

Ein am 22. Juli 2004 im BMI geführtes Gespräch mit den US-amerikanischen und britischen Streitkräften, an dem ich beteiligt war, hat dabei im Wesentlichen zu folgenden erfreulichen Ergebnissen geführt:

- Sicherheitsüberprüfungen entsprechend § 8 SÜG – einfache Sicherheitsüberprüfung (Ü 1) – nur für zivile Bedienstete und Personen, die die Liegenschaften täglich oder häufig betreten müssen (keine Besucher);
- Keine Einbeziehung von Ehegatten oder Lebenspartnern, lediglich Erfassung ihrer persönlichen Daten nach deren Zustimmung;
- Keine Sicherheitsüberprüfung von Personen mit Dienstaussweisen von Bundes- oder Landesbehörden;
- Durchführung der Sicherheitsüberprüfung ausschließlich unter Mitwirkung des BfV (Zentralstellenfunktion);
- Verwendung der Daten nur für Zwecke der Sicherheitsüberprüfung; keine Weiterleitung der Daten an Dritte, insbesondere in die USA bzw. nach Großbritannien;
- Rechtliches Gehör vor einer negativen Entscheidung;
- Grundsätzliche Pflicht zur Auskunftserteilung über gespeicherte Daten;
- Speicherung der Daten nur solange sie benötigt werden, d.h. solange das Beschäftigungsverhältnis andauert (GB) bzw. bis zwei Jahre nach Beendigung des Beschäftigungsverhältnisses (US);
- Wiederholungsüberprüfung nach zehn Jahren (GB) bzw. fünf Jahren (US) für Mitglieder von sog. Sonderprogrammen (z. B. Wachpersonal);
- Verwendung eines der Sicherheitserklärung (Ü 1) entsprechenden Formulars mit einer dem deutschen Recht entsprechenden Einwilligungserklärung.

Ob die vom BMI erstellte und mit mir abgestimmte Niederschrift, über diese Besprechung von US-amerikanischer und britischer Seite offiziell bestätigt worden ist, hat mir das BMI bislang noch nicht mitgeteilt.

Nach dieser Besprechung wurden mir Hinweise bekannt, dass die Sicherheitsüberprüfungen – zumindest durch die US-Streitkräfte – entgegen dem am 22. Juli 2004 erzielten Besprechungsergebnis nach wie vor nach dem bisherigen, nicht dem deutschen Recht entsprechenden Verfahren durchgeführt werden. Insbesondere soll die Einwilligungserklärung nicht die Anforderungen des § 4a BDSG erfüllen. Weiterhin sollen über die nach dem SÜG zulässigen Daten hinaus personenbezogene Daten abgefragt und über die Mitwirkung des BfV hinaus zusätzliche eigene Überprüfungen durch die US-Streitkräfte durchgeführt werden. Ferner soll die Einverständniserklärung den Hinweis enthalten, dass erhobene Daten an das US-Verteidigungsministerium und an Stellen außerhalb des US-Verteidigungsministeriums weitergegeben werden können. Hierzu habe ich das BMI um Stellungnahme und Klärung gebeten. Sollten sich diese Hinweise bestätigen, stünde dies in eklatantem Widerspruch zu dem am 22. Juli 2004 erzielten Besprechungsergebnis. Eine Stellungnahme des BMI lag mir bei Redaktionsschluss allerdings noch nicht vor.

6 Innere Verwaltung, Statistik

6.1 Zuwanderung

6.1.1 Das Zuwanderungsgesetz

Das am 1. Januar 2005 in Kraft getretene Zuwanderungsgesetz vom 30. Juli 2004 (BGBl. I S. 1950) bringt datenschutzrechtlich Licht und Schatten.

Wesentlicher Bestandteil des Zuwanderungsgesetzes ist das Aufenthaltsgesetz (AufenthG), das das Ausländergesetz (AuslG) ablöst. In ihm wurden die bisherigen Datenübermittlungsregelungen der §§ 75 bis 80 AuslG mit geringen Änderungen übernommen. Weitgehend gelten jedoch die datenschutzrechtlichen Regelungen des BDSG und der Landesdatenschutzgesetze. Die Datenschutzvorschriften des AufenthG kommen nur zur Anwendung, soweit sie von den allgemeinen Regelungen abweichen. Einerseits freut mich zwar diese gesetzestechnische Lösung. Auf der anderen Seite bedeuten die Regelungen im AufenthG, dass z. T. ohne stichhaltige Begründungen zu Lasten der Betroffenen von den datenschutzfreundlicheren Regelungen im allgemeinen Datenschutzrecht durch das AufenthG abgewichen wird. Dazu gehört z. B. die Regelung über den Ausschluss des Widerspruchsrechts nach § 20 Abs. 5 BDSG durch § 91 Abs. 3 AufenthG. Die in der amtlichen Begründung zu dieser Vorschrift (Bundestagsdrucksache 15/420 S. 98) gegebene Erläuterung, wonach ansonsten die Gefahr einer „erheblichen Verzögerung“ bestünde und der „Gesichtspunkt der Verfahrensbeschleunigung im Ausländerrecht von besonderer Bedeutung“ sei, überzeugt mich nicht. Mit dem Zuwanderungsgesetz ist am 1. Januar 2005 auch die Durchführungsverordnung zum Zuwanderungsgesetz vom 25. November 2004 (BGBl. I S. 2945) in Kraft getreten, deren wesentlicher Bestandteil die Aufenthaltsverordnung (AufenthV) ist.

Besonders bedeutsam aus Sicht des Datenschutzes ist, dass dem aus dem Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl) hervorgegangenen Bundesamt für Migration und Flüchtlinge (BAMF) u. a. folgende Aufgaben übertragen wurden:

- Entwicklung und Durchführung von Integrationskursen für Ausländer und Spätaussiedler;
- Führung des Ausländerzentralregisters (die tatsächliche Datenverarbeitung erfolgt allerdings als Datenverarbeitung im Auftrag weiterhin durch das Bundesverwaltungsamt, § 1 Abs. 1 Ausländerzentralregistergesetz – AZRG);
- Wissenschaftliche Forschung über Migrationsfragen;
- Koordinierung der Information über Arbeitsmigration zwischen Ausländerbehörden, der Bundesagentur für Arbeit und den deutschen Auslandsvertretungen.

Die Förderung von Integrationskursen durch den Bund, die ich mir im Berichtszeitraum angesehen habe, wird von einer Förderung der Träger von Integrationsveranstaltungen in eine Förderung der Teilnehmer an Integrationskursen umgestellt (vgl. Nr. 6.1.2.2).

Die von mir in den letzten beiden Tätigkeitsberichten (19. TB Nr. 34.1; 18. TB Nr. 5.1.3) geforderte Rechtsgrundlage für ausländerrechtliche Vermerke in ausländischen Pässen findet sich in § 99 Abs. 1 Nr. 10 AufenthG und § 56 Nr. 8 AufenthV. Damit sind auch die Kontrollstempel („Eintragungen über die Einreise, die Ausreise, das Antreffen im Bundesgebiet und über Entscheidungen der zuständigen Behörden zu solchen Papieren“) umfasst.

Inhaltlich unverändert geblieben ist im AufenthG die Regelung über die Beteiligung der Sicherheitsbehörden und Nachrichtendienste im Visumverfahren und bei der Erteilung von Aufenthaltserlaubnissen (§ 73 AufenthG). Für die Visumverfahren selbst und für die Erteilung von Aufenthaltserlaubnissen hat es dagegen eine Reihe von Änderungen gegeben. Dies gilt insbesondere für Fragen der Identitätsfeststellung sowie der Datenerfassung und -speicherung. So sind z. B. in der AufenthV Regelungen über die Speicherung von Daten von Bürgern aufgenommen worden, die visumpflichtige Ausländer einladen („Einladerdateien“). Es handelt sich dabei jedoch nicht um eine Zentraldatei, sondern um die Erfassung der Einladernamen bei den jeweiligen Auslandsvertretungen. Diese Daten müssen bei Gewährung des Visums ein Jahr nach Ablauf, wenn das Visum versagt wird, fünf Jahre nach der Entscheidung über den Antrag gelöscht werden. Forderungen nach Einführung einer zentralen Einladerzentraldatei lehne ich nach wie vor als unverhältnismäßig ab (vgl. 17. TB Nr. 5.5).

Über die Anwendung mit der durch das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361) in das AuslG eingeführten Regelung (§ 64a) durch die Sicherheitsbehörden im Konsultationsverfahren nach Artikel 17 Schengener Durchführungsübereinkommen – SDÜ berichte ich an anderer Stelle (vgl. Nr. 5.2.6).

6.1.2 Bundesamt für Migration und Flüchtlinge

Anlässlich meiner Beratungs- und Kontrollbesuche beim Bundesamt stellte ich einen erfreulich hohen Datenschutzstandard fest.

Bislang war das Asylverfahren die Hauptaufgabe des BAFl. Das hat sich mit dem Inkrafttreten des Gesetzes zur Steuerung und Begrenzung der Zuwanderung und zur Regelung des Aufenthalts und der Integration von Unionsbürgern und Ausländern – Zuwanderungsgesetz – geändert (BGBl. I S. 1950).

Dem Bundesamt wurden am 1. Januar 2005 neue Aufgaben auf dem Gebiet der Migration und Integration von Unionsbürgern und Ausländern übertragen. Hierzu gehören u. a. die Entwicklung und Durchführung von Integrationskursen (Sprach- und Orientierungskurse) für Zuwanderer, die Neuausrichtung der Migrationsberatung und die Förderung von Projekten zur sozialen und gesellschaftlichen Eingliederung der in Deutschland dauerhaft lebenden Spätaussiedler und Ausländer. Das Bundesamt wird zu einer zentralen Steuerungsstelle in Zuwanderungs- und Migrationsfragen umgestaltet.

Meine Beratungs- und Kontrollbesuche haben sich sowohl mit dem Asylverfahren als auch mit Zuwanderungs- und Migrationsfragen beschäftigt.

6.1.2.1 Alternierende Telearbeit für Einzelentscheider

Im 19. Tätigkeitsbericht (Nr. 7.1.3) hatte ich das Pilotprojekt „Alternierende Telearbeit für Einzelentscheider“ dargestellt. Das Pilotprojekt war zunächst auf zwei Jahre befristet und endete mit Ablauf des Jahres 2002. Nach dem mir im Anschluss daran vorgelegten Erfahrungsbericht bestand bei den Beschäftigten der übereinstimmende Wunsch diese weiterzuführen. Zur besseren Auslastung der telearbeitenden Einzelentscheider bat mich das Bundesamt um Prüfung, ob eine Ausweitung der (enggefassten) Dienstanweisung möglich wäre, ohne die berechtigten Interessen der Asylbewerber zu vernachlässigen.

