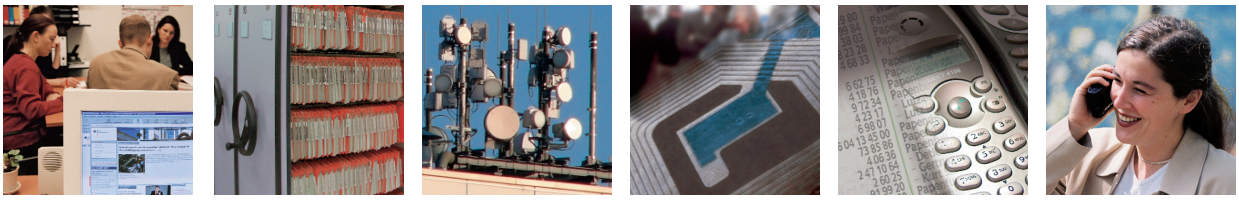
Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit



Tätigkeitsbericht zum Datenschutz für die Jahre 2007 und 2008

22. Tätigkeitsbericht

Tätigkeitsbericht 2007-2008

22. Tätigkeitsbericht

Dieser Bericht wurde am 21. April 2009 dem Präsidenten des Deutschen Bundestages, Herrn Dr. Norbert Lammert, überreicht.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Peter Schaar

Tätigkeitsbericht 2007 und 2008 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
– 22. Tätigkeitsbericht –

Inhaltsverzeichnis

Im Tätigkeitsbericht sind nur die Entschließungen abgedruckt, auf die in den Beiträgen unmittelbar Bezug genommen wird. Alle Entschließungen der Datenschutzkonferenzen und weitere Informationen finden Sie auf der Internet-Seite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter www.bfdi.bund.de.

Seite

Seite

Seite

Seite

Einführung

In die Diskussion um den Datenschutz ist in der letzten Zeit Bewegung gekommen, so sehr, dass die aktuelle Lage des Datenschutzes in Deutschland nachfolgend in einem eigenen Kapitel dargestellt wird. An dieser Stelle möchte ich auf den Punkt bringen, worum es im Kern geht: Datenschutz ist kein Selbstzweck. Vielmehr geht es um die Sicherung und Verwirklichung eines Grundrechts, das unmittelbar aus der Menschenwürde und der freien Entfaltung der Persönlichkeit folgt. Der Staat hat dies nicht nur im Verhältnis zu seinen Bürgerinnen und Bürgern zu beachten, sondern er muss in seiner Rechtsordnung insgesamt gewährleisten, dass dieses Grundrecht zur Geltung kommt. Der Datenschutz gehört zu den Grundlagen unserer Gesellschaftsordnung und muss insbesondere bei der Weiterentwicklung der Informationsgesellschaft gewährleistet sein. Die heftigen Debatten um die geplanten Änderungen des Bundesdatenschutzgesetzes für den nicht-öffentlichen Bereich lassen Zweifel zu, ob dies überall verstanden worden ist. Personenbezogene Daten von Menschen sind zunächst einmal Teil ihrer Persönlichkeit und nicht ein neuer Rohstoff für die Wirtschaft, bei dem sich jeder nach seinen eigenen Vorstellungen bedienen kann. Dies gilt auch in der schwierigen wirtschaftlichen Lage, in der wir uns derzeit befinden. Mit Sorge beobachte ich deshalb Diskussionsbeiträge, die das Eintreten für mehr und besseren Datenschutz in Zeiten wirtschaftlicher Schwierigkeiten für völlig unangemessen halten. Datenschutz ist kein Luxus, den man sich nur in guten Zeiten leisten kann; er ist Teil unserer Menschenwürde und von nachhaltiger Bedeutung für die Informationsgesellschaft der Zukunft – gerade auch in Krisenzeiten.

Auch in den letzten beiden Jahren bin ich in meiner Arbeit auf vielfältige Weise unterstützt worden. Mein Dank gilt deswegen den Abgeordneten des Deutschen Bundestages aller Fraktionen, aber auch allen anderen Vertretern öffentlicher und privater Stellen, die Interesse am Datenschutz und meiner Arbeit gezeigt, meinen Rat eingeholt und in sonstiger Weise meine Tätigkeit gefördert haben. Aber auch dort, wo Meinungsgegensätze und unterschiedliche Positionen bestehen, bin ich auf Respekt für meine Aufgaben und meine Auffassungen gestoßen. Auch dafür danke ich.

Insbesondere möchte ich an dieser Stelle meinen Mitarbeiterinnen und Mitarbeitern danken, ohne deren unermüdlichen Einsatz weit über das geschuldete Maß hinaus meine Arbeit in dieser Form nicht möglich gewesen wäre. In meinem letzten Tätigkeitsbericht hatte ich betont, die Grenzen der Belastbarkeit seien erreicht. In den letzten beiden Jahren wurden sie zum Teil überschritten. Ursache hierfür waren neben zahlreichen großen Gesetzesprojekten mit datenschutzrechtlichem Inhalt oder von datenschutzrechtlicher Relevanz die sich häufenden Datenschutzskandale, die selbst dort, wo meine unmittelbare Zuständigkeit nicht gegeben war, zu erheblicher Mehrarbeit geführt haben, erst recht aber natürlich dort, wo meine Aufgaben unmittelbar betroffen waren. Schließlich ist die Zahl der Eingaben erneut deutlich gestiegen und hat sich seit dem Jahr 2000 fast verdreifacht.

Ohne deutliche Personalverstärkung wird die Arbeit in der Zukunft nicht mit gleicher Intensität und Qualität fortgesetzt werden können.

