arzt- und Zulassungsvorbehalte;
- Schutz von Ungeborenen, Minderjährigen und nicht einsichtsfähigen Personen durch abgestufte Beschränkung zugelassener Untersuchungsziele;
- Gewährleistung des Rechts auf Nichtwissen durch differenzierte Entscheidungs- und Offenbarungsoptionen;
- Verhinderung heimlicher Gentests durch das Gebot der Probennahme direkt in ärztlicher Praxis oder Labor;
- Verhinderung von missbräuchlicher Nutzung genetischer Erkenntnisse im Arbeitsleben und im Versicherungsverhältnis durch ein grundsätzliches Verbot, Gentests oder Testergebnisse zu fordern oder entgegen zu nehmen;
- Selbstbestimmung der Betroffenen auch im Forschungsbereich durch einen grundsätzlichen Einwilligungsvorbehalt bei einzelnen Forschungsprojekten und Proben- und Gendatenbanken;
- Sicherung zuverlässiger Pseudonymisierungsverfahren bei Proben- und Gendatenbanken durch externe Datentreuhänderschaft;
- Hilfe für die Betroffenen durch die Pflicht, im Rahmen der Forschung individuell bedeutsame Untersuchungsergebnisse mitzuteilen;
- Absicherung der Regelungen durch die Einführung von Straftatbeständen.

Neben diesen bereichsspezifischen Bestimmungen zu den verschiedenen Zwecken genetischer Untersuchungen fordert die Konferenz der Datenschutzbeauftragten eine grundlegende Strafnorm im Strafgesetzbuch, um Gentests ohne gesetzliche Ermächtigung oder ohne die grundsätzlich nur für Zwecke der medizinischen Behandlung oder Forschung wirksame Einwilligung der betroffenen Person zu unterbinden.

Die Datenschutzbeauftragten des Bundes und der Länder verstehen ihre Vorschläge als Anregungen zu anstehenden Gesetzesinitiativen und zur gesellschaftspolitischen Diskussion.

Von einem Abdruck der Anlage zur Entschließung wurde wegen ihres Umfangs abgesehen. Sie ist unter www.bfd.bund.de abrufbar.

Anlage 20 (zu Nr. 8.9)

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. bis 26. Oktober 2001: EUROJUST – Vorläufer einer künftigen europäischen Staatsanwaltschaft?

Der Europäische Rat hat im Herbst 1999 in Tampere die Einrichtung einer gemeinsamen Stelle EUROJUST zur justiziellen Zusammenarbeit beschlossen. EUROJUST soll zur Bekämpfung der schweren organisierten Kriminalität eine sachgerechte Koordinierung der nationalen Staatsanwaltschaften erleichtern und die strafrechtlichen Ermittlungen unterstützen sowie die Erledigung von Rechtshilfeersuchen vereinfachen. Zusätzlich beschloss der Rat im Dezember 2000 die Einrichtung einer vorläufigen Stelle zur justiziellen Zusammenarbeit, PRO-EUROJUST genannt, die am 1. März 2001 ihre Arbeit aufgenommen hat. Diese Stelle soll bis zur Einrichtung von EUROJUST die Zusammenarbeit der Ermittlungsbehörden auf dem Gebiet der Bekämpfung der schweren grenzüberschreitenden Kriminalität verbessern und die Koordinierung von Ermittlungen anregen und verstärken. Ein Beschluss des Rates über die Einrichtung von EUROJUST soll bis Ende des Jahres 2001 verabschiedet werden.

Die Aufgabenstellung von EUROJUST führt möglicherweise dazu, dass eine europäische Großbehörde heranwächst, die Daten nicht nur über verdächtige Personen, sondern auch über Opfer und Zeugen sammeln soll, und damit zwangsläufig tief greifende Eingriffe in Bürgerrechte vornehmen würde. In diesem Falle käme als Grundlage für EUROJUST nur eine Konvention in Betracht, da für künftige Grundrechtseingriffe durch EUROJUST eine demokratische Legitimation notwendig wäre.

Mit Blick auf die sensiblen personenbezogenen Daten, die von EUROJUST erhoben, verarbeitet und genutzt werden sollen, und unter Berücksichtigung der eigenen Rechtspersönlichkeit von EUROJUST sind umfassende Datenschutzvorschriften erforderlich. Diese müssen sowohl Regelungen zur Verarbeitung, Speicherung, Nutzung, Berichtigung, Löschung als auch zum Auskunftsanspruch des Betroffenen sowie zu einer Kontrollinstanz von EUROJUST enthalten.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sind folgende datenschutzrechtliche Anforderungen an EUROJUST zu stellen:

Informationsaustausch mit Partnern

Der Informationsaustausch mit Partnern sollte EUROJUST dann erlaubt sein, wenn er zur Erfüllung seiner Aufgaben erforderlich ist. Bei Weiterleitung dieser Daten an Drittstaaten und -stellen ist die Zustimmung des Mitgliedstaates einzuholen, von dem diese Daten geliefert wurden. Sind personenbezogene Daten betroffen, so muss grundsätzlich eine Übereinkunft zwischen EUROJUST und der Partnerstelle über den Datenschutzstandard getroffen werden. Nur in absoluten Ausnahmefällen, die einer restriktiven Regelung bedürfen, sollte eine Datenübermittlung auch bei Fehlen einer solchen Vereinbarung zulässig sein.

Verarbeitung personenbezogener Daten

Der Katalog der personenbezogenen Daten, die automatisiert verarbeitet werden dürfen, ist streng am Maßstab der Erforderlichkeit und an den Aufgaben von EUROJUST zu orientieren. Eine zusätzliche Öffnungsklausel, die letztlich die Speicherung aller Daten zulassen würde, ist abzulehnen. Eine Verarbeitung der Daten von Opfern und Zeugen darf, wenn überhaupt erforderlich, nur unter einschränkenden Bedingungen vorgenommen werden.

Ermittlungsindex und Dateien

Der Ermittlungsindex sollte so ausgestaltet sein, dass es sich um eine reine Vorgangsverwaltung handelt. Sofern zusätzlich Arbeitsdateien geführt werden, sind sie genau zu bezeichnen.

Auskunftsrecht

Wenn EUROJUST Daten verarbeitet, die ursprünglich von einem Mitgliedstaat geliefert wurden, handelt es sich im Ergebnis um Daten von EUROJUST. Insofern ist ein eigener Auskunftsanspruch von Betroffenen gegenüber EUROJUST unverzichtbar. Für den Fall, dass im Strafverfolgungsinteresse oder aus sonstigen Gründen des Gemeinwohls von einer Auskunft an den Betroffenen abgesehen werden soll, muss eine Abwägung mit den Interessen des Betroffenen an einer Auskunftserteilung vorangegangen sein.

Änderung, Berichtigung und Löschung

Es sollte auch eine Regelung zur Sperrung von Daten aufgenommen werden, die dazu führt, dass Daten unter bestimmten Voraussetzungen nicht gelöscht, sondern lediglich gesperrt werden.

Speicherungsfristen

Sofern Daten nach Ablauf bestimmter sonstiger Fristen zu löschen sind, z. B. nach Ablauf der Verjährungsfrist einzelner Mitgliedstaaten, sollte sich die Speicherungsfrist bei EUROJUST nach der Frist des Mitgliedstaates richten, in dem sie am kürzesten ist, um eine mögliche Umgehung nationaler Löschungsfristen zu vermeiden. Die Prüffristen sollten zwei Jahre betragen und auch für Folgeprüfungen nicht länger sein.