Die Bitte war schon anlässlich eines Beratungs- und Kontrollbesuches im November 2002 an mich herangetragen worden. Um die Praktikabilität prüfen zu können, ließ ich mir sowohl Akten vorlegen, die aus Sicht des Einzelentscheiders und des Referatsleiters telearbeitgeeignet waren, als auch solche, die die Telearbeit ausschlossen. Ich habe festgestellt, dass gemäß den engen Regelungen in der Dienstanweisung viele Akten nicht telearbeitgeeignet waren. Die Dienstanweisung wurde daraufhin in Abstimmung mit mir überarbeitet und das Pilotprojekt um ein Jahr verlängert. Danach ist nun u. a. auch das Korrekturlesen sämtlicher Anhörungen und Bescheide des Einzelentscheiders am Telearbeitsplatz unter der Bedingung möglich, dass die am Telearbeitsplatz korrekturzulesenden Schriftstücke keine sog. Kopfleiste (Name, Geburtsdatum, Wohnort, Rechtsanwalt) sowie (im Text) keine schützenswerten Daten Dritter aus dem Herkunftsland des Asylbewerbers enthalten.

Der Erfahrungsbericht, den das Bundesamt im Frühjahr 2004 vorgelegt hat, kommt zu positiven Ergebnissen. Durch die Anpassung der Dienstanweisung konnte die Praktikabilität der Telearbeit für Einzelentscheider mit dem berechtigten Datenschutzinteresse der Asylbewerber in Einklang gebracht werden.

6.1.2.2 Das Bundesamt und die Integrationskursverordnung

Im Herbst 2004 habe ich einen Beratungs- und Kontrollbesuch beim Bundesamt im Rahmen einer Ablaufkontrolle mit den Schwerpunkten Integrationsmaßnahmen, Integrationsprogramme und Rückkehrförderung auf der Grundlage der zu dem Zeitpunkt aktuellen Rechtslage durchgeführt. Der Besuch sollte insbesondere zur Information im Hinblick auf die geplante Verordnung über die Durchführung von Integrationskursen für Ausländer und Spätaussiedler (Integrationskursverordnung) dienen. Die Ressortabstimmung wurde vom BMI unmittelbar im Anschluss an meine Kontrolle eingeleitet, sodass die Ergebnisse meines Besuches in die Beratungen einfließen konnten. Die Verordnung ist am 17. Dezember 2004 veröffentlicht worden (BGBl. I S. 3370 ff.). Wie die Regelungen in der Praxis umgesetzt werden können, bleibt

zunächst abzuwarten; ggf. müssen sie evaluiert werden. Ich werde die Entwicklungen beobachten.

Die kontrollierten Arbeitsabläufe entsprachen grundsätzlich den datenschutzrechtlichen Anforderungen. Das Bundesamt hat meine Hinweise und Anmerkungen umgesetzt und will sie auch in die Entwicklung und Einführung von IT-Anwendungen zur Unterstützung der Aufgabenerledigung einfließen lassen.

Die Auswirkungen der Integrationskursverordnung, die zum 1. Januar 2005 in Kraft getreten ist, auf die von mir kontrollierten Arbeitsabläufe bleiben abzuwarten. Ich habe dem Bundesamt meine Beratung bei der Umsetzung der Anforderungen, die sich aus dem Zuwanderungsgesetz für das Bundesamt ergeben, angeboten.

6.1.3 Passsammelstelle und Fundpapierdatenbank beim Bundesverwaltungsamt

Aufgefundene ausländische Ausweisdokumente werden beim Bundesverwaltungsamt gesammelt.

Häufig stellt sich die Frage, wie mit Pässen und anderen Personaldokumenten umgegangen werden soll, die von Ausländern in Deutschland verloren und hier aufgefunden wurden. Zu diesem Zweck hat das Bundesverwaltungsamt (BVA) eine Passsammelstelle eingerichtet, der ich im Juni 2003 einen Kontroll- und Beratungsbesuch abstattete.

Das Verfahren richtet sich nach den „Richtlinien über die Behandlung ausländischer Pässe, Passersatzpapiere, Personalausweise und Personenstandsurkunden“ des BMI. Diese sehen vor, dass die vorgenannten Personaldokumente von Ausländern, die nicht im Ausländerzentralregister erfasst sind und für die keine zuständige (Ausländer-)Behörde festgestellt werden kann, als Fundsache dem BVA (an die sog. **Passsammelstelle**) zuzuleiten sind. Das BVA gibt die Ausweisdokumente nach Prüfung an die jeweils zuständige konsularische oder diplomatische Vertretung des ausstellenden Staates in der Bundesrepublik Deutschland ab. Sofern der ausstellende Staat nicht ermittelt werden kann, werden die Ausweisdokumente für die Dauer von zehn Jahren beim BVA aufbewahrt. Dem BVA werden monatlich rund 200 Personaldokumente zugeleitet.

Bei der Kontrolle wurden sowohl Verfahrensmängel im Verantwortungsbereich des BVA als auch solche, die in der Zusammenarbeit mit dem BND begründet sind, festgestellt. Letztere konnten beim BVA nicht abschließend (auf-)geklärt werden. Ich habe das zum Anlass genommen, auch beim BND einen Beratungs- und Kontrollbesuch durchzuführen. Aufgrund dieser Kontrolle wurde das Verfahren geändert und datenschutzkonform ausgestaltet (vgl. Nr. 5.7.3).

Die Kontrolle ergab, dass in der Passsammelstelle auch Daten aus dem Ausländerzentralregister, die nicht zum Betroffenen gehören, in den Vorgängen abgelegt wurden. Dies widerspricht § 10 Abs. 3 Ausländerzentralregistergesetz, wonach die ersuchende Stelle solche Daten aus dem Ausländerzentralregister unverzüglich zu löschen und entsprechende Aufzeichnungen zu vernichten hat. Ich habe aber von einer Beanstandung abgesehen, weil

das BVA seinerzeit die umgehende Beachtung der Vorschrift zugesagt hatte. Die entsprechenden Daten werden nunmehr unverzüglich vernichtet.

Im September 2004 hat die Bundesregierung einen Gesetzentwurf zur Änderung des Aufenthaltsgesetzes und weiterer Gesetze eingebracht, wonach ein Teil der bisher der Passsammelstelle zugeleiteten Personaldokumente in einer Datenbank (**Fundpapierdatenbank**) beim BVA gespeichert werden soll. Durch den Einsatz biometrischer Verfahren, insbesondere der Gesichtserkennung (vgl. auch Nr. 4.2.2), soll eine Zuordnung von aufgefundenen ausländischen Ausweispapieren zu Ausländern erleichtert werden. Dabei handelt es sich um Dokumente von Staatsangehörigen, die beim Überschreiten der Außengrenzen im Besitz eines Visums sein müssen, sowie von Personen aus Staaten, die von der Visumpflicht befreit sind. Ein Teil der Aufgaben der Passsammelstelle würde dadurch hinfällig. Dieser sollen künftig nur noch die aufgefundenen Ausweisdokumente von visafrei einreisenden Ausländern zugeleitet werden. Die dem BVA zugeleiteten Ausweisdokumente dieses Personenkreises sollen in der neu einzurichtenden Fundpapierdatenbank erfasst werden.

Gegen die Schaffung einer Fundpapierdatenbank habe ich keine grundsätzlichen Bedenken. Allerdings hat der Bundesrat den Gesetzentwurf abgelehnt, nachdem im Vermittlungsausschuss kein Kompromiss gefunden werden konnte. Strittig war aber nicht die Fundpapierdatenbank, zumal die Innenministerkonferenz das BMI gebeten hatte, einen Gesetzentwurf für eine dateigestützte Passabgleichstelle vorzulegen. Ich gehe daher davon aus, dass die Bundesregierung erneut einen entsprechenden Gesetzentwurf einbringen wird.

6.1.4 Gehören Daten von Staatsangehörigen eines Mitgliedstaates der EU ins Ausländerzentralregister?

Bislang werden Staatsangehörige eines Mitgliedstaates der EU, die ihren Wohnsitz in der Bundesrepublik Deutschland haben, im Ausländerzentralregister gespeichert. Aus meiner Sicht verstößt dies gegen europäisches Datenschutzrecht.

Die Frage, ob Daten von Staatsangehörigen eines Mitgliedstaates der EU mit Wohnsitz in der Bundesrepublik Deutschland im Ausländerzentralregister (AZR) gespeichert werden dürfen, ist nach wie vor nicht abschließend geklärt. Ende 2000 stammte jeder vierte im AZR gespeicherte Ausländer aus einem Mitgliedstaat der EU. Mit der Erweiterung der EU zum 1. Mai 2004 hat sich diese Zahl weiter erhöht.

Bereits 1999 wurde mir vom Europäischen Parlament eine entsprechende Petition zur Stellungnahme übersandt (vgl. 18. TB Nr. 5.1.1). Meine Prüfung ergab, dass die generelle Speicherung gegen die EG-Datenschutzrichtlinie 95/46/EG verstößt. Nur in Einzelfällen, dann wenn es um die Registrierung ausländerrechtlicher Entscheidungen wie Ausweisung oder Abschiebung geht, kann eine Speicherung zulässig sein. Das BMI hat mir daraufhin mitgeteilt, es prüfe, ob eine Änderung des AZRG in das Gesetzgebungsverfahren zum Zuwanderungsgesetz aufgenommen werden könnte, mit der die Speicherung

von Daten über Unionsbürger im AZR aufgehoben würde (vgl. 19. TB Nr. 34, dort Nr. 6). Dies ist nicht geschehen (vgl. auch Nr. 6.1.1).

Zwar sind im Entwurf des Gesetzes zur Änderung des Aufenthaltsgesetzes und weiterer Gesetze (Bundestagsdrucksache 15/3784) auch umfangreiche Änderungen des AZRG vorgesehen. Dennoch wurde meiner wiederholten Forderung im Rahmen der Abstimmung dieses Entwurfes, die generelle Speicherung der Daten von Unionsbürgern im AZR auszuschließen, nicht entsprochen.

Die Europäische Kommission hat am 7. Juli 2004 ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet. Sie vertritt die Auffassung, dass eine generelle Verarbeitung personenbezogener Daten von Unionsbürgern in einem zentralen (Ausländer-)Register nicht notwendig ist im Hinblick auf Artikel 7 Buchst. e) der EG-Datenschutzrichtlinie. Ferner widerspricht die Verarbeitung dieser Daten in einem gesonderten Register für Ausländer dem Nichtdiskriminierungsprinzip aufgrund der Staatsangehörigkeit für jene, die ihr Recht ausüben, sich frei als Unionsbürger auf dem Gebiet eines Mitgliedstaates aufzuhalten, und verstoße damit gegen Artikel 12, 17 und 18 des EG-Vertrages. Das AZRG stehe daher in diesen Punkten nach Auffassung der Kommission nicht im Einklang mit dem EG-Vertrag und der europäischen Datenschutzrichtlinie.