Peter Schaar

1 Zur Lage des Datenschutzes in Deutschland

In den vergangenen beiden Jahren hat der Datenschutz die öffentliche Diskussion in einem Maße geprägt, wie man es seit der Volkszählungsdebatte Anfang der achtziger Jahre des vorigen Jahrhunderts nicht mehr erlebt hat. Die Palette der Themen, die dabei das Interesse der Medien und der Politik, nicht zuletzt aber auch der Menschen erregt haben, ist breit gestreut. Der Schutz der Privatsphäre, die Verwirklichung des Grundrechts auf informationelle Selbstbestimmung steht überraschend weit oben auf der Liste wichtiger Themen und bei vielen Bürgerinnen und Bürgern ist ein – hoffentlich nachhaltiger – Bewusstseinswandel festzustellen: Galt früher Vielen der Datenschutz als ein Randthema, das sie nicht persönlich betraf und deshalb vernachlässigt werden konnte, haben insbesondere die verschiedenen Datenskandale des Jahres 2008 deutlich werden lassen, dass jeder Einzelne betroffen ist oder zumindest betroffen sein kann. Diese Erkenntnis zeigt Wirkung, zum Einen bei den Menschen selbst, darüber hinaus aber auch in Politik und Gesellschaft. So sehr dieser Bewusstseinswandel und die breite öffentliche Debatte datenschutzrechtlicher und -politischer Fragen zu begrüßen ist, dadurch allein hat sich die Situation des Datenschutzes in Deutschland noch nicht nachhaltig verbessert. Jetzt müssen Taten folgen, nicht nur bei den gesetzlichen Regelungen, sondern auch bei den technischen Innovationen und beim Vollzug der einschlägigen Bestimmungen. Hier hat es im Berichtszeitraum allenfalls erste Schritte gegeben, aber die eigentliche Aufgabe, als Konsequenz aus dem Datenmissbrauch und seinen Ursachen den Datenschutz grundlegend zu reformieren und nachhaltig zu verbessern, liegt noch vor uns. Es bleibt abzuwarten, ob die vielen guten Ansätze und wohlmeinenden Ankündigungen tatsächlich umgesetzt werden und die Lage des Datenschutzes zum Guten hin verändern.

Die Bilanz der letzten beiden Jahre fällt in dieser Hinsicht eher gemischt aus:

Beim Datenschutz im öffentlichen Bereich war das herausragende Ereignis die Entscheidung des Bundesverfassungsgerichts vom 27. Februar 2008 (1 BvR 370/07; 1 BvR 595/07) zur Online-Durchsuchung nach dem Verfassungsschutzgesetz des Landes Nordrhein-Westfalen. Durch dieses Urteil wurde nicht nur die teils heftig geführte Debatte um die Zulässigkeit und Ausgestaltung solcher Online-Durchsuchungen zu einem gewissen Ende gebracht, das Bundesverfassungsgericht hat vielmehr erneut Vorgaben und wichtigen Antrieb für besseren Datenschutz gegeben, der in die Zukunft reichen und Auswirkungen haben wird, die weit über den eigentlich entschiedenen Fall hinausreichen. Das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ geht – wiewohl aus dem allgemeinen Persönlichkeitsrecht abgeleitet – über das Individual-Grundrecht auf informationelle Selbstbestimmung hinaus. Gerade weil auf Personalcomputern und anderen informationstechnischen Systemen eine Vielzahl persönlicher Informationen und Datenspuren gespeichert werden können, besteht hier ein besonderer Schutzbedarf, den der Staat auch bei der Verfolgung konkurrierender Ziele zu respektieren und zu gewährleisten hat. Lediglich in exzeptionellen Fällen, wenn höchste Rechtsgüter konkret bedroht werden, sind heimliche Eingriffe in dieses Grundrecht zulässig. Insofern ergänzt das neue „Computer-Grundrecht“ sowohl das Recht auf informationelle Selbstbestimmung als auch die Rechtsprechung des Bundesverfassungsgerichts zum absolut geschützten Kernbereich privater Lebensgestaltung (vgl. auch Nr. 2.1; 4.1; 8).

Auch sonst war die datenschutzrechtliche Diskussion im öffentlichen Bereich vielfach vom Spannungsverhältnis zwischen den Belangen der inneren Sicherheit und dem Grundrecht auf informationelle Selbstbestimmung geprägt: Die Vorratsdatenspeicherung (vgl. Nr. 3.2.1), die BKA-Gesetzesnovelle (vgl. Nr. 4.3.1) oder auch die europaweite Zusammenarbeit von Polizei- und Sicherheitsbehörden (vgl. Nr. 13.3) können hier als Beispiele genannt werden.

Daneben gibt es aber noch weitere wichtige Themen: Hierzu gehören die Auseinandersetzung um das Bundesmeldegesetz und ein zentrales Melderegister (vgl. Nr. 5.2; 6.5) ebenso wie die Vorbereitung der Volkszählung 2011 (vgl. Nr. 5.4) oder die Umsetzung der Europäischen Dienstleistungsrichtlinie und das Binnenmarktinformationssystem IMI (vgl. Nr. 3.4.1).

Keinen Erfolg hatte ich bislang mit meiner Forderung, endlich den datenschutzrechtlichen Auskunftsanspruch auch gegenüber der Finanzverwaltung zu gewährleisten. Obwohl auch das Bundesverfassungsgericht in einem Beschluss vom 10. März 2008 (1 BvR 2388/0) die unmittelbare Anwendbarkeit des § 19 BDSG gegenüber Finanzbehörden festgestellt hat, ist es immer noch nicht gelungen, eine entsprechende Klarstellung in der AO zu verankern oder den Bürgerinnen und Bürgern in anderer Weise ihr Recht ohne weitere Einschränkung zu sichern (vgl. Nr. 9.5).

Im nicht-öffentlichen Bereich, also beim Datenschutz in der Wirtschaft, war die Debatte von einer Reihe von Skandalen geprägt, die in dieser Häufigkeit bislang nicht für möglich gehalten wurden und nachdrücklich die enormen Defizite ins Bewusstsein rückten, die hier beim Umgang mit persönlichen Daten offensichtlich bestehen. Viele der Probleme und Fehlentwicklungen, die diese Skandale erst möglich gemacht haben, waren den Fachleuten durchaus bekannt, aber ihre jahrelangen Hinweise und Warnungen verhallten weithin ungehört. Erst der eklatante Missbrauch, der Skandal konnte das Interesse der Medien und der Öffentlichkeit wecken.

Ich selbst war unmittelbar durch die Ereignisse bei der Deutschen Telekom AG betroffen, da ich hier die datenschutzrechtliche Aufsicht führe (vgl. Nr. 3.2.2). Obwohl die staatsanwaltschaftlichen Ermittlungen und auch meine eigenen Untersuchungen noch nicht abgeschlossen sind, hat sich bereits erwiesen, dass die datenschutzrechtliche Organisation im Konzern nicht im vollen Umfang den gesetzlichen Anforderungen entsprochen hat. Die Skandale bei Lidl und anderen Handelsunternehmen und

die Massenüberprüfungen bei den Beschäftigten der Deutschen Bahn haben wohl auch dem letzten Zweifler vor Augen geführt, wie es um den Arbeitnehmerdatenschutz in Deutschland steht. Der Deutsche Bundestag hat seit vielen Jahren immer wieder einstimmig die Vorlage eines Arbeitnehmerdatenschutzgesetzes gefordert (vgl. Nr. 11.1), bislang ohne Erfolg. Als Reaktion auf den offen zu Tage getretenen Missbrauch soll jetzt gehandelt werden. Ich hoffe, dass es nicht wieder bei Ankündigungen bleibt und gesetzgeberische Taten folgen.