Datensicherheit

Erforderlich sind konkrete Vorschriften zur Datensicherheit. Um den Text des Beschlusses nicht zu überfrachten, könnte eine Regelung entsprechend Artikel 22 der Verordnung EG 45/2001 oder § 9 BDSG vorgesehen werden.

Gemeinsame Kontrollinstanz

Die Erforderlichkeit einer gemeinsamen Kontrollinstanz für EUROJUST muss außer Frage stehen. Die Unabhängigkeit dieser gemeinsamen Kontrollinstanz ist bereits durch die personelle Zusammensetzung zu gewährleisten. Sowohl für die EUROJUST-Mitglieder als auch das Kollegium müssen die Entscheidungen der gemein samen Kontrollinstanz bindender Charakter haben.

Rechtsschutz

Dem Betroffenen ist ein angemessener Rechtsschutz gegenüber EUROJUST zu gewähren. Es sollte festgelegt werden, welche nationale oder supranationale Gerichtsbarkeit für Klagen auf Auskunft, Löschung, Berichtigung und Schadensersatz zuständig ist.

Rechtsetzungsbedarf

Zur Erfüllung seiner Aufgaben muss EUROJUST Auskünfte über strafrechtliche Ermittlungsverfahren einholen. Nach geltendem Recht (§ 474 StPO) können die Ermittlungsbehörden der Bundesrepublik Deutschland derartigen Ersuchen nicht stattgeben.

Darüber hinaus bedarf der Zugrif f des deutschen EUROJUST-Mitglieds auf das Bundeszentralregister und auf das Zentrale Staatsanwalt schaftliche Verfahrensregister einer eindeutigen gesetzlichen Grundlage.

Anlage 21 (zu Nr. 28.3)

Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. bis 26. Oktober 2001: Datenschutzrechtliche Anforderungen an den „Arzneimittelpass“ (Medikamentenchipkarte)

Vor dem Hintergrund der Lipobay-Diskussion hat das Bundesministerium für Gesundheit die Einführung eines „Arzneimittelpasses“ in Form einer (elektronisch nutzbaren) Medikamentenchipkarte befürwortet; auf der Karte sollen alle ärztlichen Verordnungen verzeichnet werden. Damit soll eine größere Transparenz der Arzneimittelverordnungen erreicht werden. Bisher ist nicht ansatzweise belegt, dass die bekannt gewordenen Gefahren für die Patientinnen und Patienten dadurch entstanden sind, dass verschiedene Ärztinnen und Ärzte ohne Kenntnis voneinander unverträgliche Medikamente verordnet hätten. Deswegen ist auch nicht ersichtlich, dass die aufgetretenen Probleme mit einem Arzneimittelpass hätten verhindert werden können.

Aus datenschutzrechtlicher Sicht bestehen erhebliche Bedenken gegen eine Medikamentenchipkarte als Pflichtkarte. Die Datenschutzbeauftragten begrüßen es daher ausdrücklich, dass der Gedanke einer Pflichtkarte fallen gelassen wurde. Die Patientinnen und Patienten würden sonst rechtlich oder faktisch gezwungen, die ihnen verordneten Medikamente und damit zumeist auch ihre Erkrankung bei jedem Arzt- und/oder Apothekenbesuch ohne ihren Willen zu offenbaren. Dies würde eine wesentliche Einschränkung des Arztgeheimnisses bewirken, das auch gegenüber anderen Ärztinnen und Ärzten gilt. Zudem würde sich dadurch das Vertrauensverhältnis, das für die Behandlung und für eine funktionierende Gesundheitsfürsorge insgesamt unabdingbar ist, grundlegend verändern. Darüber hinaus wäre das Einholen einer unbeeinflussten Zweitmeinung nahezu ausgeschlossen.

Die freie und unbeeinflusste Entscheidung der Patientinnen und Patienten über Einsatz und Verwendung der Karte muss gewährleistet werden (Grundsatz der Freiwilligkeit).

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits auf ihrer 47. Konferenz im März 1994 und auf ihrer 50. Konferenz im November 1995 zum freiwilligen Einsatz von Chipkarten im Gesundheitswesen Stellung genommen; deren Zulässigkeit wird dort von verschiedenen Bedingungen zur Sicherung des Persönlichkeitsrechts der Patientinnen und Patienten abhängig gemacht. Grundlegende Voraussetzung ist vor allem die freie Entscheidung der Betroffenen (auch als Versicherte). Sie müssen entscheiden können,

- ob ihre Daten auf einer Chipkarte gespeichert werden,
- welche ihrer Gesundheitsdaten auf die Karte aufgenommen werden,
- welche ihrer Daten auf der Karte wieder gelöscht werden,
- ob sie die Karte bei einem Arzt- oder Apothekenbesuch vorlegen und
- welche ihrer Daten sie im Einzelfall zugänglich machen (die Technik muss eine partielle Freigabe ermöglichen).

Die Verantwortung für die Wahrung der Arzneimittelsicherheit tragen grundsätzlich die Ärztinnen und Ärzte sowie die Apothekerinnen und Apotheker. Sie darf nicht auf die Betroffenen abgewälzt werden. Dies gilt auch, wenn sie von dem „Arzneimittelpass“ keinen Gebrauch machen.

Der Chipkarteneinsatz darf nicht zur Entstehung neuer zentraler Datensammlungen über Patientinnen und Patienten führen.

Datenschutzrechtlich problematisch wäre es, den „Arzneimittelpass“ auf der Krankenversichertenkarte gemäß § 291 SGB V zu implementieren. Eine solche Erweiterung wäre allenfalls vertretbar, wenn die „Funktion Krankenversichertenkarte“ von der „Funktion Arzneimittelpass“ informationstechnisch getrennt würde, sodass die Patientinnen oder Patienten bei einem Arzt- oder Apothekenbesuch nicht gezwungen werden, ihre gesamten Gesundheitsdaten ungewollt zu offenbaren. Ihre Entscheidungsfreiheit, wem gegenüber sie welche Gesundheitsdaten offenlegen, müsste also durch die technische Ausgestaltung der Karte gewährleistet sein.

Die Betroffenen müssen ferner das Recht und die Möglichkeit haben, ihre auf der Chipkarte gespeicherten Daten vollständig zu lesen.

Die Verwendung der Karte außerhalb des medizinischen Bereichs, z. B. durch Arbeitgeberinnen und Arbeitgeber oder Versicherungen, muss gesetzlich verboten und sanktioniert werden.

Anlage 22 (zu Nr. 10.2)

Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. bis 8. März 2002:
Neues Abrufverfahren bei den Kreditinstituten

Nach der Novelle des Gesetzes über das Kreditwesen soll die zuständige Bundesanstalt die von den Kreditinstituten vorzuhaltenden Daten, wer welche Konten und Depots hat, ohne Kenntnis der Kundinnen und Kunden zur eigenen Aufgabenerfüllung oder zugunsten anderer öf fentlicher Stellen abrufen können. Dies ist ein neuer Eingrif f in die Vertraulichkeit der Bankbeziehungen.

Dieser Eingriff in die Vertraulichkeit der Bankbeziehungen muss gegenüber den Kundinnen und Kunden zumindest durch eine aussagekräftige Information transparent gemacht werden. Die Konferenz fordert daher, dass zugleich mit der Einführung dieses Abrufverfahrens eine V erpflichtung der Kreditinstitute zur generellen Information der Kundinnen und Kunden vorgesehen wird und diese die Kenntnisnahme schriftlich bestätigen. Dadurch soll zugleich eine ef fektive Wahrnehmung des Auskunftsrechts der Kundinnen und Kunden gewährleistet werden.