Ich teile diese Auffassung und werde das Verfahren ebenso aufmerksam verfolgen wie das aufgrund des Vertragsverletzungsverfahrens zur Zeit ruhende verwaltungsrechtliche Verfahren, mit dem der Petent die Löschung seiner Daten aus dem AZR verfolgt.

6.1.5 Eurodac – eine Erfolgsgeschichte?

Seit 15. Januar 2003 ist Eurodac in Betrieb.

Das **Europäische dactyloskopische** Fingerabdrucksystem Eurodac, über dessen Regelungen ich berichtete (vgl. 17. TB Nr. 5.7; 19. TB Nr. 7.1.1), hat planmäßig am 15. Januar 2003 seine Tätigkeit aufgenommen.

Ich habe dies zum Anlass genommen, mich bei den für die nationale Umsetzung der Eurodac-Verordnung zuständigen Stellen über die Arbeitsabläufe zu informieren. Dazu habe ich die Zentrale des Bundesamtes für Migration und Flüchtlinge (früher: Bundesamt für die Anerkennung ausländischer Flüchtlinge) sowie eine Außenstelle und das BKA besucht. Gegen die Arbeitsabläufe zur Erstellung, Bearbeitung und Übermittlung der sog. Eurodac-Treffer bestehen keine Bedenken. Die zentrale Datenbank in Luxemburg wird durch den europäischen Datenschutzbeauftragten kontrolliert (vgl. Nr. 3.2.3)

Erfahrungsgemäß weckt eine solche Datenbank Begehrlichkeiten. So hat Deutschland bereits im Herbst 2001 vorgeschlagen, die in der zentralen Eurodac-Datenbank gespeicherten Daten auch für polizeiliche Zwecke zu nutzen. Die Einbeziehung des Eurodac-Datenbestandes würde dabei die Zuordnung polizeilicher Erkenntnisse zu Fingerabdrücken von Personen, die sich in anderen Mitgliedstaaten als Asylbewerber aufhalten, ermöglichen. Hierdurch würde die Strafverfolgung erheblich erleichtert

und auch Sicherheitsrisiken könnten bereits im Vorfeld erkannt werden.

Eine solche Nutzung der Daten für polizeiliche Zwecke ist aufgrund der strikten Zweckbindung der Eurodac-Verordnung an das Dubliner Übereinkommen nicht möglich. Die Daten dürfen nur zur Bestimmung des für die Prüfung des Asylantrages zuständigen Mitgliedstaates bzw. nur zur entsprechenden Prüfung des Asylantrages verwendet werden. Für darüber hinausgehende Vorstellungen wäre eine Änderung der Eurodac-Verordnung notwendig.

Ich werde die Entwicklungen in diesem Bereich weiter verfolgen.

6.2 Biometrie in Ausweisdokumenten

Biometrische Verfahren sollen – trotz erheblicher Zweifel an der Zuverlässigkeit der vorgesehenen Technik – in Ausweisdokumente integriert werden.

Das Lichtbild ist seit jeher Bestandteil von Ausweisdokumenten. Durch die Einbringung eines digitalisierten Lichtbildes wird es grundsätzlich möglich sein, nach der abgebildeten Person in einer Datenbank zu suchen. Fingerabdrücke waren in anderen Staaten bereits Bestandteil von Ausweisdokumenten (vgl. 19. TB, Nr. 2.2.3, 2.3.4).

Die Notwendigkeit der Einführung elektronisch auswertbarer biometrischer Merkmale wird vor allem mit Sicherheitsgewinnen begründet:

- Die Fälschungssicherheit der Papiere werde erhöht.
- Die Verwendung falscher oder gestohlener Dokumente werde unterbunden.
- Kontrollen in sicherheitsempfindlichen Bereichen, etwa an Flughäfen, würden beschleunigt.

Auf Basis der inzwischen gewonnenen Erkenntnisse habe ich Zweifel, ob die biometriegestützten Reisedokumente tatsächlich die versprochenen Sicherheitsgewinne mit sich bringen, denn

- bereits heute ist die Fälschungssicherheit deutscher Pässe und Personalausweise weitestgehend gewährleistet (vgl. 19. TB Nr. 7.2),
- wenn biometriegestützte Pässe in Staaten ohne geordnetes Personenstandswesen ausgestellt werden, kann die Ausstellung von biometriegestützten Dokumenten auf andere Personen nicht verhindert werden,
- angesichts hoher Fehlerquoten bei automatisierten Auswertungsverfahren ist mit erheblichen individuellem Nachbereitungsaufwand zu rechnen.

Durch das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361) waren in das Passgesetz (§ 4 Abs. 3 und 4 PassG) und in das Personalausweisgesetz (§ 1 Abs. 4 und 5 PersauswG) Regelungen eingefügt worden, die prinzipiell die Aufnahme biometrischer Merkmale in Ausweisdokumente vorsehen. Auf ihrer 63. Sitzung im März 2002 hatte sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit dem Thema befasst und eine Entschließung verabschiedet, in der sie bestimmte Anforderungen an die

Einführung biometrischer Merkmale in Ausweispapieren stellt (vgl. Kasten zu Nr. 6.2).

Im nationalen wie im internationalen Bereich gab es in der Folgezeit zahlreiche Aktivitäten zur Einführung biometrischer Merkmale in Ausweisdokumente. Maßgebliche Impulse kommen dabei von der Internationalen Zivilluftfahrt-Organisation (International Civil Aviation Organization – ICAO), einer Sonderorganisation der Vereinten Nationen (VN), die sich bereits seit Jahren mit der Einführung biometrischer Verfahren in Ausweisdokumente befasst. Seit September 2000 favorisiert die ICAO das Gesichtserkennungsverfahren. Nach dem 11. September 2001 wurden die Arbeiten deutlich intensiviert. Die ICAO und die von ihr beauftragte Internationale Standardisierungsorganisation ISO arbeiten anderen nationalen Standardisierungsorganisationen zu, wie z. B. dem Deutschen Institut für Normung e. V. An den Vorgaben der ICAO sowohl hinsichtlich der Frage, welche biometrischen Merkmale in Ausweisdokumente eingeführt werden sollen, als auch hinsichtlich der Nutzung bestimmter Techniken orientieren sich sowohl die Europäischen Kommission und der Europäische Rat sowie die Bundesregierung. Die Vorgaben der ICAO bilden damit – obwohl sie völkerrechtlich nicht verbindlich sind – einen faktischen internationalen Standard bei der Einführung biometrischer Merkmale und Verfahren.

Hinsichtlich des praktischen Nutzens biometrischer Merkmale – sowohl zur Verifikation wie auch zur Identifikation – sei nur auf die Vielzahl technischer Probleme hingewiesen, die zum großen Teil noch nicht gelöst sind. Der vom Büro für Technikfolgenabschätzung (TAB) dem Deutschen Bundestag vorgelegte Bericht verweist darauf, dass für die prinzipiell gut erforschten biometrischen Anwendungen von digitaler Hand- und Iriserkennung die Erkennungsleistung bislang noch nicht großflächig getestet wurden. Aber auch bei den genauer untersuchten Fingerabdruck- und Gesichtserkennungsverfahren ist festzuhalten, dass im Masseneinsatz immer noch eine sehr große Anzahl von Personen falsch erkannt wird. So können Fingerabdrücke nicht bei allen Menschen abgenommen werden.

Eine hohe Falscherkennung bzw. Falschakzeptanz wären bei einem biometrischen System unter Sicherheitsaspekten Ausschlusskriterien, d. h. diese Verfahren wären für einen Masseneinsatz ungeeignet. Fehlerhafte Rückweisungen hätten hingegen für die Betroffenen nicht nur diskriminierende Auswirkungen und würden zu einer schlechten Akzeptanz des Verfahrens beim Nutzer führen. Die Falschrückweisungsproblematik lässt sich auch nicht durch Kombination verschiedener biometrischer Merkmale – etwa Fingerabdruck und Gesichtserkennung – lösen; vielmehr würde möglicherweise nunmehr eine Person bereits dann zurückgewiesen, wenn nur ein biometrisches Merkmal nicht passt. Im Ergebnis würde sich dadurch die Falschrückweisungsquote eventuell noch erhöhen.

Das TAB hat in seinem Bericht zudem auf den hohen finanziellen Aufwand bei der Einführung biometrischer Verfahren hingewiesen.

Hinweis: „Zweiter Sachstandbericht – Biometrie und Ausweisdokumente“ des TAB, Bundestagsdrucksache 15/4000, www.tab.fzk.de/de/projekt/zusammenfassung/ab93.pdf

Kasten zu Nr. 6.2

63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 7. und 8. März 2002

EntschlieÙung: Biometrische Merkmale in Personalausweisen und Pässen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eingehend über Geeignetheit, Erforderlichkeit und Angemessenheit der beabsichtigten Einführung biometrischer Merkmale in Ausweisen und Pässen diskutiert. Sie hat ein Positionspapier des Arbeitskreises Technik, das detaillierte Prüfpunkte für die Erprobungsphase einer solchen Maßnahme nennt, zustimmend zur Kenntnis genommen. Für den Fall, dass das Vorhaben trotz noch bestehender Bedenken realisiert werden sollte, hat sie übereinstimmend folgende Anforderungen formuliert:

1. Fälschliche Zurückweisungen berechtigter Personen durch automatisierte Personenerkennungssysteme sind auch bei ständiger Verbesserung der Technik prinzipiell nicht zu vermeiden. Es dürfen deshalb nur Verfahren in Betracht gezogen werden, bei denen die Fehlerquote zumutbar gering ist. In Fehlerfällen muss dafür Sorge getragen werden, dass eine die Betroffenen nicht diskriminierende rasche Aufklärung erfolgt.
2. Zu berücksichtigen ist, dass bei der Anwendung biometrischer Verfahren Zusatzinformationen anfallen können (z. B. Krankheits-, Unfall-, Beschäftigungsindikatoren). Es muss sichergestellt werden, dass die gespeicherten und verarbeiteten Daten keine Rückschlüsse auf zusätzliche personenbezogene Merkmale erlauben.
3. Systeme, die biometrische Daten aus Ausweisen ohne Kenntnis der Betroffenen verarbeiten (sog. passive Systeme), sind abzulehnen.
4. Der Gesetzgeber hat die Verwendung biometrischer Daten in Ausweisen und Pässen grundsätzlich auf die Feststellung beschränkt, dass die dort gespeicherten Daten mit den Merkmalen der jeweiligen Ausweisinhaber und -inhaberinnen übereinstimmen; dies muss erhalten bleiben. Die Verwendung der biometrischen Merkmale für andere öffentliche Zwecke (außer der gesetzlich zugelassenen Verwendung aus dem Fahndungsbestand) wie auch für privatrechtliche Zwecke (Versicherung, Gesundheitssystem) ist auszuschließen. Deshalb hat der Gesetzgeber zu Recht die Einrichtung zentraler Dateien ausgeschlossen. Diese gesetzgeberische Entscheidung darf nicht durch den Aufbau dezentraler Dateien umgangen werden.
5. Die Entscheidung über das auszuwählende biometrische Erkennungssystem verlangt ein abgestimmtes europäisches Vorgehen.