Die aufgedeckten Missstände beim Handel mit personenbezogenen Daten und die illegale Weitergabe von Kontoverbindungen und anderen geschützten persönlichen Daten haben zu einem Spitzengespräch der betroffenen Bundesminister und der Datenschutzaufsichtsbehörden geführt (vgl. Nr. 2.2), bei dem wichtige Änderungen für den Datenhandel verabredet wurden. Den betroffenen Bürgerinnen und Bürgern soll ein Stück weit die Entscheidung über den Umgang mit ihren persönlichen Daten zurückgegeben werden. Die Bundesregierung hat hierzu im Dezember 2008 einen Gesetzentwurf vorgelegt, der derzeit in den parlamentarischen Gremien behandelt wird (vgl. Nr. 2.3 und 3.4.5). Ein weiterer Gesetzentwurf soll den Datenschutz bei Score-Verfahren und im Auskunfteiwesen verbessern (Nr. 2.3 und 3.4.4).

So wichtig diese angestrebten Verbesserungen im Detail sind, dürfen sie doch nicht darüber hinwegtäuschen, dass die Modernisierung des Datenschutzrechts in seiner Struktur und in seinen grundlegenden Regelungsmechanismen heute dringender ist denn je.

Beim Eintritt in das Zeitalter allgegenwärtiger Datenverarbeitung („ubiquitous computing“) erweisen sich die hergebrachten Begriffe des Datenschutzrechts (verantwortliche Stelle, Auftragnehmer, personenbezogene Daten) genauso als diskussionsbedürftig wie die dem Datenschutzrecht zu Grunde liegenden Prinzipien, etwa die Konzepte der Erforderlichkeit oder der Zweckbindung und seine Aufsplitterung in eine Vielzahl von Rechtsvorschriften.

Bereits vor gut zehn Jahren wurde eine intensive Diskussion über die Modernisierung des Datenschutzrechts geführt, deren immer noch lesenswerte Ergebnisse (insbesondere das „Professorengutachten“ von Garstka, Roßnagel und Pfitzmann) Ende 2001, unmittelbar nach ihrer Erstellung, allerdings in einer Ministeriumsschublade landeten und inzwischen einigen Staub angesetzt haben dürften. In der damaligen politischen Stimmungslage, die geprägt war durch die Terroranschläge am 11. September 2001, erschien der Datenschutz Vielen bestenfalls nachrangig, vielfach sogar eher hinderlich. Zum Versanden der Datenschutzdiskussion mag auch beigetragen haben, dass sie über eine bloße Problembeschreibung und einige Regelungsansätze nicht hinausgekommen ist. Insbesondere war es seinerzeit unterblieben, einen neuen Entwurf für das Bundesdatenschutzgesetz zu erarbeiten.

Diese Erfahrungen sollten bedacht werden, wenn in der nächsten Legislaturperiode des Deutschen Bundestages die überfälligen Arbeiten an der Modernisierung des Datenschutzrechts wieder aufgenommen werden. Es müssten dabei konkrete Wegmarken definiert werden, welche die Etappen zu einem wirklich neuen und zeitgemäßen Datenschutzgesetz abstecken. Zu beachten ist auch, dass sich diese Diskussion nicht auf Datenschutzexperten beschränken darf und politische und wirtschaftliche Aspekte von vornherein einbeziehen muss. Von erheblicher Relevanz dürfte darüber hinaus auch der Fortgang der Datenschutzdebatte auf internationaler und europäischer Ebene sein. Noch ist nämlich nicht entschieden, ob sich der europäische Ansatz des Datenschutzes, verkörpert vor allem in der EG-Datenschutzrichtlinie von 1995, in Konkurrenz mit anderen Ansätzen (etwa aus dem US-amerikanischen und pazifischen Bereich) behaupten kann. Dies kann dann umso eher gelingen, wenn in anderen Rechtsordnungen entwickelte und dort erfolgreiche Regelungsansätze, etwa die aus dem US-amerikanischen Raum stammende Verpflichtung zur Information über Datenschutzverstöße („security breach notification“), aufgenommen und in das europäische Rechtssystem integriert werden.

Bei alledem dürfen auch die unübersehbaren Änderungen im Bewusstsein und Verhalten der Menschen nicht ignoriert werden, die neue Freizügigkeit im Internet, aber auch der alltägliche selbstverständliche Umgang mit Informationstechnik. Bereits in den Ursprungsjahren des Datenschutzes ging es ja nicht darum, den Einzelnen vor jeglicher Form von Verarbeitung seiner Daten zu bewahren, sondern es ihm zu ermöglichen, selbst darüber zu bestimmen, „wer was über ihn weiß“. Diese Maxime ist allerdings unter den Bedingungen des Internets und der allgegenwärtigen Datenverarbeitung, wo Daten quasi als Nebenprodukte der Kommunikation oder der Erbringung irgendwelcher Dienstleistungen entstehen, heute unrealistischer denn je. Die zunehmende Komplexität technologischer Systeme erschwert die Herstellung von Transparenz im Sinne einer umfassenden Kenntnis des Betroffenen hinsichtlich der zu seiner Person verarbeiteten Daten. Umso wichtiger ist eine Komplexitätsreduktion, bei der die wesentlichen Informationen vermittelt und dem Einzelnen eine faktische Möglichkeit zur Entscheidung über echte Alternativen gegeben wird. Immer umfangreichere Datenschutzinformationen und Einwilligungsklauseln bewirken eher das Gegenteil: sie werden meistens nicht einmal zur Kenntnis genommen, sondern bloß abgehakt in der Hoffnung, es werde schon nichts passieren. So wünschenswert eine möglichst hohe Granularität der von den Betroffenen einzustellenden Systemparameter sein mag, sind doch die meisten Nutzer damit hoffnungslos überfordert. Von entscheidender Bedeutung wird es deshalb sein, die Grundeinstellung technologischer Systeme datenschutzfreundlich zu gestalten, das heißt, sie auf Datenvermeidung und Datensparsamkeit auszulegen (vgl. Nr. 8 ff.).