Die Erweiterung der Pflichten de r Kreditinstitute, Kontenbewegungen auf die Einhaltung gesetzlicher Bestimmungen mithilfe von EDV-Programmen zu überprüfen, verpflichtet die Kreditinstitute außerdem zu einer entsprechend intensiven Kontenüberwachung (so genanntes „know your customer principle“). Die Konferenz der Datenschutzbeauftragten des Bundes und der Lände r fordert, dass die Überprüfung in einer Weise stattfindet, die ein datenschutzkonformes Vorgehen sicherstellt.

Anlage 23 (zu Nr. 11.3.4.1)

Entschließung zwischen der 63. und 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Mai 2002:
Geplanter Identifikationszwang in der Telekommunikation

Das Bundesministerium für Wirtschaft und Technologie hat einen Entwurf zur Änderung des Telekommunikationsgesetzes veröffentlicht. Der Entwurf hat das Ziel, jeden Anbieter, der geschäftsmäßig T elekommunikationsdienste erbringt, dazu zu verpflichten, Name n, Anschriften, Geburtsdaten und Rufnummern seiner Kundinnen und Kunden zu erheben. Die Kundinnen und Kunden werden verpflichtet, dafür ihren Personalausweis vorzulegen, dessen Nummer ebenfalls gespeichert werden soll. Die beabsichtigten Änderungen sollen in erster Linie dazu führen, auch Nutzerinnen und Nutzer von Prepaid-Karten (also die Erwerberinnen und Erwerber von SIM-Karten ohne Vertrag) im Mobilfunk erfassen zu können. Die erhobenen Daten sollen allein dem Zweck dienen, den Sicherheitsbehörden zum jederzeitigen Online-Abruf über die Regulierungsbehörde für T elekommunikation und Post bereitzustehen. Im gleichen Zuge sollen die Zugriffsmöglichkeiten der Sicherheitsbehörden auf diese Daten dadurch erheblich erweitert werden, indem auf die Kundendateien nach abstrakten Merkmalen zugegriffen werden kann.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen dieses Vorhaben ab. Unter der unscheinbaren Überschrift „Schließen von Regelungslücken“ stehen grundlegende Prinzipien des Datenschutzes zur Disposition. Kritikwürdig an dem geplanten Gesetz sind insbesondere die folgenden Punkte:

- Der geplante Grundrechtseingriff ist nicht erforderlich, um die Ermittlungstätigkeit der Sicherheitsbehörden zu erleichtern. Seine Eignung ist zweifelhaft: Auch die Gesetzesänderung wird nicht verhindern, dass Straftäterinnen und Straftäter bewusst und gezielt in kurzen Zeitabständen neue Prepaid-Karten erwerben, Strohleute zum Erwerb einsetzen, die Karten häufig – teilweise nach jedem Telefonat – wechseln oder die Karten untereinander tauschen. In der Begründung wird nicht plausibel dargelegt, dass mit dem geltenden Recht die Ermittlungstätigkeit tatsächlich behindert und durch die geplante Änderung erleichtert wird. Derzeit laufende Forschungsvorhaben beziehen diese Frage nicht mit ein.

- Der Entwurf widerspricht auch dem in den Datenschutzrichtlinien der Europäischen Union verankerten Grundsatz, dass Unternehmen nur solche personenbezogenen Daten verarbeiten dürfen, die sie selbst zur Erbringung einer bestimmten Dienstleistung benötigen.

- Die Anbieter würden eine Reihe von Daten auf V orrat speichern müssen, die sie selbst für den Vertrag mit ihren Kunden nicht benötigen. Die ganz überwiegende Zahl der Nutzerinnen und Nutzer von Prepaid-Karten, darunter eine große Zahl Minderjähriger, würde registriert, obwohl sie sich völlig rechtmäßig verhalten und ihre Daten demzufolge für die Ermittlungstätigkeit der Strafverfolgungsbehörden nicht benötigt werden. Das Anhäufen von sinn- und nutzlosen Datenhalden wäre die Folge.

- Die gesetzliche Verpflichtung, sich an dem Ziel von Datenvermeidung und Datensparsamkeit auszurichten, würde konterkariert. Gerade die Prepaid-Karten sind ein gutes praktisches Beispiel für den Einsatz datenschutzfreundlicher Technologien, da sie anonymes Kommunizieren auf unkomplizierte W eise ermöglichen. Die Nutzung dieser Angebote darf deshalb nicht von der Speicherung von Bestandsdaten abhängig gemacht werden.

- Mit der Verpflichtung, den Personalausweis vorzulegen, würden die Anbieter zusätzliche Informationen über die Nutzerinnen und Nutzer erhalten, die sie nicht benötigen, z. B. die Nationalität, Größe oder Augenfarbe. Die vorgesehene Pflicht, auch die Personalausweisnummern zu registrieren, darf auch künftig keinesfalls dazu führen, dass die Ausweisnummern den Sicherheitsbehörden direkt zum Abruf bereit gestellt werden und sie damit diese Daten auch für die V erknüpfung mit anderen Datenbeständen verwenden können.

- Auch Krankenhäuser, Hotels, Schulen und Hochschulen sowie Unternehmen und Behörden, die ihren Mitarbeiterinnen und Mitarbeitern das pr ivate Telefonieren gestatten, sollen verpflichtet werden, die Personalausweisnummern der Nutzerinnen und Nutzer zu registrieren.

- Die Befugnis, Kundendateien mit unvollständigen oder ähnlichen Suchbegriffen abzufragen, würde den Sicherheitsbehörden eine V ielzahl personenbezogener Daten unbeteiligter Dritter zugänglich machen, ohne dass diese Daten für ihre Aufgaben erforderlich sind. Die notwendige strikte Beschränkung dieser weit reichenden Abfragebefugnis durch Rechtsverordnung setzt voraus, dass ein entsprechender V erordnungsentwurf bei der Beratung des Gesetzes vorliegt.

Der Formulierungsvorschlag des Bundeswirtschaftsministeriums lässt eine Auseinandersetzung mit dem Recht auf informationelle Selbstbestimmung der Kundinnen und Kunden der T elekommunikationsunternehmen weitgehend vermissen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Gesetzgeber auf, auf die geplante Änderung des Telekommunikationsgesetzes zu verzichten und vor weiteren Änderungen die bestehenden Befugnisse der Sicherheitsbehörden durch unabhängige Stellen evaluieren zu lassen.

Anlage 24 (zu Nr. 11.3.3**)**

Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. bis 25. Oktober 2002 zu: Systematische verdachtslose Datenspeicherung in der Telekommunikation und im Internet

Gegenwärtig werden sowohl auf nationaler als auch auf europäischer Ebene Vorschläge erörtert, die den Datenschutz im Bereich der Telekommunikation und der Internetnutzung und insbesondere den Schutz des Telekommunikationsgeheimnisses grundlegend infrage stellen.

Geplant ist, alle Anbieter von Telekommunikations- und Multimediadiensten zur verdachtslosen Speicherung sämtlicher Bestands-, Verbindungs-, Nutzungs- und Abrechnungsdaten auf Vorrat für Mindestfristen von einem Jahr und mehr zu verpflichten, auch wenn sie für die Geschäftszwecke der Anbieter nicht (mehr) notwendig sind. Das so entstehende umfassende Datenreservoir soll dem Zugriff der Strafverfolgungsbehörden, der Polizei und des Verfassungsschutzes bei möglichen Anlässen in der Zukunft unterliegen. Auch auf europäischer Ebene werden im Rahmen der Zusammenarbeit der Mitgliedstaaten in den Bereichen „Justiz und Inneres“ entsprechende Maßnahmen – allerdings unter weit gehendem Ausschluss der Öffentlichkeit – diskutiert.