6.2.1 Die EU-Pass-Verordnung

Künftig soll der Pass der EU-Bürger einen RFID-Chip enthalten, in dem auch biometrische Merkmale gespeichert werden.

Am 13. Dezember 2004 hat der Rat der Europäischen Union (Ministerrat) die „Verordnung (EG) Nr. 2252/2004 des Rates über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten“ beschlossen (EU-Pass-Verordnung – ABl. Nr. L 385 vom 29. Dezember 2004, S. 1). Mit dieser Verordnung werden die Pässe in den Mitgliedstaaten der Europäischen Union weiter vereinheitlicht. Die beschlossene EU-Pass-Verordnung zielt auf die Schaffung einheitlicher Normen für Sicherheitsmerkmale sowie auf die Einführung biometrischer Merkmale in die Pässe der EU-Bürger.

Bei der Diskussion über die Einführung biometrischer Merkmale in die Pässe der EU-Bürger bestand zwischen den EU-Staaten Einigkeit hinsichtlich des digitalisierten Lichtbildes als aufzunehmendes biometrisches Merkmal. Allerdings gab es unterschiedliche Auffassungen darüber, in welcher Form die Lichtbilddaten in einen in den Pass integrierten Chip aufgenommen werden sollen: lediglich als Template – d. h. in Form eines elektronischen Referenzmusters des Lichtbildes – oder als Rohdaten. Da man sich auf europäischer Ebene weitgehend an die Vorgaben der ICAO halten will, hat man sich für die Speicherung des Rohdatensatzes entschieden.

Die Diskussion über ein zweites biometrisches Merkmal konzentrierte sich rasch auf den digitalen Fingerabdruck. Umstritten war allerdings, ob dieses zweite biometrische Merkmal verbindlich vorgeschrieben oder fakultativ bleiben sollte. Während einige Mitgliedstaaten im Sommer 2004 noch mit ihrem Ansinnen, das zweite biometrische Merkmal verbindlich vorzuschreiben, gescheitert waren, führten interne Beratungen der sog. G-5-Gruppe (Deutschland, Frankreich, Italien, Spanien, Vereinigtes Königreich) dazu, dass der Ministerrat für Justiz und Inneres bei seiner Sitzung am 25. Oktober 2004 den bereits im Konsultationsverfahren im Europäischen Parlament (EP) befindlichen Verordnungsvorschlag ohne weitere Begründung dahingehend änderte, den digitalisierten Fingerabdruck als weiteres verbindliches Merkmal vorzusehen. Nur wenige Tage vor Verabschiedung der Stellungnahme des EP wurde diesem daher ein geänderter Verordnungsvorschlag übersandt. Das EP hat diesen neuen Vorschlag zur Kenntnis genommen, seine Stellungnahme aber zu dem alten Vorschlag abgegeben, der lediglich die fakultative Aufnahme von digitalisierten Fingerabdrücken vorsah.

Ein weiteres datenschutzrechtliches Problem war in den Erwägungsgründen des Verordnungsentwurfs nur am Rande erwähnt worden. Dort war unter dem Aspekt „langfristige Perspektive“ die Schaffung eines europäischen Passregisters, d. h. einer europäischen Zentraldatei mit den Angaben zu allen in den EU-Mitgliedstaaten herausgegebenen Pässen angesprochen. Hiergegen hat sich nicht nur die Art. 29-Gruppe mit einem Schreiben vom 18. August 2004 an den Vorsitzenden des Rates, den Präsidenten der Europäischen Kommission, den Präsidenten

des EP und weitere europäische Stellen gewandt. Auch das EP hat sich in seiner Stellungnahme vom 2. Dezember 2004 ausdrücklich gegen eine zentrale Datenbank der Pässe und Reisedokumente ausgesprochen.

Am 13. Dezember 2004 hat der Ministerrat die EU-Pass-Verordnung beschlossen, ohne inhaltlich die Stellungnahme des EP in wesentlichen Teilen zu berücksichtigen. Die Art. 29-Gruppe unterstützt die Position des EP und fordert, dass

- in den Verordnungstext ein ausdrückliches Verbot einer zentralen Datenbank aufgenommen wird,
- die biometrischen Daten nur verwendet werden dürfen, um die Echtheit des Dokuments und die Identität des Inhabers mittels direkt verfügbarer vergleichbarer Merkmale zu prüfen (Verifikation), wenn das Vorzeigen des Passes gesetzlich vorgeschrieben ist,
- auf dem Pass keine weiteren Daten als die gesetzlich zugelassenen gespeichert werden,
- der Zweck, zu dem die Daten aus dem Pass gelesen, gespeichert, verändert oder gelöscht werden dürfen, ebenso konkret bestimmt sein soll, wie die staatlichen Stellen, die die Daten lesen, speichern, verändern oder löschen dürfen.

Außerdem halten es alle Datenschutzkontrollinstanzen in den Mitgliedstaaten der EU für wünschenswert, wenn der in der EU-Pass-Verordnung vorgesehene Ausschuss bei seinen Beratungen vor der Beschlussfassung von Beauftragten der Art. 29-Gruppe datenschutzrechtlich beraten wird, damit die festzulegenden technischen Spezifikationen von vornherein datenschutzrechtlichen Anforderungen genügen.

6.2.2 Neue Techniken für Reisedokumente bei der Bundesdruckerei GmbH

Bei der Bundesdruckerei GmbH habe ich mich über die technischen Möglichkeiten der Einführung biometrischer Merkmale in Pässe und andere Ausweispapiere informiert.

Mit der Einführung biometrischer Merkmale in den Reispass aufgrund der EU-Pass-Verordnung (vgl. Nr. 6.2.1) soll eine neue Technik in die Reisedokumente eingeführt werden. Dabei bleiben Zweifel, ob die Einführung biometrischer Merkmale einen Gewinn für die Fälschungssicherheit von Reisedokumenten bedeutet. Soweit eine zusätzliche Fälschungssicherheit für Reisedokumente angesprochen wird, wird dies eher auf die Einführung einer Chiptechnologie zurückzuführen sein. Dabei soll aber nicht verkannt werden, dass schon die bisherigen deutschen Reispässe und Personalausweise ein sehr hohes technisches Niveau im Hinblick auf Fälschungssicherheit haben.

Bei Besuchen in der Bundesdruckerei habe ich mich erkundigt, welche technischen Möglichkeiten zur Implementierung eines Chips in den Reispass bestehen. Deutlich wurde dabei, dass nach den Vorgaben der ICAO nur ein 2D-Barcode oder ein sogenannter RFID-Chip (Radio Frequency Identification-Chip, vgl. Nr. 4.2.1) für die Aufnahme biometrischer Merkmale in Ausweisdokumente in

Frage kommen. Die 2D-Barcode-Technologie soll für die internationalen Berufsausweise für Seeleute (vgl. Nr. 6.2.5) genutzt werden. Demgegenüber sieht die EU-Pass-Verordnung die Nutzung eines RFID-Chips vor.

6.2.3 Biometrische Merkmale bei Visa- und Aufenthaltserlaubnissen

Im Rahmen der gemeinsamen Visapolitik der Europäischen Union soll Biometrie in die Visaverfahren und in Aufenthaltstitel für Drittstaatsangehörige integriert werden.

Bereits vor dem 11. September 2001 hatten das Auswärtige Amt und das BMI damit begonnen, das Lichtbild in das Visumetikett aufzunehmen. Mit der Verordnung (EG) Nr. 334/2002 vom 18. Februar 2002 (ABl. Nr. L 53 S. 7) hat der Rat festgelegt, dass ein nach „Hochsicherheitsnormen hergestelltes Lichtbild“ in das Visumetikett integriert wird.

Am 24. September 2003 legte die Kommission einen Verordnungsvorschlag vor, der nicht nur die Einführung biometrischer Merkmale (digitales Lichtbild, zwei digitale Fingerabdrücke vom flachen Finger) in Visa und Aufenthaltstiteln für Drittstaatenangehörige vorsah, sondern auch die Schaffung einer nationalen wie auch einer gemeinschaftlichen Datenbank (VIS = Visa Information System) mit alphanumerischen Informationen (z. B. Name, Adresse, Geburtsdaten), biometrischen Daten (digitalisiertes Lichtbild, Fingerabdrücke) sowie sonstigen eingescannten Dokumenten (gedacht war an Pässe, Geburtsurkunden etc.) der Visaantragsteller.

Unter dem Eindruck der Anschläge vom 11. März 2004 in Madrid forderte der Rat die Kommission auf, Vorschläge zur Verbesserung der Interoperabilität europäischer Datenbanken vorzulegen und außerdem zu erkunden, welche Synergieeffekte zwischen bestehenden und künftigen Informationssystemen (SIS II, VIS und Eurodac) zur Verhütung und Bekämpfung des Terrorismus erzielt werden könnten.

Nach dem am 8. Juni 2004 gefallenen Beschluss des Rates zur Bereitstellung der Finanzmittel haben die Vorarbeiten zur Errichtung dieses Systems begonnen. Dabei wird von Seiten der Kommission eine identische technische Plattform wie das neue Schengen Informationssystem (SIS II – vgl. Nr. 3.3.2.1) angestrebt.

Alle Maßnahmen in diesem Bereich wirken sich erheblich auf die Grundrechte der Ausländer aus, die ein Visum zur Einreise in einen sog. Schengenstaat beantragen. Im erweiterten Europa rechnet man ab 2007 mit etwa 20 Mio. Visaanträgen pro Jahr. Die Datenbank wird daher im laufenden Verfahren bis zu 100 Mio. Menschen betreffen.