Schließlich darf nicht vergessen werden, dass die wesentlichen Wertentscheidungen unserer Gesellschaft in der Verfassung niedergelegt sind. In der demokratischen Informationsgesellschaft gebührt dem Schutz des Rechts auf informationelle Selbstbestimmung auch explizit Verfassungsrang. Es überzeugt einfach nicht, dass diejeni-

gen, die Artikel 13 (Unverletzlichkeit der Wohnung) und Artikel 16 GG (Asylrecht) im Stile einer Verwaltungsvorschrift ergänzt haben, um diese Grundrechte einzuschränken, nun gegen die Aufnahme des Datenschutzes in die Verfassung damit argumentieren, man dürfe dieselbe nicht unnötig aufblähen.

Entscheidend für eine nachhaltige Verbesserung des Datenschutzes in Deutschland sind aber nicht nur die gesetzlichen Bestimmungen. Die besten Vorschriften nützen wenig, wenn ihre Einhaltung nicht überwacht und Rechtsverstöße nicht sanktioniert werden. Die Datenschutzaufsichtsbehörden in Deutschland sind gemessen an ihren stetig wachsenden Aufgaben hoffnungslos unterbesetzt und haben kaum rechtliche Möglichkeiten, rechtswidrige Datenverarbeitungen zu unterbinden und festgestellte Verstöße wirksam zu sanktionieren. Dies gilt auch für meine Dienststelle (vgl. Nr. 15.11). Den Bürgerinnen und Bürgern ist nicht zu vermitteln, wenn Eingaben unverhältnismäßig lange in Bearbeitung sind und ihnen nicht mit dem gebotenen Nachdruck nachgegangen werden kann. Noch weniger ist ihnen zu vermitteln, dass die Datenschutzaufsicht insbesondere im nicht-öffentlichen Bereich nur sehr sporadisch von sich aus Kontrollen vornehmen und rechtswidrige Datenverarbeitungen aufdecken kann. So wächst Staatsverdrossenheit, wie die wachsende Zahl von Eingaben zeigt, die sich mit der vermeintlichen Hilf- und Wirkungslosigkeit der Datenschutzaufsicht auseinander setzen. An dieser Stelle müssen die Weichen neu gestellt werden, wenn die Lage des Datenschutzes in Deutschland nachhaltig verbessert werden soll.

2 Datenschutzrechtlicher Rahmen

2.1 Weiterentwicklung des Datenschutzrechts

Die grundlegende Modernisierung des Datenschutzrechts wird weiter verschoben. Initiativen gibt es nur zu einzelnen Bereichen.

Das in seiner Grundstruktur aus den siebziger Jahren des vorigen Jahrhunderts stammende BDSG bedarf einer grundlegenden und umfassenden Modernisierung (vgl. etwa 21. TB Nr. 2.1). Die Diskrepanz zwischen der Situation, auf die das Gesetz seinerzeit zugeschnitten wurde, und der zwischenzeitlich vollzogenen rasanten Entwicklung der Informationstechnologie wird immer größer. Dadurch kommt es zunehmend zu Fehlentwicklungen, deren Rückführung sehr viel schwieriger und aufwändiger werden wird, als wenn sie von vornherein datenschutzrechtlich begleitet worden wären. Deshalb findet die Forderung nach einer grundlegenden Modernisierung und Weiterentwicklung des Datenschutzrechts volle Unterstützung. Auch der Deutsche Bundestag hat dies bereits mehrfach angemahnt. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Frühjahr 2008 in Berlin noch einmal auf die Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts hingewiesen (Berliner Erklärung, vgl. Kasten zu Nr. 2.1). Dennoch sind auch im Berichtszeitraum keine wesentlichen Schritte in diese Richtung eingeleitet worden, sieht man einmal von den eher bescheidenen Ansätzen zur Änderung des BDSG in der 14. Legislaturperiode ab, die jedoch das Grundproblem des Datenschutzrechts, seine unübersichtliche Struktur und teilweise unangemessene Regelungsansätze, nicht lösen werden. Die im Jahre 2001 verabredete sog. zweite Stufe der Novellierung des BDSG, die eine weit reichende Überarbeitung des Datenschutzrechts zum Gegenstand haben sollte, wird damit immer dringender.

Gleichwohl war die seit meinem letzten Tätigkeitsbericht verstrichene Zeit nicht nur von Stillstand gekennzeichnet.

So hat das Bundesverfassungsgericht am 27. Februar 2008 eine historische Entscheidung getroffen (vgl. 1 BvR 370/07) und ein neues Grundrecht entwickelt – das Grundrecht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Ebenso wie das im Volkszählungsurteil 1983 entwickelte Recht auf informationelle Selbstbestimmung ist es eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts.

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schützt die Bürgerinnen und Bürger vor den neuartigen Gefahren, die mit der Nutzung von vernetzten Computern, mobilen und multifunktionalen Geräten verbunden sind. Angesichts des ungebremsten technischen Fortschritts und der gewandelten Lebensverhältnisse sind informationstechnische Systeme allgegenwärtig und für viele Menschen unverzichtbar. Personalcomputer, Mobiltelefone, Kleinstcomputer, Unterhaltungsgeräte oder sonstige elektronische Geräte, z. B. Navigationssysteme, sind heute vertraute und unerlässliche Gebrauchsgegenstände. Die zunehmende Vernetzung dieser Systeme vertieft die Persönlichkeitsgefährdungen. Das Internet als komplexer Verbund von Rechnernetzen verdeutlicht exemplarisch diese Entwicklung. Es eröffnet den Zugriff auf eine unübersehbare Fülle von Informationen und neuen Kommunikationsmöglichkeiten (z. B. Sprachtelefonie). Folge dieser Nutzung ist die automatisierte, d. h. durch das System eigenständig und vielfach ohne das Wissen des Betroffenen vollzogene, Erhebung und Verarbeitung von Daten über das Verhalten und die Eigenschaften der Nutzer. Hieraus können weit reichende Persönlichkeitsprofile gewonnen werden.

Das neue Grundrecht gilt für alle informationstechnischen Systeme, die – allein oder vernetzt – umfängliche oder aussagekräftige personenbezogene Daten enthalten können. Nicht erforderlich ist, dass sich diese Daten bereits im System befinden. Es genügt vielmehr, dass das System derartige Daten verarbeiten kann.

Das Grundrecht schützt das Vertrauen der Berechtigten, selbst über ihr System, dessen Leistungen, Funktionen und Inhalte bestimmen zu können. Können Dritte unberechtigt auf dieses System zugreifen, liegt bereits ein Grundrechtseingriff vor – unabhängig davon, ob der Zugriff leicht oder nur mit erheblichem Aufwand möglich ist.