Die Datenschutzbeauftragten des Bundes und der Länder treten diesen Überlegungen mit Entschiedenheit entgegen. Sie haben schon mehrfach die Bedeutung des Telekommunikationsgeheimnisses als unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft hervorgehoben. Immer mehr menschliche Lebensäußerungen finden heute in elektronischen Netzen statt. Sie würden bei einer Verwirklichung der genannten Pläne einem ungleich höheren Überwachungsdruck ausgesetzt als vergleichbare Lebensäußerungen in der realen Welt. Bisher muss niemand bei der Aufgabe eines einfachen Briefes im Postamt seinen Personalausweis vorlegen oder in einer öffentlichen Bibliothek registrieren lassen, welche Seite er in welchem Buch aufschlägt. Eine vergleichbar umfassende Kontrolle entsprechender Online-Aktivitäten (E-Mail-Versand, Nutzung des WorldWideWeb), wie sie jetzt erwogen wird, ist ebenso wenig hinnehmbar.

Zudem hat der Gesetzgeber erst vor kurzem die Befugnisse der Strafverfolgungsbehörden erneut deutlich erweitert. Die praktischen Erfahrungen mit diesen Regelungen sind von unabhängiger Seite zu evaluieren, bevor weiter gehende Befugnisse diskutiert werden.

Die Konferenz der europäischen Datenschutzbeauftragten hat in ihrer Erklärung vom 11. September 2002 betont, dass eine flächendeckende anlassunabhängige Speicherung sämtlicher Daten, die bei der zunehmenden Nutzung von öffentlichen Kommunikationsnetzen entstehen, unverhältnismäßig und mit dem Menschenrecht auf Achtung des Privatlebens unvereinbar wäre. Auch in den Vereinigten Staaten sind vergleichbare Maßnahmen nicht vorgesehen.

Mit dem deutschen Verfassungsrecht ist eine verdachtslose routinemäßige Speicherung sämtlicher bei der Nutzung von Kommunikationsnetzen anfallender Daten auf Vorrat nicht zu vereinbaren. Auch die Rechtsprechung des Europäischen Gerichtshofs lässt eine solche Vorratsspeicherung aus Gründen bloßer Nützlichkeit nicht zu.

Die Konferenz fordert die Bundesregierung deshalb auf, für mehr Transparenz der Beratungen auf europäischer Regierungsebene einzutreten und insbesondere einer Regelung zur flächendeckenden Vorratsdatenspeicherung nicht zuzustimmen.

Anlage 25 (zu Nr. 17.2.1)

Beschluss der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 24. und 25. Oktober 2002 zum Umgang mit personenbezogenen Daten in Sachakten des Verfassungsschutzes

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass bei den von V erfassungsschutzämtern geführten Personen- und Sachakten Unterschiede bei der Löschung bzw . Vernichtung auftreten. Während Personenakten nach Ablauf der gesetzlichen Fristen – unter Beachtung archivrechtlicher Regelungen – regelmäßig gelöscht oder vernichtet werden, geschieht dies bei Sachakten, die in der Regel auch personenbezogene Daten enthalten, oftmals nicht. Dies darf aber nicht dazu führen, dass diese Daten – anders als die Daten in Personenakten – noch weiter verwandt werden dürfen.

Die Konferenz fordert, dass in Sachakten personenbezogene Angaben, die nicht mehr erforderlich sind, auch in Ländern ohne gesetzliches Löschungsgebot zumindest zu sperren sind.

Anlage 26 (zu Nr. 3.2.5)

Abfrage zur Umsetzung des Bundesdatenschutzgesetzes (BDSG)

Behörde

Name/ Bezeichnung:	
Straße	
PLZ/Ort	
Telefon/Telefax	
E-Mail-Adresse	
Internet-Adresse/URL	

Datenschutzbeauftragte(r)

Name	
Telefon-Nr.	
E-Mail-Adresse	
Name Abwesenheitsvertretung	
Telefon-Nr.	
E-Mail-Adresse	

Fragen: (Zutreffendes ggfls. durch Anklicken ankreuzen)

1. Die/der Datenschutzbeauftragte ist der Leiterin/dem Leiter der Behörde unmittelbar unterstellt ?	ja	nein
2. **wenn ja**:		
2.1 die Funktion ist als Stabsstelle eingerichtet ?	ja	nein
2.2 die Unterstellung unter die Leitung ist in anderer Weise sichergestellt, z. B. durch Ansiedelung im Referat bzw. der Organisationseinheit mit direkter Unterstellung unter die Leitung in der Funktion als Datenschutzbeauftragte(r)?	ja	nein

noch Anlage 26

3. Die unmittelbare Unterstellung unter die Leitung ist im Organigramm der Behörde kenntlich ?	ja	nein
4. Die Bestellung der/des Datenschutzbeauftragten wurde den Beschäftigten bekannt gegeben ?	ja	nein
5. Eine Bekanntmachung als Ansprechpartner für die Bürgerinnen und Bürger in Datenschutzfragen ist erfolgt ?	ja	nein
wenn ja,		
5.1 der/die Datenschutzbeauftragte ist in der Internetpräsentation der Behörde als Ansprechpartner in Datenschutzfragen benannt?	ja	nein
5.2 die Bekanntmachung erfolgte durch Pressemitteilung?	ja	nein
5.3 die Bekanntmachung erfolgte in sonstiger Weise?	ja	nein
6. Eine Entlastung ist für die Aufgabenwahrnehmung im Datenschutz wie folgt geregelt:		
6.1 Volle Entlastung für die Aufgabenwahrnehmung von anderen Aufgaben	ja	nein
6.2 Vereinbarte Entlastung von anderen Aufgaben im Umfang von (Angabe in %)		
Wenn **keine Entlastung** festgelegt wurde:	%	
6.3 Nach eigener Einschätzung durch den Datenschutzbeauftragten beträgt der durchschnittliche Anteil für die		

noch Anlage 26

Aufgabenwahrnehmung im Datenschutz (Angabe in %)	%
6.4 Es erfolgt eine Unterstützung des Datenschutzbeauftragten durch zugewiesene Mitarbeiter bzw. Hilfspersonal i.S.v. § 4f Abs. 5 BDSG?	Ja nein
7. Für wie viele Beschäftigte an wie vielen Standorten (mit Entfernungsangabe, wenn Standorte weit verteilt) ist der/die Datenschutzbeauftragte der Behörde zuständig?	
8. Zur Arbeitssituation der/des Datenschutzbeauftragten in meiner Behörde möchte ich auf folgendes ergänzend hinweisen:	

Anlage 27 (zu Nr. 21.2.1)

Rundschreiben des Bundesministeriums des Innern an die Obersten Bundesbehörden vom 30. Januar 2002, Az. D I 1 – 215 080-1/1: Hinweise zur Personalaktenführung

Der Bundesbeauftragte für den Datenschutz hat in seinem letzten Tätigkeitsberichten einige V ollzugsdefizite im Bereich des Personalaktenrechts moniert. V or diesem Hintergrund weise ich auf folgende, offensichtlich wiederholt verletzte Regeln der Personalaktenführung hin:

- Die Beihilfebearbeitung muss abgeschottet erfolgen. Insbesondere ist die zwingend als Teilakte zu führende Beihilfeakte von der übrigen Personalakte einer/eines Beschäftigten getrennt aufzubewahren (vgl. § 90a BBG)
- Gesundheitszeugnisse, psychologische und ärztliche Gutachten etc., die außerhalb der Beihilfebearbeitung angefordert oder vor gelegt worden sind, sind in einem verschlossenen Umschlag zur Grundakte zu nehmen (vgl. Rechtsgedanke des § 46a Abs. 2 Satz 1 BBG).
- Unterlagen zur V orbereitung und Entscheidung über Stellenbesetzungsverfahren einschließlich den Unterlagen über die Beteiligung der Personalvertretungen an solchen Maßnahmen sind nicht in den Personalakten der jeweiligen Bewerber/Bewerberinnen oder gar der letztlich ausgewählten Person zu führen, sondern sind in einer gesonderten Sachakte zusammenzufassen. Dieser Sachakte kommt selbst insoweit keine Personalaktenqualität zu, wie sie Personalaktendaten enthält (vgl. auch Gesetzesbegründung in Bundestagsdrucksache 12/544 Seite 1l und 16).