Die Art. 29-Gruppe (vgl. Nr. 3.2.1) hat sich mit ihrer Stellungnahme Nr. 7/2004 vom 11. August 2004 kritisch mit den Vorschlägen der Kommission auseinandergesetzt. Sie betont, dass bei allem Verständnis für das Bestreben „Visa-Shopping“ und „Identitätsdiebstahl“ zu bekämpfen, der Schutz der Grundrechte gewahrt werden muss. Sie hat Bedenken geäußert, ob bei der Schaffung einer

Zentraldatei mit biometrischen Merkmalen aller Ausländer, die ein Visum beantragt haben, der Grundsatz der Verhältnismäßigkeit beachtet wird. Außerdem wurde dringend die Schaffung von präzisen Zweckbestimmungsregelungen angemahnt. Insbesondere für den Chip, der nach den ursprünglichen Plänen auf dem Visum aufgebracht werden sollte, wurden hohe Anforderungen an die Sicherheit formuliert. Für den Fall von Erkennungsfehlern bei biometriegestützten Grenzkontrollen müssen die betroffenen Personen über die Ursachen der Zurückweisung unterrichtet werden. Ferner müssen sie die Möglichkeit erhalten, ihren Standpunkt darlegen zu können, bevor eine Entscheidung getroffen wird (Artikel 15 der EG-Datenschutzrichtlinie).

Ein am 28. Dezember 2004 vorgelegter neuer Verordnungsvorschlag der Kommission berücksichtigt einen Teil dieser Forderungen. Er sieht vor, in VIS alphanumerische und biometrische Daten (digitalisiertes Lichtbild, Fingerabdrücke), aber keine sonstigen eingescannten Dokumente zu speichern. Dafür sollen aber Verknüpfungen zu anderen Anträgen gespeichert werden. Für die Daten ist eine Lösungsfrist von fünf Jahren vorgesehen. Der Vorschlag enthält auf Grund von Schwierigkeiten bei der Verwendung der RFID-Technik keine Regelung über die Speicherung biometrischer Merkmale in den Visaetiketten. Genutzt werden soll das VIS nicht nur bei Visaverfahren, sondern auch im Asylverfahren und zur Identifizierung und Rückführung illegaler Einwanderer. Die Art. 29-Gruppe beabsichtigt, zu dem Entwurf kurzfristig Stellung zu nehmen und damit zu einer Berücksichtigung datenschutzrechtlicher Belange bei der anstehenden Beratung des EP beizutragen.

Kasten zu Nr. 6.2.3

Das VIS soll folgenden Zwecken dienen:

- Unterstützung im Kampf gegen Betrug,
- Verbesserung der konsularischen Zusammenarbeit zwischen den Mitgliedstaaten bei der Erteilung von Visa,
- Unterstützung bei der Identifizierung des Visuminhabers,
- Prävention gegen „Visa-Hopping“ („Bekomme ich das Visum nicht von dem einen Schengenstaat, gehe ich zur Auslandsvertretung eines anderen Schengenstaates“),
- Prävention gegen „Visa-Shopping“ (Suche nach dem „vorteilhaftesten“ Visum),
- Unterstützung bei Anfragen nach dem Dubliner Übereinkommen,
- Unterstützung bei der Identifizierung und der Rückführung von Drittstaatsangehörigen,
- Beitrag zur internationalen Sicherheit und im Kampf gegen den Terrorismus.

6.2.4 **Pilottestverfahren zur Gesichtserkennung im Bundesverwaltungsamt**

Gesichtserkennung in Visaverfahren reicht als alleiniges Suchkriterium nach früheren Visaentscheidungen nicht aus.

Durch das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361) wurde § 29 Abs. 1 Ausländerzentralregistergesetz dahingehend geändert, dass in der beim Bundesverwaltungsamt (BVA) geführten zentralen Visadatei auch das Lichtbild des Visumantragstellers gespeichert werden kann. In der zentralen Visadatei waren mit Ablauf des Berichtszeitraums mehr als drei Mio. Entscheidungen über Visaanträge aus mehr als 175 Auslandsvertretungen gespeichert. Zu diesen Datensätzen waren Ende 2004 mehr als 1,7 Mio. Lichtbilder von Visumantragstellern aufgenommen worden.

Das BVA hat in dem Pilotprojekt „Biometrie im VISA-Verfahren des Bundesverwaltungsamtes“ die sog. „Kleine Biometrielösung“ entwickelt, wobei ich die frühe und gute Zusammenarbeit mit dem BVA hervorheben möchte (vgl. auch Nr. 4.2.2.). Ziel des Projektes war zunächst die Prüfung, ob die Leistungsfähigkeit biometrischer Gesichtserkennungsverfahren für den geplanten Einsatz in dem Masseverfahren Visaerteilung ausreicht. Wesentliches Ergebnis der Tests war, dass der Datensatz in der Visadatei mit Hilfe des Gesichtserkennungsverfahrens im Regelfall wiedergefunden wird, wenn der betreffende Visumantragsteller dasselbe Bild einreicht, das er auch bei seinem letzten Antrag vorgelegt hat. Legt er ein anderes Bild vor, verschlechtert sich die Wiedererkennungsrates jedoch deutlich. Unterschiede bei der Erkennungsleistung aufgrund des Herkunftslandes oder der ethnischen Zugehörigkeit des Visumantragstellers konnten bei den Tests nicht nachgewiesen werden.

Insgesamt zog das BVA das Fazit, dass die Gesichtserkennung im Visaverfahren zwar nicht als alleiniges Suchkriterium ausreicht, herkömmliche alphanumerisch/phonetischen Suchkriterien jedoch sinnvoll ergänzen kann. Da die Gesichtserkennungsverfahren – wie alle anderen biometrischen Verfahren auch – aufgrund der laufenden Forschung sich in den nächsten Jahren noch deutlich verbessern können, werde ich die Entwicklungen auch hier aufmerksam verfolgen. Zur entsprechenden europäischen Entwicklung vgl. Nr. 6.2.3.

6.2.5 **Der Seefahrer-Ausweis**

Auch die Seefahrer-Ausweise werden in Zukunft digitalisierte Lichtbilder und Fingerabdrücke enthalten. Zusätzlich sollen die Daten in einer nationalen Datenbank zur Überprüfung der Echtheit des Ausweises gespeichert werden.

Die Internationale Arbeitsorganisation (International Labour Organization – ILO) hat am 5. Juni 2003 das „Übereinkommen Nr. 185 über Ausweise für Seeleute“ verabschiedet, das im Februar 2005 in Kraft treten wird. Es sieht die Aufnahme des digitalisierten und/oder Originallichtbildes

sowie von Fingerabdrücken in den Ausweis für Seeleute in Form eines 2D-Barcodes vor. Dieser Ausweis für Seeleute ist ein Berufsausweis, der nach dem Übereinkommen ausdrücklich kein Reisedokument ist, dem Inhaber aber bestimmte Vergünstigungen gewährt (Landgang während der Liegezeit des Schiffes ohne Beantragung eines Visums, Transit vom oder zum Schiff oder zwischen Schiffen mit Visum unter erleichterten Bedingungen). Zusätzlich zur Aufnahme biometrischer Merkmale in diesen Berufsausweis sollen die Daten der weltweit ca. 1,2 Mio. Seeleute im Ausgabeland des Ausweises, d. h. dezentral in nationalen Datenbanken, gespeichert werden.

Für das Vorhaben gelten prinzipiell dieselben Vorbehalte wie gegenüber der Verwendung biometrischer Daten in sonstigen Ausweisdokumenten. Das „Übereinkommen über Ausweise für Seeleute“ enthält einige datenschutzrechtlich erfreuliche Regelungen. Dazu gehört, dass die in der nationalen Datenbank gespeicherten Merkmale abschließend geregelt sind und nur der Verifikation dienen sollen. Ausdrücklich wird in dem Übereinkommen gefordert, die Datensicherheit zu garantieren und das Recht des Betroffenen auf Datenschutz („right of privacy“) zu beachten. Auch das Auskunftsrecht des betroffenen Seemanns ist – sowohl hinsichtlich der auf der Ausweiskarte als auch hinsichtlich der in der Datenbank gespeicherten Daten – datenschutzrechtlich zufriedenstellend geregelt. Bedenken habe ich lediglich hinsichtlich der Datenübermittlungsregelungen, die mit den Vorgaben der EG-Datenschutzrichtlinie dann kollidieren können, wenn – was sehr wahrscheinlich ist – die Daten von Seeleuten aus EU-Mitgliedstaaten von Behörden aus Drittstaaten ausgelesen und/oder an diese übermittelt werden, wenn diese nicht das von der EG-Datenschutzrichtlinie geforderte angemessene Datenschutzniveau besitzen. Eine derartige Datenübermittlung könnte jedoch dadurch gerechtfertigt sein, dass sich die Mitgliedstaaten, die das Übereinkommen ratifiziert haben, verpflichten, die Daten nur für Zwecke der Verifikation des Ausweises zu nutzen.

6.3 **Die Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) und das Stasi-Unterlagen-Gesetz (StUG)**

Dem sensiblen Bereich der BStU gilt nach wie vor mein besonderes Augenmerk. Ich habe die Zentrale der BStU in Berlin und eine Außenstelle besucht und im schriftlichen Verfahren beraten.

6.3.1 **Der „Fall Kohl“ – Fortsetzung**

Auch nach einer weiteren Runde im Rechtsstreit sind die Konsequenzen im „Fall Kohl“ nicht absehbar.

Nach dem ersten Urteil des Bundesverwaltungsgerichts vom 8. März 2002 (vgl. 19. TB Nr. 7.6.1) galt zunächst, dass die BStU im Fall Kohl gegen dessen Willen in keinem Fall Unterlagen herausgeben durfte. Dies war nach der neu gefassten Abwägungsklausel des § 32 StUG (5. Gesetz zur Änderung des Stasi-Unterlagen-Gesetzes)

vom 6. September 2002 jedoch wieder zweifelhaft. Zur Klärung haben die Parteien erneut die Gerichte angerufen.

Nach dem zweiten Urteil des Bundesverwaltungsgerichts (BVerwG, 3 C 41.03 vom 23. Juni 2004) ist das geänderte StUG einschränkend verfassungskonform auszulegen und anzuwenden. Hierfür hat das Gericht Kriterien festgelegt. Die BStU hat angekündigt, ihre internen Richtlinien für die Herausgabe von Akten zu überarbeiten und die Praxis entsprechend zu ändern. Konkrete Angaben über die Änderungen und deren Bedeutung für die Praxis liegen mir bisher nicht vor. Fest steht, dass eine Herausgabe von Unterlagen ohne Zustimmung des Betroffenen noch sensibler geprüft werden muss und nur noch in ganz besonderen Ausnahmefällen möglich ist.