Dieser weit reichende Grundrechtsschutz verpflichtet nicht nur den Staat zur bestmöglichen Schutzgewährung, sondern auch die Hersteller dieser Systeme. Angesichts der stetig fortschreitenden technischen Entwicklung ist die Erfüllung dieser verfassungsgerichtlichen Verpflichtung ein dynamischer, d. h. fortwährender Prozess. Ich hoffe, dass die Konsequenzen aus dieser weit reichenden Entscheidung von den politisch Verantwortlichen erkannt und zügig umgesetzt werden.

Die Bundesregierung hat punktuell datenschutzrechtliche Probleme aufgegriffen. So hat sie im Sommer 2008 den Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes (Bundestagsdrucksache 16/10529) in das Gesetzgebungsverfahren eingebracht, durch das Scoring-Verfahren für die betroffenen Bürgerinnen und Bürger transparenter und die Tätigkeit von Auskunfteien besser geregelt werden sollen (vgl. Nr. 2.3 und Nr. 3.4.4).

Als Reaktion auf die 2008 bekannt gewordenen Missstände beim Handel mit personenbezogenen Daten hat die Bundesregierung in einem weiteren, vom Kabinett am 10. Dezember 2008 beschlossenen Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften (Bundesratsdrucksache 4/09) eine Reihe von Änderungen im BDSG und die Einführung eines bundesweiten Datenschutzaudits vorgesehen (vgl. Nr. 2.3, 2.4, 3.4.5).

Damit ist zwar insgesamt Bewegung in die datenschutzrechtlichen Regelungen gekommen, was ich durchaus begrüße. Diese notwendigen Änderungen im Detail können aber eine grundlegende Überarbeitung des Datenschutzrechts einschließlich seiner Kontroll- und Sanktionsmechanismen nicht ersetzen. Die Forderung nach einer grundlegenden Revision verliert deswegen nicht an Bedeutung, sondern wird noch dringlicher.

Kasten zu Nr. 2.1

75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008

Berliner Erklärung:
Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts

Regelungen insbesondere zum großen Lauschangriff, zur Telekommunikationsüberwachung, zur Rasterfahndung, zur Online-Durchsuchung, zur automatischen Auswertung von Kfz-Kennzeichen und zur Vorratsspeicherung von Telekommunikationsdaten haben die verfassungsrechtlich zwingende Balance zwischen Sicherheitsbefugnissen der staatlichen Behörden und persönlicher Freiheit der Bürgerinnen und Bürger missachtet. Das Bundesverfassungsgericht hat mit einer Reihe von grundlegenden Entscheidungen diese Balance wieder hergestellt und damit auch den Forderungen der Datenschutzbeauftragten des Bundes und der Länder größtenteils Rechnung getragen.

Die Herausforderungen für den Datenschutz gehen aber weit über die genannten Bereiche hinaus. Datenverarbeitungssysteme dringen immer stärker in alle Lebensbereiche ein und beeinflussen den Alltag. Das Internet ist zum Massenmedium geworden. Vielfältig sind dabei die Möglichkeiten, das persönliche Verhalten zu registrieren und zu bewerten. Der nächste Quantensprung der Informationstechnik steht unmittelbar bevor: Die Verknüpfung von Informationstechnik mit Körperfunktionen, insbesondere bei der automatisierten Messung medizinischer Parameter und bei der Kompensation organischer Beeinträchtigungen. Die Miniaturisierung von IT-Systemen geht so weit, dass demnächst einzelne Komponenten nicht mehr mit bloßem Auge wahrgenommen werden können (Nanotechnologie).

Das Handeln staatlicher und nicht-öffentlicher Stellen ist verstärkt darauf gerichtet, viele Daten ohne klare Zweckbestimmung zu sammeln, um sie anschließend vielfältig auszuwerten, beispielsweise um versteckte Risiken aufzudecken oder um persönliches Verhalten unbemerkt zu beeinflussen. Geht es der Wirtschaft etwa darum, durch Scoring-Verfahren die Kundinnen und Kunden vorab einzuschätzen, gewinnt die immer exzessivere Registrierung und automatisierte Beobachtung für staatliche Stellen an Bedeutung. In beiden Bereichen wird ganz normales Verhalten registriert, unabhängig von konkreten Gefahren oder Verdachtsmomenten. Auch diejenigen, die sich nichts haben zu schulden kommen lassen, werden einem verstärkten Kontroll- und Anpassungsdruck ausgesetzt, der Einschüchterungseffekte zur Folge haben wird.

Der Schutz der Grundrechte, nicht zuletzt des Datenschutzes, dient in einer demokratischen Gesellschaft auch dem Gemeinwohl und ist zunächst Aufgabe jeglicher Staatsgewalt. Darüber hinaus ist er eine gesamtgesellschaftliche Aufgabe. Schließlich ist jede Bürgerin und jeder Bürger auch zur Eigenverantwortung aufgerufen. Hilfen zum informationellen Selbstschutz müssen zur Verfügung gestellt werden, die es den Betroffenen ermöglichen, eine Erfassung ihres Verhaltens zu vermeiden und selbst darüber zu entscheiden, ob und wem gegenüber sie Daten offenbaren. Von zunehmender Bedeutung sind auch Projekte, die das Datenschutzbewusstsein fördern, um vor allem jüngere Menschen von einem fahrlässigen Umgang mit ihren persönlichen Daten abzuhalten.

Alle diese Maßnahmen tragen zur Entwicklung einer neuen Datenschutzkultur bei. Voraussetzung dafür ist auch, dass nicht länger versucht wird, die verfassungsrechtlichen Grenzen und Spielräume auszureizen. Stattdessen muss dem Gebot der Datenvermeidung und -sparsamkeit Rechnung getragen werden.

2.2 Der „Datenschutzgipfel“ und seine Folgen

Auf dem vom Bundesminister des Innern initiierten Spitzentreffen im September 2008 konnte Einvernehmen über einen Maßnahmekatalog zur Begrenzung des Datenhandels erzielt werden. Dieser muss auch ohne Abstriche umgesetzt werden.