  Allerdings kann die Bewerbung einer/eines Beschäftigten auf einen Dienstposten als solche oder der Abdruck eines entsprechenden Bewerbungsschreibens sowie die Entscheidung, soweit sie ausschließlich eine Person betrifft, auch zu deren Personenakte genommen werden.
- Zur Sicherstellung eines umfassenden Einsichtsrechts der/des betroffenen Beschäftigten ist ein V erzeichnis aller Teil- und Nebenakten anzulegen und zur Grundakte zu nehmen (vgl. § 90 Abs. 2 Satz 4 BBG).
- Im Rahmen der laufenden Aktenbereinigung sind
  - Unterlagen aus der Personalakte zu entfernen und zu vernichten, die nicht Personalaktendaten im Sinne von § 90 Abs. 1 BBG sind. Gleiches gilt für so genannte „Vorakten“, d. h. Personalakten aus V ortätigkeiten bei anderen Dienstherren und/oder Behörden;
  - im Übrigen Unterlagen aus den V orakten in die entsprechenden Teile (Grund- oder Teilakten) der jeweiligen Personalakte einzuordnen;
  - die unterschiedlichen Au fbewahrungsfristen zu beachten und zu nutzen, vor allem
  - die Unterlagen über Beihilfen, Heilfürsorge, Heilverfahren, Unterstützungen, Erholungsurlaub, Erkrankungen, Umzugs- und Reisekosten nach Abschluss der Bearbeitung nur noch fünf Jahre aufzubewahren;
  - Unterlagen, aus denen die Art einer Erkrankung ersichtlich ist und die im Rahmen der Bearbeitung von Beihilfe, Heilfürsorge und Heilverfahren vor gelegt und/oder angefordert worden sind, unverzüglich der/dem Beschäftigten zurückzugeben.

Anlage 28 (zu Nr. 21.4)

Rundschreiben des Bundesbeauftragten für den Datenschutz an die Obersten Bundesbehörden vom 17. September 2002, Az. III – 460 – 1/20:
Abschottung der Beihilfestelle gegenüber der Personalverwaltung

In der Vergangenheit habe ich mich mehrfach zur Bearbeitung von Beihilfen sowie zur Abschottung der Beihilfebearbeitung von der übrigen Personalverwaltung geäußert; vgl. 15. Tätigkeitsbericht, Abschnitt 9.5.2.1; 16. Tätigkeitsbericht, Abschnitt 23.4.3; 17. Tätigkeitsbericht, Abschnitt 18.5; 18. Tätigkeitsbericht, Abschnitt 18.5.1.

Bei der Bearbeitung von Einzeleingaben habe ich festgestellt, dass Probleme bei der Abschottung der Beihilfebearbeitung dadurch entstehen können, dass in einer Organisationseinheit sowohl Beihilfen als auch die übrigen Personalausgaben bearbeitet werden. Derartige Probleme treten auch auf, wenn innerhalb einer Organisationseinheit bestimmte Mitarbeiter ausschließlich mit der Beihilfebearbeitung betraut sind.

In § 90a BBG sind folgende Regelungen zum Umgang mit Beihilfeakten getroffen worden:

- Unterlagen über Beihilfen sind stets als Teilakte zu führen.
- Diese Teilakte ist von der übrigen Personalakte getrennt aufzubewahren.
- Die Beihilfeakte soll in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden.
- Zugang zur Beihilfeakte sollen nur Beschäftigte dieser Organisationseinheit haben.
- Die Beihilfeakte darf für andere als für Beihilfezwecke nur verwendet oder weitergegeben werden, wenn der Beihilfeberechtigte und der bei der Beihilfegewährung berücksichtigte Angehörige im Einzelfall einwilligt, die Einleitung oder Durchführung eines im Zusammenhang mit einem Beihilfeantrag stehenden behördlichen oder gerichtlichen Verfahrens dies erfordert oder soweit es zur Abwehr erheblicher Nachteile für das Gemeinwohl, einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist.

Eine Einengung des Begriffs „übrige Personalverwaltung“, wie sie in der Begründung zu § 90a BBG enthalten ist (Personalverwaltung im engeren Sinn) kann im Hinblick auf die neueren Regelungen zum Umgang mit besonderen Kategorien personenbezogener Daten nicht vorgenommen werden; auf Artikel 8 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und auf § 3 Abs. 9 BDSG in der seit 23. Mai 2001 geltenden Fassung darf ich ausdrücklich hinweisen.

Aus den vorgenannten Gründen halte ich eine strikte Abschottung der Beihilfebearbeitung von der gesamten übrigen Personalverwaltung – also auch von der Bearbeitung der sonstigen Personalausgaben – für dringend erforderlich.

Folgende organisatorische Lösungen könnten dabei getroffen werden:

a) Die Beihilfebearbeitung wird von einer Stelle außerhalb der Personalverwaltung der Behörde wahr genommen.

b) Die Beihilfebearbeitung für die Beschäftigten wird einer anderen Behörde übertragen, die die Aufgabenerledigung ggf. für mehrere Behörden zentral, einheitlich und dadurch möglicherweise sogar ökonomischer wahrnimmt.

Beide Lösungen halte ich für datenschutzgerecht. Soweit mir bekannt ist, ist die Bearbeitung von Beihilfen bereits von einzelnen Bundesbehörden auf andere Bundesbehörden übertragen worden.

Über meine Auffassung zur Beihilfebearbeitung werde ich auch in meinem 19. Tätigkeitsbericht berichten.

In diesem Zusammenhang weise ich vorsorglich darauf hin, dass Beihilfedaten nach § 90g Abs. 2 BBG automatisiert nur im Rahmen ihrer Zweckbestimmung und nur von den übrigen Personaldateien technisch und organisatorisch getrennt verarbeitet und genutzt werden dürfen.

Ich würde es begrüßen, wenn Sie die Organisation der Beihilfebehörde in Ihrem Geschäftsbereich unter Berücksichtigung meiner Auffassung überprüfen und – falls erforderlich – entsprechend ändern würden.

Ich wäre Ihnen dankbar, wenn Sie die Behörden Ihres Geschäftsbereichs sowie die Ihrer Rechtsaufsicht unterliegenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts unterrichten würden.

Anlage 29 (zu Nr. 28.1)

Gemeinsame Erklärung des Bundesministeriums für Gesundheit und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen

Das Bundesministerium für Gesundheit und die V erbände und Organisationen auf Spitzenebene sprechen sich für einen verstärkten Einsatz von Telematikanwendungen im Gesundheitswesen aus.

Sie stimmen darin überein, da ss damit die gemeinsamen Zielsetzungen

- Verbesserung der Qualität de r medizinischen V ersorgung, u. a. der Arzneimittelsicherheit,
- Verbesserung patientenorientierter Dienstleistungen,
- Stärkung der Eigenverantwortung, Mitwirkungsbereitschaft und –initiative der Patienten,
- Steigerung der Wirtschaftlichkeit und Leistungstransparenz im Gesundheitswesen,
- Optimierung von Arbeitsproz essen und Bereitstellung von aktuellen Steuerungsinformationen

erreicht werden können.