Die Urteile im Wortlaut finden Sie unter <http://www.bundesverwaltungsgericht.de>.

6.3.2 „Steckbriefe“ von Stasi-Mitarbeitern im Internet

Ehemalige Stasi-Mitarbeiter beschwerten sich über die Veröffentlichung ihrer Lebensläufe mit Lichtbild auf den Seiten einer Außenstelle der BStU im Internet.

Durch mehrere Eingaben von Petenten und den Hinweis einer Landesbeauftragten für den Datenschutz wurde ich im Februar 2004 darauf aufmerksam, dass auf den Internetseiten der BStU personenbezogene Daten ehemaliger Stasi-Mitarbeiter veröffentlicht wurden. Die Eingaben der Petenten richteten sich vor allem auch gegen die Art und Weise der Veröffentlichung, weil sie einem „Steckbrief“ ähnlich sei. Nach einer ersten Überprüfung habe ich die BStU gebeten, die Rechtsgrundlage für eine solche Veröffentlichung auch in Bezug auf Art und Weise ihrer Darstellung noch einmal zu prüfen. Die BStU hat sich für die Veröffentlichung auf ihren Gesetzesauftrag gemäß § 37 Abs. 1 Nr. 5 StUG berufen, die Öffentlichkeit umfassend über den Staatssicherheitsdienst der DDR zu informieren. Wegen der Art und Weise der Veröffentlichung wurden die beanstandeten Seiten jedoch umgehend entfernt. Die BStU hat darüber hinaus den Vorgang zum Anlass genommen, eine interne Arbeitsgruppe mit der Erarbeitung von Richtlinien für eine Veröffentlichung personenbezogener Daten im Internet zu beauftragen. Diese liegen noch nicht vor. Ich gehe davon aus, dass die BStU sich wieder weitgehend an ihre ursprüngliche Praxis halten wird: Seit längerem werden über das Führungspersonal des ehemaligen Ministeriums für Staatssicherheit nach einer ausführlichen erläuternden Vorbemerkung Kurzbiografien in Blockform und ohne Bild veröffentlicht.

6.4 Datenschutz im Bundesministerium des Innern

2003 habe ich einen Beratungs- und Kontrollbesuch beim BMI durchgeführt. Das BMI hat die dabei festgestellten Mängel inzwischen weitgehend beseitigt.

Bei einem Beratungs- und Kontrollbesuch im Bundesministerium des Innern habe ich den Umgang mit perso-

nenbezogenen Daten im nicht-automatisierten Verfahren sowie die Führung von Personalakten und der Versorgungsakten sowie der Teilakten „Besoldung, Vergütung, Löhne, Beihilfen“, die beim Bundesverwaltungsamt – Außenstelle Berlin-Lichtenberg – bearbeitet werden, kontrolliert (Prüfergebnisse zum Bereich Personalwesen vgl. Nr. 10.5).

Zum Zeitpunkt des Besuches verfügte das BMI nicht mehr über einen behördlichen Datenschutzbeauftragten (bDSB). Der bisherige bDSB war in den Ruhestand gegangen und ein Nachfolger – entgegen der zwingenden Vorschrift des § 4f BDSG – noch nicht bestellt. Ich habe das BMI gebeten, dafür Sorge zu tragen, dass die dringend erforderliche Bestellung eines bDSB umgehend vorgenommen wird. Zudem habe ich deutlich gemacht, dass ich die lediglich nominelle Bestellung eines bDSB als Zusatzfunktion zu seinen sonstigen Aufgaben in einer so großen und vielgestaltigen Behörde wie dem BMI für nicht ausreichend halte. So sind vielmehr die Bereitstellung entsprechender Arbeitskapazitäten in Form einer – zumindest teilweisen – Freistellung von anderen Aufgaben sowie nötigenfalls die Zuweisung von Hilfspersonal gem. § 4f BDSG und die Anbindung an die Leitungsebene zwingend erforderlich. Da das BMI diesen Forderungen – wenn auch mit fast einem Jahr Verspätung – durch Bestellung einer Referatsleiterin auf einer halben Stelle, allerdings ohne Unterstützungspersonal, weitgehend nachgekommen ist, habe ich von einer förmlichen Beanstandung abgesehen. Dies auch, weil ich bei der Kontrolle keine sonstigen schwerwiegenden datenschutzrechtlichen Mängel beim Umgang mit personenbezogenen Daten in den kontrollierten Abteilungen festgestellt hatte. Zudem hat das BMI meine Anregungen übernommen und entsprechende Änderungen veranlasst.

Diesen ersten Beratungs- und Kontrollbesuch im BMI habe ich bewusst auf vier Abteilungen beschränkt; ich habe mir aber weitere Besuche, insbesondere des Sicherheitsbereichs, ausdrücklich vorbehalten.

6.5 Neues bei der Bundesakademie für öffentliche Verwaltung

Das Interaktive Fortbildungssystem für die Bundesverwaltung – IFOS-Bund – soll den am Fortbildungsprozess Beteiligten die Arbeit und den Informationsaustausch erleichtern.

Die Bundesakademie für öffentliche Verwaltung (BAköV) hat zusammen mit der Fachhochschule des Bundes für öffentliche Verwaltung (FH Bund) das System **IFOS-Bund** entwickelt. Dieses intranet-/internetbasierte System erleichtert es den am Fortbildungsprozess Beteiligten, Planungen, Veröffentlichungen und Buchungen von Fortbildungsveranstaltungen sowie die erforderliche Kommunikation und Information in Fortbildungsangelegenheiten zu erledigen.

Ich habe IFOS-Bund im November 2002 kontrolliert. Meine dabei geäußerten Anregungen und Empfehlungen hinsichtlich der Gestaltung des Anfrageformulars und der

Speicherdauer der Formulare Daten wurden von der BAKöV in das System eingearbeitet. Als besonderes positiv habe ich folgende Systemeinstellungen bewertet:

- Die Zugriffsberechtigungen der Mitarbeiter der BAKöV, insbesondere auf die Daten der Teilnehmer, sind stark eingegrenzt.
- Alle bearbeitenden Zugriffe werden protokolliert und können so nachvollzogen werden.

Mittelfristig soll das System IFOS-Bund zu einer „**virtuellen Lernplattform**“ ausgebaut werden. Bereits jetzt stellt das System Lerninhalte webbasiert zur Verfügung. Allerdings wurden notwendige Zusatzfunktionen, beispielsweise die Einrichtung von veranstaltungsbegleitenden oder veranstaltungsunabhängigen Foren und Chaträumen oder die Nutzung eines sog. Persönlichen Schreibtisches in einer E-Learning-Umgebung, noch nicht in das System implementiert.

Die Lernplattform soll unterteilt werden in einen öffentlich-zugänglichen Bereich, einen geschützten und einen besonders geschützten Bereich, in dem der Zugang ausschließlich durch die Fortbildungsverantwortlichen in den Behörden erfolgen kann. Der Zugang soll sowohl über die Lernplattform selbst als auch über IFOS-Bund möglich sein.

Im Januar 2005 beginnt ein einjähriger Probetrieb. Dabei sind vor allem die Funktionalitäten zur Bearbeitung der personenbezogenen Angaben bei der Benutzererkennung, bei der Erwartungsabfrage vor dem Seminar, bei der Abgabe von Arbeitsproben, bei der Überprüfung von Zugriffsberechtigungen, bei der Speicherung der Anmelde Daten und bei den Lösungsfristen von datenschutzrechtlichem Interesse. Da es sich bei der Lernplattform um einen Teledienst handelt, müssen insbesondere die Regelungen des Teledienstschutzgesetzes beachtet werden.

Ich werde den Praxistest und die Weiterentwicklung des Gesamtsystems weiter begleiten.

6.6 Personenkennziffer im Melderecht

Im Meldewesen sind datenschutzrechtlich problematische Entwicklungen festzustellen.

Wiederholt stellte ich fest, dass der datenschutzrechtliche Standard des Melderechtsrahmengesetzes (MRRG) wenig befriedigend ist (zuletzt 19. TB Nr. 7.3). Die Situation hat sich im Berichtszeitraum noch verschlechtert, weil aus den unterschiedlichsten Gründen Änderungen im Melderecht vorgenommen wurden, um zusätzliche Wünsche an Meldedaten zu befriedigen. So wird über das Steuerrecht praktisch ein zentrales Melderegister eingeführt. Zudem sollen sowohl in den kommunalen Melderegistern als auch in dem Zentralregister einheitliche steuerliche Identifikationsnummern gespeichert werden. Es muss verhindert werden, dass sich hieraus eine vom Bundesverfassungsgericht in seinem Volkszählungsurteil abgelehnte Personenkennziffer (vgl. Nr. 8.2) entwickelt.

Gleichzeitig gibt es verstärkten Informationsbedarf zwischen Waffen- und Meldebehörden aufgrund der Neuordnung des Waffenrechtes. Zu Aufregung führten auch Wählerpotenzialanalysen, für die Wahlforschungsinstitute Meldedaten nutzten, um Aussagen über die politischen Präferenzen der Wahlberechtigten zu gewinnen. Ich vertrete hierzu die Auffassung, dass aufgrund der engen Zweckbindung des § 22 MRRG ein Abgleich der nur für Wahlwerbezwecke den Parteien übermittelten Meldedaten mit anderen Daten unzulässig ist. Aufmerksam beobachte ich ferner die Entwicklungen im eGovernment mit elektronischen Abfragen und Abgleichen und den Bestrebungen um eine grenzüberschreitende europaweite Melderegisterauskunft.

6.7 Personenstandsgesetz – Ahnenforschung

Die Ahnenforschung soll durch eine Reform des Personenstandsrechts erleichtert werden.

Das Ziel der vom BMI seit langem geplanten Reform des Personenstandsgesetzes ist es, die immer beliebter werdende Ahnenforschung zu erleichtern. Die Ahnenforscher stoßen nicht selten auf Schwierigkeiten, weil die Nutzung der staatlichen Personenstandsbücher denselben strengen Regeln unterworfen ist, wie die Verwendung aktueller Beurkundungen. Die Nutzung kann nur von Personen verlangt werden, auf die sich der Eintrag bezieht sowie von deren Ehegatten, Vorfahren und Abkömmlingen. Andere Personen (z. B. Verwandte der Seitenlinie) haben nur dann ein Benutzungsrecht, wenn sie „ein rechtliches Interesse glaubhaft machen“, was für die Ahnenforschung nach allgemeiner Rechtsauffassung verneint wird, da ihr nur ein berechtigtes Interesse zugestanden wird. Mich erreichen deshalb viele Eingaben von Familienforschern, die fälschlich annehmen, dass der Datenschutz diese strenge Regelung erfordert. In Anlehnung an einen von mir vor geraumer Zeit unterbreiteten Vorschlag ist nunmehr seitens des BMI daran gedacht, die Benutzung schon bei berechtigtem Interesse zuzulassen, wenn die Betroffenen seit mindestens 30 Jahren verstorben sind oder – sollte der Todestag nicht bekannt sein – wenn deren Geburtsdatum mindestens 110 Jahre zurückliegt.