Die im Frühjahr und Sommer 2008 bekannt gewordenen Datenschutzskandale, von denen einige personenbezogene Daten von Millionen Bürgerinnen und Bürgern betrafen, haben schlagartig den Umfang des Handels mit personenbezogenen Daten in das Bewusstsein von Medien, Gesellschaft und Politik gerückt (vgl. u. a. unter Nr. 11.1). Waren diese Praktiken und der vielfältige Miss-

Kasten zu Nr. 2.2

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. September 2008

Entschlossenes Handeln ist das Gebot der Stunde

Nie haben sich in der jüngeren Geschichte die Skandale um den Missbrauch privater Daten in der Wirtschaft so gehäuft wie heute und damit deutlich gemacht, dass nicht nur im Verhältnis Bürger-Staat das Grundrecht auf informationelle Selbstbestimmung bedroht ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt – zuletzt in ihrer Berliner Erklärung vom 4. April dieses Jahres – auf diese Gefahren hingewiesen, die von massenhaften Datensammlungen privater Unternehmen und ihrer unkontrollierten Nutzung ausgehen. Sie hat auch deshalb den Gesetzgeber zu einer grundlegenden Modernisierung und Verbesserung des Datenschutzrechts aufgefordert und eine neue Datenschutzkultur angemahnt.

Dass jetzt endlich im politischen und gesellschaftlichen Raum die Problematik erkannt und diskutiert wird, ist zu begrüßen. Dabei kann und darf es aber nicht bleiben, nur entschlossenes Handeln kann die Bürgerinnen und Bürger vor weiterem Missbrauch ihrer persönlichen Daten schützen und das verlorene Vertrauen wiederherstellen.

Das vom Grundgesetz garantierte Recht eines Jeden, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu entscheiden, muss endlich die ihm gebührende Beachtung finden Die Weitergabe von persönlichen Angaben zu Werbezwecken darf nur mit ausdrücklicher Einwilligung der Betroffenen zulässig sein. Daten sind mit einem Vermerk über ihre Quelle zu kennzeichnen. Der Abschluss von Verträgen darf nicht von der Einwilligung in die Datenübermittlung zu Werbezwecken abhängig gemacht werden. Verstöße gegen den Datenschutz dürfen nicht ohne Konsequenzen bleiben, sondern müssen strikt geahndet werden. Deshalb müssen die bestehenden Lücken in den Bußgeld- und Strafbestimmungen geschlossen und der Bußgeld- und Strafrahmen für Datenschutzverstöße deutlich erhöht werden. Diese Sofortmaßnahmen, die bereits Gegenstand des Spitzentreffens im Bundesministerium des Innern am 4. September 2008 waren, können vom Deutschen Bundestag noch in den bereits vorliegenden Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes aufgenommen werden.

Gesetzgeberische Maßnahmen allein helfen aber nicht weiter, wenn ihre Einhaltung nicht ausreichend kontrolliert und Verstöße nicht sanktioniert werden können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, die Datenschutzaufsichtsbehörden endlich organisatorisch, personell und finanziell in die Lage zu versetzen, ihren Beratungs- und Kontrollaufgaben flächendeckend, unabhängig und wirkungsvoll nachkommen zu können, und entsprechend der EU-Datenschutzrichtlinie mit wirksamen Einwirkungsbefugnissen auszustatten, die sie bisher nicht haben.

Außerdem müssen Konzepte zur grundlegenden Modernisierung des Datenschutzes entwickelt und umgesetzt werden. Wichtige Themen sollten dabei noch in dieser Legislaturperiode angegangen werden:

- Verbesserung der Protokollierung des Datenzugriffs in automatisierten Verfahren
- Stärkung der datenschutzrechtlichen Auskunftsrechte
- Pflicht zur Information der betroffenen Personen und der Aufsichtsbehörden bei Datenpannen und missbräuchlicher Datennutzung
- Gewinnabschöpfung aus unbefugtem Datenhandel
- Einführung eines gesetzlich geregelten Datenschutzaudits, mit dem unabhängig und qualifiziert die Datenschutzkonformität von Verfahren und Produkten bestätigt wird
- Stärkung der betrieblichen Datenschutzbeauftragten als Organ der Selbstkontrolle
- Spezialisierung der Strafverfolgungsbehörden
- Anerkennung von Datenschutzbestimmungen als verbraucherschützende Normen

Nur wenn jetzt den Ankündigungen Taten folgen und entschlossen gehandelt wird, können die Bürgerinnen und Bürger künftig vor Datenmissbrauch und Verletzung ihres Grundrechts auf informationelle Selbstbestimmung besser als in der Vergangenheit geschützt werden.

brauch bis dahin nur den Datenschutzaufsichtsbehörden bekannt, deren wiederholte Hinweise und Warnungen ungehört verhallten, rückte das Thema plötzlich in die Schlagzeilen und sensibilisierte viele Menschen dafür, wie gefährdet auch ihre Privatsphäre und ihre personenbezogenen Daten sind.

Auf Initiative des Bundesministers des Innern trafen sich daraufhin am 4. September 2008 die Spitzenvertreter der Aufsichtsbehörden der Länder für den nicht-öffentlichen Bereich mit den Bundesministern bzw. -ministerinnen des Innern, der Justiz, für Ernährung, Landwirtschaft und Verbraucherschutz und dem Staatssekretär des Ministeriums für Wirtschaft und Technologie zu einem Gespräch, an dem auch ich teilgenommen habe. Hierbei verständigten sich die beteiligten Bundesressorts und die Aufsichtsbehörden der Länder in großer Übereinstimmung auf einen Maßnahmekatalog, der insbesondere folgende Eckpunkte zur Änderung der gesetzlichen Grundlagen enthielt:

– Daten sollen für Werbezwecke nur noch nach Einwilligung des Betroffenen weitergegeben werden
– Einführung eines gesetzlichen Koppelungsverbots für marktbeherrschende Unternehmen
– Erweiterung der Bußgeldtatbestände für Datenschutzverstöße
– Schaffung einer Möglichkeit, unrechtmäßig erworbene Gewinne aus illegaler Datenverwendung abschöpfen zu können.

Zusätzlich ergingen Prüfaufträge zu folgenden Punkten:

– Stärkung der betrieblichen Datenschutzbeauftragten,
– Einführung einer Kennzeichnungspflicht für die Herkunft personenbezogener Daten,
– Einführung einer Informationspflicht bei Datenschutzpannen.

Weiter kündigte der Bundesminister des Innern die Vorlage eines Datenschutzauditgesetzes an.