Um diese Zielsetzungen zu erre ichen, sollen in einem Kooperationsverbund eine neue T elematikinfrastruktur auf der Basis einer einheitlichen Rahmenarchitektur entwickelt, die elektronische Kommunikation verbessert bzw . eingeführt (eRezept, eArztbrief) und die Krankenversichertenkarte zusätzlich als Gesundheitskarte angeboten werden. Die Gesundheitskarte soll auch Werkzeug für den datengeschützten Zugriff auf personenbezogene Gesundheitsdaten sein. Die Gesundheitskarte soll den europäischen Notfalldatensatz des Patienten, seine persönliche Identifikation/Authentifizierung sowie Verweisfunktionen u. a. auf die Arzneimitteldokumentation und das elektr onische Zuzahlungsmanagement des Patienten enthalten.

Das BMG begrüßt in diesem Zusammenhang die Initiative der Selbstverwaltung, eine T elematikplattform für das Gesundheitswesen in Deutschland aufzubauen und die modellhafte Erprobung einer weiterentwickelten Krankenversichertenkarte als Gesundheitskarte mitzutragen.

Diese Entwicklung greift auf europäischer Ebene auf die Beschlüsse von Barcelona, auf das Aktionsprogramm der Bundesregierung zur Informationsgesellschaft und seinen Fortschrittsbericht sowie auf die Vorarbeiten des Aktionsforums Telematik im Gesundheitswesen zurück.

Das Bundesministerium für Gesundheit und die V erbände und Organisationen auf Spitzenebene werden bei der Vorbereitung und Durchführung von Projekten eng zusammenarbeiten und gemeinsame Zielse tzungen unterstützen. Dabei wird angestrebt, die unterschiedlichen technischen Lösungsansätze der Modellprojekte er gebnisoffen nach gemeinsam festzulegenden Kriterien im Hinblick auf Kosten und Akzeptanz zu evaluieren und gewonnene Erfahrungen zu nutzen, um zu einer flächendeckenden T elematikplattform für das deutsche Gesundheitswesen zu gelangen.

Modellversuche dürfen nur unter strenger Beachtung des Datenschutzes und des Selbstbestimmungsrechtes des Patienten durchgeführt werden.

Leistungserbringer haben bereits heute eine Reihe von Dokumentationspflichten zu erfüllen. Diese bleiben unberührt. Es besteht Einigkeit, dass die mit dem Ausbau zur Gesundheitskarte verbundene Speicherung und V erarbeitung der Gesundheitsdaten als freiwilliges Angebot an die Versicherten zu gestalten ist, insbesondere

- dass die Datenhoheit der Patienten und der Grundsatz der Freiwilligkeit der Sp eicherung von Gesundheitsdaten bewahrt wird;
- dass Patienten entscheiden können, welche ihrer Gesundheitsdaten aufgenommen und welche gelöscht werden;
- dass Patienten entscheiden können, ob und welche Daten sie einem Leistungserbringer zugänglich machen;
- dass keine zentral gespeicherten Datensammlungen über Patientinnen und Patienten entstehen;
- dass Patienten und Versicherte das Recht haben, über sie gespeicherte Daten vollständig zu lesen;
- dass die Verwendung der gespeicherten Patientendaten selbstverständlich nur innerhalb des gesetzlichen Rahmens unter W ahrung des bestehenden Schutzniveaus (z. B. Beschlagnahmeschutz in der Arztpraxis) erlaubt ist.

Im Rahmen der Gesundheitskarte und des Aufbaus der Telematikplattform werden das eR ezept, der eArztbrief und die Arzneimitteldokumentation als Einstieg in die elektronische Patientenakte auf der Grundlage einer geeigneten Informations-, Kommunikations- und Sicherheitsinfrastruktur eingeführt.

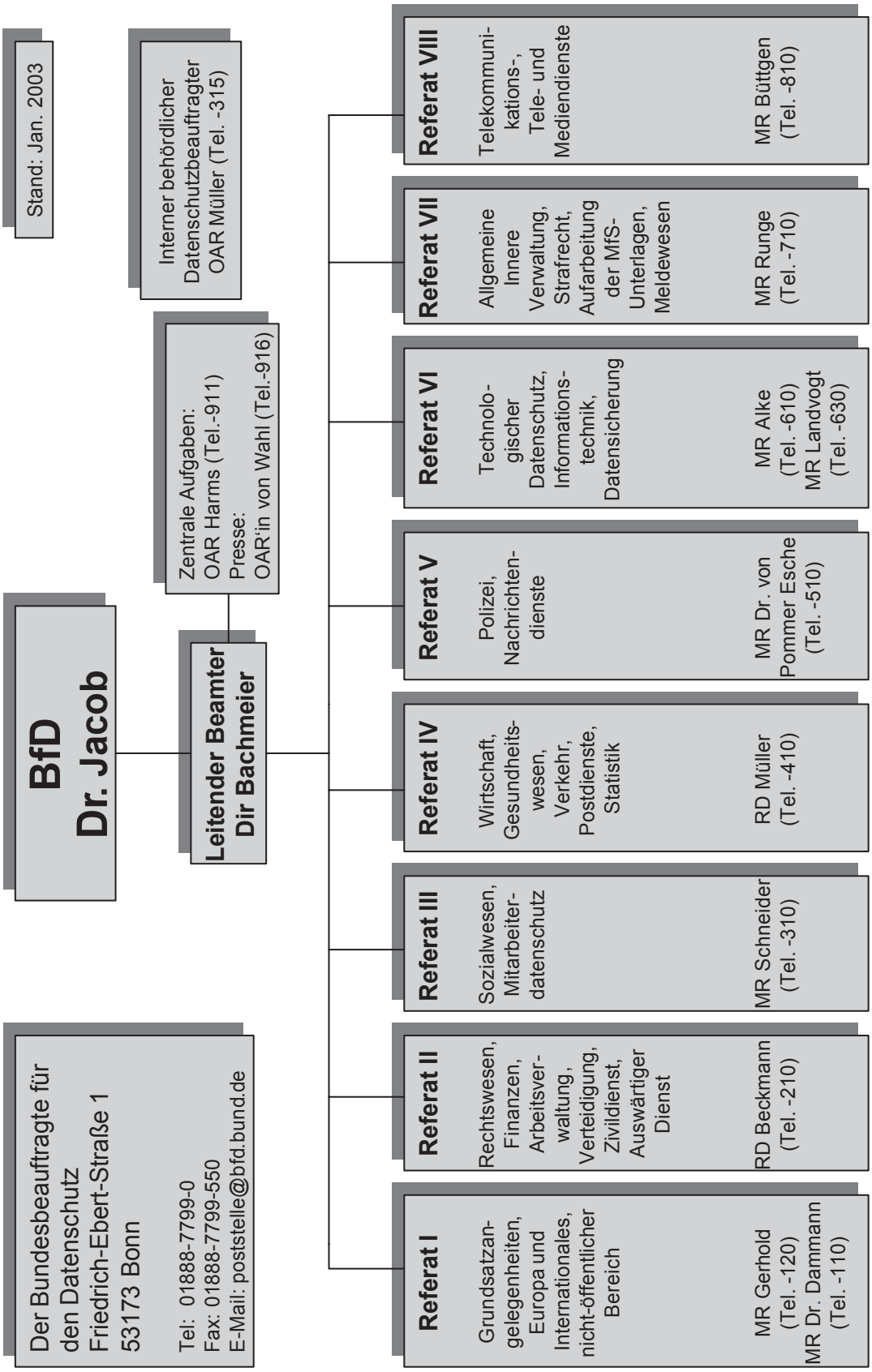
Die Projekte sollen nach dem Grundkonsens dieser Erklärung in gegenseitiger Abst immung unter Einbeziehung des Datenschutzbeauftragten begleitet werden, internationalen Normen entsprechen und interoperabel (unter anderem mit der Health Professional Card) angelegt sein. Dabei sollen im Rahmen des stufenweisen Aufbaus der T elematikplattform das eRezept im Zusammenwirken mit der bisherigen Krankenversichertenkarte und Serverstrukturen und die Gesundheitskarte mit erweiterten Anwendungen in einem Kooperationsverbund erprobt, evaluiert und eingeführt werden. Für das Vorhaben wird der Dialog mit allen gesellschaftlichen Kräften, insbesondere den Patienten, gesucht.