Weitere Schwerpunkte der vorgesehenen Reform sind die Einführung elektronischer Personenstandsregister, die Abschaffung des Familienbuchs und die Reduzierung der Beurkundungsdaten. Das BMI hat angekündigt, einen entsprechenden Änderungsentwurf 2005 vorzulegen.

6.8 Staatsangehörigkeitsdatei

Endlich gibt es konkrete Hoffnungen auf die Schaffung einer Rechtsgrundlage für die Staatsangehörigkeitsdatei des Bundesverwaltungsamtes (BVA).

Ich habe bereits in früheren Tätigkeitsberichten (16. bis 19. TB vgl. dort zuletzt Nr. 7.7) darauf hingewiesen, dass beim BVA seit 1982 eine Datei zum Nachweis der Staatsangehörigkeit (Staatsangehörigkeitsdatei – STADA) ohne ausreichende Rechtsgrundlage geführt wird. Nach mehreren vergeblichen Anläufen wurde zur Schaffung der

erforderlichen Rechtsgrundlage bei dem federführend zuständigen BMI eine Arbeitsgruppe eingerichtet, die in Abstimmung mit den Ländern entsprechende Vorschläge für bereichsspezifische datenschutzrechtliche Regelungen im Staatsangehörigkeitsrecht erarbeitet hat. Diese sollen – neben anderen Regelungen – in den Referentenentwurf eines weiteren „Gesetzes zur Änderung des Aufenthaltsgesetzes und anderer Gesetze“ Eingang finden. Der Referentenentwurf soll im Frühjahr 2005 in die Ressortabstimmung gehen, so dass die Änderung hoffentlich im Herbst 2005 in Kraft treten kann und die STADA dann endlich eine Rechtsgrundlage hat.

6.9 Richtlinie der Bundesregierung zur Korruptionsprävention

Die Richtlinie zur Korruptionsprävention in der Bundesverwaltung wurde 2004 neu gefasst.

Zur Verbesserung der Korruptionsprävention wurde die Richtlinie zur Korruptionsprävention in der Bundesverwaltung 2004 neu gefasst (BAnz Nr. 148 S. 17745). Problematisch war vor allem die Nutzung von Daten aus Sicherheitsüberprüfungen für die Korruptionsprävention.

Eine Nutzung der im Rahmen einer Sicherheitsüberprüfung erhobenen Daten für andere Zwecke ist nur nach Maßgabe des § 21 Sicherheitsüberprüfungsgesetz (SÜG) zulässig, wobei der Gesetzgeber eine strenge Zweckbindung vorgesehen hat. Ich habe mich gegen die Überlegung gewandt, § 21 SÜG dahingehend zu erweitern, die im Rahmen einer Sicherheitsüberprüfung erhobenen Daten auch für Zwecke der Korruptionsprävention zu nutzen. Die in § 21 Abs. 1 Nr. 2 SÜG normierte Beschränkung auf den Bereich der Repression ist durch keine Form der Auslegung dieser Norm zu relativieren. Insofern wäre eine Novellierung des SÜG erforderlich gewesen.

Auch nach den vorliegenden Erkenntnissen sind die Ergebnisse einer Sicherheitsüberprüfung im Hinblick auf die Korruptionsprävention nicht einschlägig. Es ist auch kein Fall bekannt, in dem eine Personalunion zwischen der Ansprechperson für Korruptionsprävention und dem Sicherheitsbeauftragten verhindert hätte, dass eine ungeeignete Person in einem besonders korruptionsgefährdeten Bereich eingesetzt wurde.

Ich begrüße deshalb die ausdrückliche Klarstellung in der Empfehlung zu Nr. 5 der Richtlinie, dass zur Ansprechperson nicht bestellt werden kann, wer der für Sicherheitsüberprüfungen zuständigen Organisationseinheit angehört.

6.10 Flexibilisierung der amtlichen Statistik

Aus Sicht der Statistiker wäre die Nutzung von Verwaltungsdaten hilfreich, da dies die Erhebungskosten senken könnte. Ein generelles Zugangsrecht der Statistik zu Verwaltungsregistern begegnet aber erheblichen rechtlichen Bedenken.

Im Berichtszeitraum sind aus dem Bereich der amtlichen Statistik Wünsche laut geworden, in verstärktem Umfang bereits vorhandene Verwaltungsregister zu nutzen. Eine

solche Flexibilisierung führe zu einer nennenswerten Entlastung der Wirtschaft, da anstelle der Befragung der Betroffenen *nur* die Verwaltung eingebunden werde.

Die Nutzung von Verwaltungsregistern ist kein datenschutzrechtliches Tabu-Thema, denn bereits heute werden Verwaltungsdaten bei mehr als 40 Prozent der Erhebungen genutzt. Dieser „Vereinfachungsweg“ – anstelle der Betroffenen die Verwaltung zu befragen – darf aber nicht zu Beeinträchtigungen auf Seiten der Betroffenen führen. Unter datenschutzrechtlichen Aspekten macht es nämlich keinen großen Unterschied, ob der Bürger direkt und mit Auskunftszwang befragt wird oder ob die Daten, ohne den Betroffenen im Einzelfall zu informieren, durch Rückgriff auf vorhandene Verwaltungsdaten besorgt werden. Amtliche Statistik mit Auskunftszwang ist Eingriffsverwaltung. Und Eingriffe des Staates in die Verhältnisse seiner Bürger bedürfen einer gesetzlichen Legitimation. Unter diesem Gesetzesvorbehalt steht auch ein allgemeines Zugangsrecht der Statistik zu Verwaltungsregistern. Insbesondere, wenn es sich um eine pauschale gesetzliche Regelung handelt, welche die mit einer Auskunftspflicht verbundenen Erhebungen bei Betroffenen ersetzen soll. Ein Zwang zur Angabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und die Angaben für diesen Zweck geeignet und erforderlich sein müssen. Zwar kann für statistische Zwecke eine enge und konkrete Zweckbindung der Daten nicht verlangt werden, zum Ausgleich dafür müssen aber der Informationserhebung und -verarbeitung entsprechende Schranken gegenüberstehen.

Die bisherige Vorgehensweise, gesetzlich festzulegen, welche Daten für welche Auswertungen benötigt werden und woher die Daten kommen sollen, hat sich in der Praxis durchaus bewährt.

Ein vom damaligen Bundesministerium für Wirtschaft und Technologie in Auftrag gegebenes Gutachten des Instituts für Angewandte Wirtschaftsforschung von 1999 hat sich mit genau dieser Fragestellung auseinandergesetzt. Die Registerinventur, in die „alle irgendwie brauchbar erscheinenden Register“ einbezogen wurden, ergab, dass letztendlich nur drei bis vier Register für eine Substitution tauglich erscheinen, und zwar die Betriebs- und Versicherungendatei der Bundesagentur für Arbeit, die Dateien der Finanzverwaltung, Dateien kommunaler Ämter für öffentliche Ordnung/Gewerbebeamter sowie Dateien der Industrie- und Handelskammer und Handwerkskammern. Selbst bei diesen Registern seien mehr oder weniger umfangreiche EDV-Änderungen und sog. Trimmungen – das sind inhaltliche Veränderungen der Register, damit sie den statistischen Erfordernissen genügen – erforderlich. Ein allgemeines Zugangsrecht zu Verwaltungsregistern könnte daher nur dann nützlich sein, wenn der Statistik zugleich das Recht eingeräumt würde, die Verwaltungsregister auf die statistischen Belange inhaltlich und organisatorisch auszurichten und trotz föderaler Verwaltungshoheit die Vereinheitlichung von kommunalen und Länderregistern vorzuschreiben.

Insofern scheint nicht ein fehlendes allgemeines Zugangsrecht der Statistik das Problem, sondern die nicht vorhandenen gebrauchsfertigen Verwaltungsregister.

Ich sehe somit für die Schaffung eines generellen gesetzlichen Zugangsrechts der Statistik zu Verwaltungsdaten weder eine verfassungsgemäße Möglichkeit, noch eine praktikable Verbesserung der Situation. Aus meiner Sicht kann und sollte jedoch darüber diskutiert werden, inwieweit künftig ein Stammdatensatz pro Unternehmen, der für verschiedene Statistiken herangezogen werden kann, Erleichterungen bringt. Diskutabel ist ferner die Rückmeldung plausibilisierter Daten in Einzelfällen (z. B. Anschrift, Rechtsform, Wirtschaftszweig, Organzugehörigkeit) und die Zusammenarbeit mit der Verwaltung bei der Gestaltung der Verwaltungsregister.

Der Datenschutz ist kein unüberwindbares Hindernis für die Verwendung von Verwaltungsdaten für Wirtschaftsstatistiken. Deshalb bin ich sicher, dass sich vertretbare Lösungen finden lassen werden.

6.11 Mikrozensusgesetz – was gibt es Neues?

Durch das Mikrozensusgesetz 2005 werden nicht mehr alle Erhebungsmerkmale im Gesetz selbst, sondern durch eine Rechtsverordnung festgelegt.

Die Grundidee des Mikrozensus ist, mit einer Auswahl der Bevölkerung nach mathematisch-statistischen Verfahren ein annähernd wirklichkeitsgetreues Abbild der gesamten Bevölkerung darzustellen. Die Ergebnisse bilden eine Grundlage für politische Entscheidungen, z. B. im Bereich der Arbeits-, Sozial-, Familien-, Gesundheits- oder Bildungspolitik; sie finden Eingang in Regierungsberichte, in das Jahresgutachten des Sachverständigenrates zur Begutachtung der gesamtwirtschaftlichen Entwicklung und stehen Wissenschaft und Forschung zur Verfügung.