Parallel dazu wurde unter der Leitung des Vorsitzenden der Ständigen Konferenz der Innenminister und -senatoren der Länder, dem brandenburgischen Innenminister, eine länderoffene Arbeitsgruppe gebildet, die einerseits prüfen sollte, welche Verbesserungsmöglichkeiten es hinsichtlich des Vollzugs der Datenschutzkontrolle im nichtöffentlichen Bereich gebe, und andererseits Vorschläge zur Änderung des BDSG erarbeiten sollte. Hieran nahm neben den Vertretern von zwölf Länderaufsichtsbehörden auch der BfDI teil. Die Arbeitsgruppe hat Mitte Oktober 2008 ihren abschließenden Bericht vorgelegt, der eine Vielzahl von Vorschlägen zur Änderung des BDSG und weitere Maßnahmen enthielt.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beteiligte sich an der Diskussion und verabschiedete am 16. September 2008 eine Entschließung, die die Konsequenzen auflistet, die aus den Skandalen zu ziehen sind (vgl. Kasten zu Nr. 2.2).

2.3 Datenschutz in der Privatwirtschaft – zwei Gesetzesnovellen sollen die Rechte der Betroffenen stärken

Im Berichtszeitraum rückte der Datenschutz in der Privatwirtschaft in den Fokus. Gleich zwei Gesetzentwürfe sollen hier für mehr Transparenz und besseren Schutz personenbezogener Daten sorgen.

Entsprechend den Ergebnissen des Spitzentreffens hat das Bundesministerium des Innern im September 2008 einen ersten Diskussionsentwurf zur Änderung des BDSG vorgelegt. Während Artikel 1 des Entwurfs das angekündigte Datenschutzauditgesetz enthält (vgl. hierzu Nr. 2.4), sieht Artikel 2 als wichtigste Regelungen die grundsätzliche Abschaffung des sog. „Listenprivilegs“ in § 28 Absatz 3 Nummer 3 und ein Verbot für marktbeherrschende Unternehmen vor, Vertragsabschlüsse an die Einwilligung des Vertragspartners in die Weitergabe seiner personenbezogenen Daten zu Werbezwecken zu koppeln (Koppelungsverbot). Außerdem sollten die Bußgeldtatbestände für Datenschutzverstöße erweitert und der Bußgeldrahmen erhöht werden, verbunden mit der Möglichkeit, zur Abschöpfung unrechtmäßig erworbener Gewinne aus illegaler Datenverarbeitung im Einzelfall den Bußgeldrahmen auch überschreiten zu können. Von den erteilten Prüfaufträgen wurde die Stärkung der betrieblichen Datenschutzbeauftragten durch die Einführung eines besonderen Kündigungsschutzes und die Einführung einer Informationspflicht bei Datenschutzpannen berücksichtigt, wenn auch unter einschränkenden Bedingungen (vgl. zur inhaltlichen Bewertung auch Nr. 3.4.5). Einzig die Pflicht, die Herkunft personenbezogener Daten zu kennzeichnen, fand keinen Eingang in den Entwurf, möglicherweise auch deshalb, weil Unsicherheit über die technische Realisierbarkeit dieses Vorschlags bestand (vgl. auch Nr. 8.5).

Dieses Gesetzgebungsvorhaben fand zwar viel Zuspruch in der Öffentlichkeit, stieß aber auch auf heftige Kritik der betroffenen wirtschaftlichen Kreise, die in teils drastischen Stellungnahmen auf ihrer Ansicht nach zu erwartende Auswirkungen auf Unternehmen und Arbeitsplätze hinwiesen. Die Proteste waren so heftig, dass ein Abrücken von diesem Vorhaben nicht mehr ausgeschlossen werden konnte.

Zur Unterstützung des am 4. September 2008 auf dem Spitzentreffen gefundenen Konsenses bekräftigte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf ihrer Sitzung am 6./7. November 2008 in zwei Entschließungen die Notwendigkeit, Adress- und Datenhandel künftig nur auf der Grundlage einer Einwilligung der Betroffenen zuzulassen (vgl. Kasten a zu Nr. 2.3), und die Erforderlichkeit, durch eine umfassende Informationspflicht bei Datenschutzpannen mehr Transparenz zu schaffen (vgl. Kasten b zu Nr. 2.3).

Trotz des heftigen Lobbydrucks beschloss die Bundesregierung am 10. Dezember den Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften (Bundesratsdrucksache 4/09), der trotz zahlreicher Änderungen und Ergänzungen in Einzelpunkten im Kern dem ursprünglichen

Gesetzentwurf des BMI entspricht. Ich hoffe sehr, dass jetzt auch Bundesrat und Bundestag dem Vorhaben zustimmen werden und dieses ohne weitere Abstriche noch in dieser Legislaturperiode verabschiedet werden kann. Es wäre der Öffentlichkeit nicht zu vermitteln, wenn dieses wichtige Gesetzesvorhaben, das die Konsequenz aus millionenfachem Datenmissbrauch zieht und den Bürgerinnen und Bürgern die Verfügungsmacht über ihre personenbezogenen Daten ein Stück weit zurückgeben will, doch noch am Widerstand derer scheitern sollte, die erhebliche Gewinne dadurch erzielen, dass sie ohne Zustimmung der Betroffenen mit deren Daten Handel treiben.

Kasten a zu Nr. 2.3

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008

Adress- und Datenhandel nur mit Einwilligung der Betroffenen

Der auf dem „Datenschutzgipfel“ im September 2008 gefundene Konsens, den Adress- und Datenhandel zukünftig nur auf der Grundlage einer Einwilligung zuzulassen, ist in Politik und Gesellschaft auf breite Zustimmung gestoßen. Nur eine solche Lösung respektiert das informationelle Selbstbestimmungsrecht und damit die Wahlfreiheit der Verbraucherinnen und Verbraucher. Wer davon jetzt abrücken will, verkennt die auf Grund der jüngsten Datenskandale ans Licht gekommenen Missstände, deren Ursache nicht nur in der kriminellen Energie Einzelner zu suchen ist. Um die Daten der Betroffenen tatsächlich wirksam schützen zu können, muss die Wahlmöglichkeit der Menschen von Maßnahmen flankiert werden, die die Herkunft der Daten jederzeit nachvollziehbar machten.