Die Beteiligten sind sich einig, dass sie aufgrund des erwarteten gemeinsamen Nutzens die weiteren Fragen der Ausgestaltung, Funktionalisierung, Standardisierung und Finanzierung gemeinsam lösen wollen und zu diesem Zwecke eine Steuerungsgruppe einrichten.

noch Anlage 29

Diese Erklärung wird getragen von:

dem Bundesministerium für Gesundheit
dem Verband der Angestellten-Krankenkassen e.V.
dem Arbeiter-Ersatzkassen-Verband e.V.
der Kassenärztlichen Bundesvereinigung
der Bundesvereinigung Deutscher Apothekerverbände
der Bundesärztekammer – Arbeitsgemeinschaft der Deutschen Ärztekammern
der Deutschen Krankenhausgesellschaft
dem AOK Bundesverband
dem BKK Bundesverband
der Kassenzahnärztlichen Bundesvereinigung
dem Verband der privaten Krankenversicherung
dem Bundesverband der landwirtschaftlichen Krankenkassen
der Bundesknappschaft Bochum
dem IKK-Bundesverband
dem Hauptverband der gewerblichen Berufsgenossenschaften e.V.
der See-Krankenkasse
und dem Aktionsforum Telematik im Gesundheitswesen


Stand: Jan. 2003
Interner behördlicher Datenschutzbeauftragter OAR Müller (Tel. -315)
Zentrale Aufgaben: OAR Harms (Tel.-911) Presse: OAR'in von Wahl (Tel.-916)
BfD Dr. Jacob
Leitender Beamter Dir Bachmeier
Der Bundesbeauftragte für den Datenschutz Friedrich-Ebert-Straße 1 53173 Bonn
Tel: 01888-7799-0 Fax: 01888-7799-550 E-Mail: poststelle@bfd.bund.de
Referat I
Grundsatzangelegenheiten, Europa und Internationales, nicht-öffentlicher Bereich
MR Gerhold (Tel. -120) MR Dr. Dammann (Tel. -110)
Referat II
Rechtswesen, Finanzen, Arbeitsverwaltung, Verteidigung, Zivildienst, Auswärtiger Dienst
RD Beckmann (Tel. -210)
Referat III
Sozialwesen, Mitarbeiterdatenschutz
MR Schneider (Tel. -310)
Referat IV
Wirtschaft, Gesundheitswesen, Verkehr, Postdienste, Statistik
RD Müller (Tel. -410)
Referat V
Polizei, Nachrichtendienste
MR Dr. von Pommer Esche (Tel. -510)
Referat VI
Technologischer Datenschutz, Informationstechnik, Datensicherung
MR Alke (Tel. -610) MR Landvogt (Tel. -630)
Referat VII
Allgemeine Innere Verwaltung, Strafrecht, Aufarbeitung der MfS-Unterlagen, Meldewesen
MR Runge (Tel. -710)
Referat VIII
Telekommunikations-, Tele- und Mediendienste
MR Büttgen (Tel. -810)

Sachregister

Als Fundstelle ist die Nummer des Abschnitts oder des Beitrages angegeben, in dem der Begriff verwendet wird.

Abkürzungsverzeichnis/Begriffe

AA	Auswärtiges Amt
ABl.	Amtsblatt der Europäischen Gemeinschaften
Abs.	Absatz
AFIS	Automatisiertes Fingerabdruck-Identifizierungssystem
AG	Aktiengesellschaft: aber auch: Arbeitsgruppe
AGB	Allgemeine Geschäftsbedingungen
AIS	Arbeitgeber-Informations-Service
AK II	Arbeitskreis II „Innere Sicherheit“ der IMK
AKE	Arbeitsgruppe Koordinierte Ermittlungen
AO	Abgabenordnung
APC	Arbeitsplatzcomputer
ASYLON	Asyl-online
AsylVfG	Asylverfahrensgesetz
AuslG	Ausländergesetz
AuslDatV	Ausländerdateien-Verordnung
AVmG	Altersvermögensgesetz
AWG	Außenwirtschaftsgesetz
AZR	Ausländerzentralregister
AZR-Gesetz	Ausländerzentralregistergesetz
BA	Bundesanstalt für Arbeit
BAFl	Bundesamt für die Anerkennung ausländischer Flüchtlinge
BAN	Bundesgrenzschutzaktennachweis
BAR	Bundesarbeitsgemeinschaft für Rehabilitation
BAZ	Bundesamt für den Zivildienst
BBG	Bundesbeamtengesetz
BBfA	Bundesbeauftragter für Asylangelegenheiten
BDO	Bundesdisziplinarordnung
BDSG	Bundesdatenschutzgesetz
BfA	Bundesversicherungsanstalt für Angestellte
BfD	Bundesbeauftragter für den Datenschutz
BfD/BA	Beauftragter für den Datenschutz der Bundesanstalt für Arbeit
BfDBw	Beauftragter für den Datenschutz der Bundeswehr
BfF	Bundesamt für Finanzen
BFiO	Büro Führungskräfte zu internationalen Organisationen
BfV	Bundesamt für Verfassungsschutz
BG	Berufsgenossenschaft
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGS	Bundesgrenzschutz
BGSG	Bundesgrenzschutzgesetz
BITKOM	Bundesverband Informationswirtschaft, Kommunikation und neue Medien e.V.
BK	Bundeskanzleramt
BKA	Bundeskriminalamt
BKA-Gesetz (BKAG)	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
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
BMWA	Bundesministerium für Wirtschaft und Arbeit
BMWi	Bundesministerium für Wirtschaft und Technologie
BND	Bundesnachrichtendienst
BNDG	Gesetz über den Bundesnachrichtendienst

BSHG	Bundessozialhilfegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStU	Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BVA	Bundesverwaltungsamt, aber auch: Bundesversicherungsamt
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfSchG	Bundesverfassungsschutzgesetz
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungssammlung des Bundesverwaltungsgerichts
BvS	Bundesanstalt für vereinigungsbedingte Senderaufgaben
BWpV	Bundeswertpapierverwaltung
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
bzw.	beziehungsweise
ca.	circa
CC	Common Criteria for Information Technology Security Evaluation
CC IVBB	Competence Center Informationsverbund Berlin-Bonn
CD/CD-ROM	Compact Disc-Read Only Memory
CERT	Computer Emergency Response Team
CEN	Comité Européen de Normalisation
CJ-PD	Projektgruppe Datenschutz des Europarates
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
d. h.	das heißt
DAV	Dienstanschlussvorschriften
DDR	Deutsche Demokratische Republik
DHCP	Dynamic Host Configuration Protocol
DHS	Deportment of Home Security
DMP	Disease-Management-Programme
DNA	Desoxyribonoclein acid (acid=Säure)
DNS	Domain Name Service
drbd	Distributed Replicated Block Device
Drs.	Drucksache
DTAG	Deutsche Telekom AG
Düsseldorfer Kreis	oberstes Koordinierungsgremium der obersten Aufsichtsbehörden für den Datenschutz
DV/dv	Datenverarbeitung
ECHELON	Abhörsystem der National Security Agency
E-Commerce	Elektronic Commerce/Elektronischer Handel
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft(en)
EG-ZIS	Europäisches Zollinformationssystem
E-Mail	Electronic Mail
EP	Europäisches Parlament
EStG	Einkommensteuergesetz
EU	Europäische Union
Eurodac	Europäisches daktyloskopisches Fingerabdrucksystem zur Identifizierung von Asylbewerbern
Europol	Europäisches Polizeiamt
etc.	et cetera
e.V.	eingetragener Verein
EVN	Einzelverbindungsnachweis
EWG	Europäische Wirtschaftsgemeinschaft
EWR	Europäischer Wirtschaftsraum
f.	folgend
FAG	Fernmeldeanlagengesetz
FATF	Financial Action Task Force