Das Mikrozensusgesetz 2005 (MZG) ist – wie seine Vorgänger – zeitlich befristet und gilt für acht Jahre, um den Erhebungsbedarf überprüfen und gegebenenfalls anpassen zu können. Nachdem im Mikrozensusgesetz 1996 den Anregungen des BfD Rechnung getragen worden war (vgl. 16. TB Nr. 30.4), habe ich mich auf die Änderungen dieses Gesetzes konzentriert. Die entscheidende Veränderung besteht darin, nicht mehr sämtliche Einzelfragen (Erhebungsmerkmale) im Gesetz selbst zu regeln, sondern die Regelung auf Fragenkomplexe zu beschränken, aus denen dann die konkreten Fragen entwickelt und im Wege einer Rechtsverordnung gesetzlich festgelegt werden können. So kann z. B. das im MZG formulierte Merkmal „Art, Anlass und Dauer der Arbeitssuche“ zu mehreren Fragen führen: Einerseits nach dem Grund (z. B. Entlassung, eigene Kündigung und freiwillige Unterbrechung) und andererseits nach der Tätigkeit (z. B. Selbständiger, Arbeitnehmer und Voll- oder Teilzeit). Ich habe dabei geprüft, ob die gewählten Umschreibungen dem Gebot der Normenklarheit entsprechen, d. h. ob die Fragenkomplexe hinreichend deutlich Inhalt und Umfang

der Erhebungsmerkmale bestimmen. Da der Fragebogen aber erst im Zusammenhang mit der späteren Rechtsverordnung entwickelt werden soll, wird sich meine Prüfung bei jeder konkreten Fragestellung fortsetzen. Die Umstellung wurde gewählt, um eine größere Flexibilität für statistische Erhebungen zu erreichen, indem neue Fragestellungen einbezogen oder andere nuanciert werden können, ohne das Gesetz selbst ändern zu müssen. Die Auskunftspflicht der Befragten besteht für die meisten Daten fort. Die zur freiwilligen Beantwortung stehenden Fragen wurden mit ganz geringen Ausnahmen (z. B. fehlende Antworten zum Schulabschluss mit der Folge mangelnder Aussagefähigkeit, daher jetzt Auskunftspflicht) beibehalten.

Ich habe deshalb noch einmal die generelle Auskunftspflicht der Befragten zur Diskussion gestellt und nach Alternativen mit geringerem Eingriffcharakter für den Bürger gefragt. Die Statistiker haben eingewandt, dass bei einer 1 Prozent Stichprobe die Datenbasis zu gering sei, um Ausfälle durch eine Beantwortungsquote, die unter 50 Prozent liegen würde, aufzufangen. Man sei aber bemüht, dem Grundrecht auf informationelle Selbstbestimmung Rechnung zu tragen, indem Fragen nach sensiblen Daten weitgehend der freiwilligen Auskunft überlassen seien. Gleichwohl habe ich auf die vom Bundesverfassungsgericht angemahnte Methodendiskussion hingewiesen, die sich auch auf Stichprobenerhebungen und Entwicklungen sozialwissenschaftlicher Hochrechnungsverfahren erstreckt. Weitere Neuerungen betreffen eher technisch-organisatorische Maßnahmen. Ich werde mich an der weiteren Konkretisierung des Fragenprogramms im Rahmen der zu erlassenden Rechtsverordnung beteiligen.

6.12 Volkszählungstest – Beginn eines neuen Zeitalters?

Bei künftigen Volkszählungen könnte möglicherweise auf aufwändige Befragungen aller Einwohner verzichtet werden. In den letzten Jahren wurde getestet, ob Dateien der Verwaltung geeignet sind, zu gleichen Ergebnissen zu gelangen.

Auf der Grundlage des Zensusstestgesetzes vom 27. Juli 2001 (vgl. 19. TB Nr. 7.9) haben die Statistischen Ämter des Bundes und der Länder Tests zur Erprobung eines registergestützten Zensusverfahrens durchgeführt, deren erste Ergebnisse nun vorliegen. Dabei wurde ein Alternativkonzept getestet, das anstelle der herkömmlichen Volkszählung – soweit möglich – die Nutzung vorhandener Verwaltungsregister, insbesondere der Melderegister und Dateien der Bundesagentur für Arbeit (BA), vorsieht. Gegenstand des Tests waren: Die Qualität der Melderegister und der Dateien der BA, die Verfahren zur statistischen Bereinigung der Melderegisterdaten und der Zusammenführung der verschiedenen Daten sowie das Verfahren zur Generierung von Haushaltszusammenhängen. Dazu wurden zu einem bestimmten Stichtag Daten aus den Melderegistern und den Dateien der BA für ausgewählte Gemeinden und Gebäude an die Statistischen

Ämter übermittelt sowie eine Gebäude- und Wohnungstichprobe bei den Eigentümern der ausgewählten Gebäude durchgeführt. Ferner wurde eine Befragung bei den Bewohnern durchgeführt und deren Angaben mit den Registerdaten verglichen.

Der Zensus testet nach Einschätzung des BMI ergeben, dass ein registriertes Zensus möglich ist und die getesteten statistischen Methoden und Verfahren geeignet erscheinen. Die Registernutzung müsse jedoch durch primärstatistische Elemente ergänzt werden. Insbesondere müssten die Melderegisterdaten als Grundlage belastbarer amtlicher Einwohnerzahlen überprüft und gegebenenfalls korrigiert werden, wozu Stichprobenerhebungen vorgesehen seien. Vor dem Hintergrund der für das Jahr 2010 durch die EU geplanten gemeinschaftsweiten Zensusrunde könnte das neue Verfahren zu diesem Zeitpunkt zur Anwendung kommen. Ich werde die weiteren Vorbereitungsmaßnahmen aufmerksam begleiten und dabei insbesondere darauf achten, dass – entsprechend der Entscheidung des Bundesverfassungsgerichts in seinem Volkszählungsurteil vom 15. Dezember 1983 (BVerfGE 65, 1 ff.) – keine für die Statistik erhobenen Daten für Verwaltungszwecke genutzt werden, also eine unzulässige Zweckänderung vermieden wird.

6.13 Archivbestände und ihre objektive Wahrheit

Archivbestände können auch Unterlagen enthalten, die nicht der objektiven Wahrheit entsprechen. Betroffene haben in diesen Fällen die Möglichkeit, eine eigene Darstellung zu den Archivalien hinzuzufügen.

Ein Petent teilte mir mit, dass er beim Bundesarchiv in der NSDAP-Mitgliederkartei als Mitglied gespeichert sei. Tatsächlich sei er jedoch zu keinem Zeitpunkt Mitglied der NSDAP gewesen; zum Zeitpunkt des angeblichen Beitritts sei er noch nicht volljährig gewesen, so dass er bereits aus diesem Grund nicht Mitglied der NSDAP hätte werden können. Das Bundesarchiv lehnte einen Antrag des Petenten auf Löschung ab.

Das Recht auf informationelle Selbstbestimmung verleiht dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung personenbezogener Daten zu entscheiden. Das Bundesarchivgesetz enthält in § 4 Abs. 3 eine Regelung, die diesem Schutzzweck Rechnung tragen will. Dort heißt es: *Wird festgestellt, dass personenbezogene Angaben unrichtig sind, so ist dies in den Unterlagen zu vermerken oder auf sonstige Weise festzuhalten. Bestreitet ein Betroffener die Richtigkeit personenbezogener Angaben, so ist ihm die Möglichkeit einer Gegendarstellung einzuräumen. Das zuständige Archiv ist verpflichtet, die Gegendarstellung den Unterlagen hinzuzufügen.* Vor diesem Hintergrund hat das Bundesarchiv eine Gegendarstellung des Petenten zu den Unterlagen genommen. Mit diesem Verfahren war der Petent jedoch nicht einverstanden, er beharrte vielmehr auf der Löschung der fehlerhaften Angaben.

Ich habe zwar einerseits großes Verständnis für den Ärger des Petenten, verstehe aber andererseits auch die Inten-

tion des Gesetzgebers. Das Problem liegt darin, dass es gerade zu den Aufgaben des Archivs zählt, Situationen und Lebenssachverhalte so zu dokumentieren, wie sie sich aufgrund der archivierten Aufzeichnungen darstellen. Wenn das Handeln von Stellen der NSDAP fehlerhaft war und innerhalb des nationalsozialistischen Gewaltsystems rechtswidrige Merkmale aufwies, dann ist gerade die Aufbewahrung derartiger Unterlagen als Beleg solchen Handelns unverzichtbar. Auch die Regelung in § 4 Abs. 3 BArchG verfolgt denselben Zweck, da durch die Hinzufügung der Gegendarstellung die Nachvollziehbarkeit und Offenlegung des fehlerhaften Handelns belegt wird. Der damit einhergehende Eingriff in das Recht auf informationelle Selbstbestimmung ist bei Abwägung der unterschiedlichen Rechtsgüter hinzunehmen. Zum Schutz der Persönlichkeitsrechte werden solche Unterlagen nicht in Bibliotheken mit freiem Zugang aufbewahrt, sondern in Archiven, wo sie nur unter besonderen Voraussetzungen eingesehen werden dürfen. So darf beispielsweise Archivgut, das sich auf natürliche Personen bezieht, grundsätzlich erst 30 Jahre nach dem Tod der Betroffenen durch Dritte genutzt werden. Diese Schutzfrist kann verkürzt werden, wenn die Nutzung für ein wissenschaftliches Forschungsvorhaben unerlässlich ist und schutzwürdige Belange der Betroffenen angemessene Berücksichtigung finden. Eine Veröffentlichung oder eine andere Form der Bekanntgabe in personenbezogener Form ist archivrechtlich und datenschutzrechtlich unzulässig. Auch wenn es für den Petenten im konkreten Einzelfall unbefriedigend ist, so halte ich die gesetzliche Regelung im BArchG für angemessen.

7 Rechtswesen

7.1 Akustische Wohnraumüberwachung

Zu den wichtigsten Ereignissen im Berichtszeitraum zählt das Urteil des Bundesverfassungsgerichts vom 3. März 2004 zur akustischen Wohnraumüberwachung.

7.1.1 Urteil des Bundesverfassungsgerichts vom 3. März 2004

Das Urteil des Bundesverfassungsgerichts zum „Großen Lauschangriff“ ist ein wichtiger Orientierungspunkt bei der Abwägung zwischen den Belangen der inneren Sicherheit und den Rechten des Einzelnen.

In seinem richtungsweisenden Urteil hat das BVerfG deutliche Grenzen für das heimliche Abhören von Wohnungen mit akustischen Hilfsmitteln gesetzt (vgl. Kasten zu Nr. 7.1.1). Eine Minderheit des Senats hat den Artikel 13 Abs. 3 GG, der die verfassungsrechtliche Grundlage der Wohnraumüberwachung darstellt, als „verfassungswidriges Verfassungsrecht“ gewertet. Nach der Meinung der Senatsmehrheit muss Artikel 13 Abs. 3 GG restriktiv und in einer an der Menschenwürde orientierten Weise interpretiert werden. Es muss sichergestellt sein, dass die akustische Wohnraumüberwachung nicht in den unantastbaren Bereich der privaten Lebensgestaltung eindringt. Die Fortentwicklung dieses in ständiger Recht-