FeV	Fahrerlaubnis-Verordnung
ff.	folgende
FIU	Financial Intelligence Unit
FÜV	Fernmelde-Überwachungs-Verordnung
G 10	Artikel 10-Gesetz
GBA	Generalbundesanwalt beim Bundesgerichtshof
gem.	gemäß
GG	Grundgesetz
ggf.	gegebenenfalls
GGO	Gemeinsame Geschäftsordnung der Bundesministerien
GmbH	Gesellschaft mit beschränkter Haftung
GPL	GNU General Public License
GwG	Geldwäschegesetz
Hartz-Kommission	Kommission „Moderne Dienstleistungen am Arbeitsmarkt“
HmbGVBl.	Hamburgisches Gesetz- und Verordnungsblatt
HPC	Health Professional Card
HTML	Hypertext Markup Language-Standardisierte Seitenbeschreibungssprache für Seiten im Internet/Intranet
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
IAO	International Awareness Office
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ICHEIC	International Commission on Holocaust Era Insurance Claims
IKPO	Internationale Kriminalpolizeiliche Organisation
IMK	Ständige Konferenz der Innenminister und -senatoren der Länder
IMSI	International Mobile Subscriber Identity
INPOL	Informationssystem der Polizei
InsO	Insolvenzordnung
IP	Internet Protocol
IP6	Internet Protocol Version 6
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Informationstechnik
ITSEC	Information Technology Security Evaluation Criteria
ITF	Internet Task Force
IuK	Informations- und Kommunikationstechnologie
IVBB	Informationsverbund Berlin-Bonn
KAN	Kriminalaktennachweis
KBA	Kraftfahrt-Bundesamt
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung
KOM	Europäische Kommission
KSV	Kreditschutzvereinigung GmbH
LAN	Local Area Network
LBA	Luftfahrt-Bundesamt
LfD	Landesbeauftragter für den Datenschutz
LG	Landgericht
LKA	Landeskriminalamt
LuftVG	Luftverkehrsgesetz
LuftVZO	Luftverkehrs-Zulassungs-Ordnung
LuftVZÜV	Luftverkehr-Zuverlässigkeitsüberprüfungsverordnung

m.E.	meines Erachtens
MAD	Militärischer Abschirmdienst
MADG	Gesetz über den MAD
MAdLAN	Multilinguales Adresssystem im Local Area Network
MARIS	Migration Asyl Reintegrationssystem (Workflowsystem)
MDK	Medizinischer Dienst der Krankenversicherung
MoZArT	Modellprojekte zur Verbesserung der Zusammenarbeit zwischen Arbeitsämtern und Trägern der Sozialhilfe
MRRG	Melderechtsrahmengesetz
NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
Nrn.	Nummern
o. g.	oben genannt
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OLG	Oberlandesgericht
OP-Protokoll	Operationsprotokoll
OpenLdap	ein freier Server auf der Grundlage des Lightweight Directory access Protocol (LDAP)
OSS	Open Source Software
PC	Personalcomputer
PDSV	Postdienstunternehmen-Datenschutzverordnung
PEPSY	Personalverwaltungssystem des Auswärtigen Amtes
PERFIS	Personalführungs- und Informationssystem der Bundeswehr
PersVG	Personalvertretungsgesetz
PET	Privacy Enhancing Technology
PIN	persönliche Identifikationsnummer
PKGr	Parlamentarisches Kontrollgremium
PKGrG	Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes-Kontrollgremium
PostG	Postgesetz
Protection Profile	Schutzprofil
PSA	Personal-Service-Agentur
PZD	Personenzentraldatei
RegTP	Regulierungsbehörde für Telekommunikation und Post
Reha	Rehabilitation
Residenture	eine mit Billigung der Regierung des Einsatzlandes eingerichtete Auslandsdienststelle eines Nachrichtendienstes
S.	Seite
s.	siehe
SaD	System zur automatisierten Datenschutzprüfung
s. o.	siehe oben
s. u.	siehe unten
SAP R/3HR	Datenbanksystem der Fa. SAP (Personalinformationssystem)
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 IX	Sozialgesetzbuch Neuntes Buch (Rehabilitation und Teilhabe behinderter Menschen)

SGB X	Sozialgesetzbuch Zehntes Buch (Sozialverwaltungsverfahren und Sozialdatenschutz)
SGB XI	Sozialgesetzbuch Elftes Buch (Soziale Pflegeversicherung)
SigG	Signaturgesetz
SIRENE	Supplementary Information Request at the National Entry (=Nationales Büro im Rahmen der Schengen-Kooperation)
SIS	Schengener Informationssystem
SMS	Short Message Service
sog.	sogenannt
SSL	Secure Socket Layer
STADA	Staatsangehörigkeitsdatei
Stasi	Staatssicherheitsdienst der ehemaligen DDR
StDAV	Steuerdaten-Abruf-Verordnung
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StUG	Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz)
StVBG	Steuerverkürzungsbekämpfungsgesetz
SÜG	Sicherheitsüberprüfungsgesetz
TB	Tätigkeitsbericht
TBG	Terrorismusbekämpfungsgesetz
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikations-Datenschutzverordnung
THA	Treuhandanstalt
TK	Telekommunikation
TK-Anlage	Telekommunikationsanlage
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung
TKV	Telekommunikations-Kundenschutzverordnung
TMS	Travel-Management-System
u. a.	unter anderem
u. Ä.	und Ähnliches
u. U.	unter Umständen
UKlaG	Unterlassungsklagengesetz
UKPV	Unabhängige Kommission zur Überprüfung des Vermögens der Parteien und Massenorganisationen der DDR
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
usw.	und so weiter
UVT	Unfallversicherungsträger
UWG	Gesetz gegen den unlauteren Wettbewerb
VDR	Verband Deutscher Rentenversicherungsträger
vgl.	vergleiche
v.H.	von Hundert
VwVfG	Verwaltungsverfahrensgesetz
WAP	Wireless Application Protocol
WEWIS	Wehrersatzwesen-Informationssystem
WP	Working Paper
www	World wide web
z. B.	zum Beispiel
z. T.	zum Teil
ZDG	Zivildienstgesetz
ZDPersAV	Verordnung über die Führung der Personalakten im Zivildienst – Zivildienst-Personalaktenverordnung –

ZERV	Zentrale Ermittlungsstelle der Kriminalpolizei für Regierungs- und Vereinigungskriminalität beim Polizeipräsidenten in Berlin
ZFnrG	Zollfahndungsneuregelungsgesetz
ZIS	Zollinformationssystem
ZKA	Zollkriminalamt
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister
ZWG	Zollverwaltungsgesetz

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
18.	1999–2000	14/5555

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 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