Die von der Werbewirtschaft gegen die Einwilligungslösung ins Feld geführten Argumente sind nicht überzeugend. Die behaupteten negativen Folgen für den Wirtschaftsstandort sind nicht zu belegen. Unabhängig davon gilt: Es gibt keine schutzwürdigen Interessen für die Beibehaltung von Geschäftsmodellen, die darauf beruhen, hinter dem Rücken und ohne Information der Betroffenen mit deren Daten Handel zu treiben. Die Einführung des Einwilligungsprinzips würde im Gegenteil zielgenaueres und wirksameres Direktmarketing erlauben. Die Bundesregierung sollte sich deshalb nicht von ihrer Absicht abbringen lassen, die beim „Datenschutzgipfel“ gegebenen Zusagen zur schnellen Verbesserung des Datenschutzes einzulösen. Sie würde es sonst versäumen, die notwendigen Lehren aus den jüngsten Skandalen zu ziehen. Der Referentenentwurf des Bundesinnenministeriums zur Änderung des Bundesdatenschutzgesetzes im Bereich des Adress- und Datenhandels (Stand: 22. Oktober 2008) zieht mit der Einwilligungslösung – bei aller Verbesserungswürdigkeit im Detail – die einzig richtige und notwendige Konsequenz aus den zahlreichen Datenskandalen und darf nicht verwässert werden.

Kasten b zu Nr. 2.3

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008

Mehr Transparenz durch Informationspflichten bei Datenschutzpannen

In den letzten Monaten hat eine Reihe von gravierenden Datenschutzverstößen die Aufmerksamkeit der Öffentlichkeit und der Medien gefunden. In vielen dieser Fälle lag der Verlust oder Missbrauch personenbezogener Daten längere Zeit zurück und war der verantwortlichen Stelle bekannt, ohne dass die Betroffenen oder die zuständige Datenschutzaufsichtsbehörde hierüber informiert worden wären. Dadurch wurde ihnen die Möglichkeit genommen, Sicherheitsmaßnahmen zu ergreifen und mögliche Schäden zu begrenzen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt deswegen die Forderung, alle verantwortlichen Stellen – grundsätzlich auch alle öffentlichen Stellen – gesetzlich zu verpflichten, bei Verlust, Diebstahl oder Missbrauch personenbezogener Daten unverzüglich die hiervon betroffenen Bürgerinnen und Bürger und die zuständigen Aufsichts- oder Kontrollbehörden sowie gegebenenfalls auch die Öffentlichkeit zu unterrichten. Dies entspricht ihrer datenschutzrechtlichen Verantwortung und ermöglicht es den Betroffenen, negative Konsequenzen solcher Datenschutzpannen abzuwenden oder einzugrenzen. Hinter diesem Interesse hat der Wunsch der entsprechenden Stellen zurückzustehen, solche Vorkommnisse geheim zu halten, um keinen Imageschaden oder keine wirtschaftlichen Nachteile zu erleiden.

Etliche Staaten haben bereits entsprechende Regelungen. Eine solche Informationspflicht würde die Transparenz erhöhen und das Vertrauen der Betroffenen in eine korrekte Datenverarbeitung stärken. Darüber hinaus würde sie einen wichtigen Anstoß geben, mehr für Datenschutz und Datensicherheit zu tun.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, entsprechende umfassende Informationspflichten für Unternehmen und öffentliche Stellen im Bundesdatenschutzgesetz und den Landesdatenschutzgesetzen zu schaffen. Die übrigen aus Anlass der Datenschutzskandale in einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16. September 2008 erläuterten Forderungen zur Novellierung des Bundesdatenschutzgesetzes werden bekräftigt.

Bereits im Sommer 2007 hatte die Bundesregierung ein Gesetz zur Änderung des Bundesdatenschutzgesetzes (Bundestagsdrucksache 16/10529) auf den Weg gebracht, das zu mehr Transparenz bei Scoring-Verfahren und klareren Regelungen für Auskunfteien sorgen soll. Nachdem ich in früheren Tätigkeitsberichten immer wieder auf datenschutzrechtliche Probleme bei Auskunfteien und Score-Verfahren hingewiesen hatte, forderte der Deutsche

Bundestag in seiner Entschließung zu meinem 20. TB vom 17. Februar 2005 (Bundestagsdrucksache 15/4597) die Bundesregierung auf, bis zum Jahresende zu prüfen, „ob und wie, etwa durch Regelungen zur Beschränkung der Profilbildung, zur Begrenzung der zentralen Auskunfteien auf branchenspezifische Auskunftssysteme und zur Stärkung der Rechtsposition der Betroffenen gegenüber zentralen Auskunfteien und ihren Vertragspartnern, ein wirksamer Schutz der Betroffenen“ erreicht werden könne (vgl. Anlage 4; 21. TB Nr. 9.1).

Der daraufhin vom BMI mit erheblicher Zeitverzögerung vorgelegte Bericht führte dann im Sommer 2007 zu einem ersten Gesetzentwurf, der aber aus unserer Sicht die Position der Betroffenen gegenüber Auskunfteien und Score-Verfahren nicht ausreichend stärkte. Die 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deswegen im Oktober 2007 in einer Entschließung Nachbesserung bei den Auskunfteiregelungen gefordert (vgl. Kasten c zu Nr. 2.3).

Nach langwierigen Beratungen und zahlreichen Änderungen wurde der Gesetzentwurf (vgl. zur inhaltlichen Bewertung Nr. 3.4.4) im August 2008 von der Bundesregierung beschlossen und dem Bundesrat zugeleitet, der seinerseits eine Vielzahl von Änderungen vorschlug, die alle darauf abzielen, den Datenschutz bei Auskunfteien und Score-Verfahren zu stärken (vgl. Bundesratsdrucksache 548/1/08). Zu meinem Bedauern hat die Bundesregierung in ihrer Gegenäußerung diese substantiellen Vorschläge ganz überwiegend nicht aufgegriffen. Die Behandlung des Gesetzentwurfs in den Ausschüssen des Deutschen Bundestages hatte bei Redaktionsschluss noch nicht begonnen. Ich hoffe sehr, dass zumindest ein Teil der Vorschläge des Bundesrats doch noch Eingang in das Gesetz finden werden.

Kasten c zu Nr. 2.3

Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2007

Gesetzesinitiativen der Bundesregierung zu Auskunfteien und Scoring: Nachbesserung bei Auskunfteienregelungen gefordert

Die fortschreitende technologische Entwicklung führt zu immer weiter reichender Erfassung und Verknüpfung von persönlichen Daten und ermöglicht deren Auswertung für Kontroll- und Präventionszwecke. In der Privatwirtschaft ist daher ein engmaschiges Netz verschiedener Auskunftssysteme und branchenübergreifender Zentraldateien entstanden, die durch Profilbildung das Verhalten eines jeden Menschen ohne dessen Wissen und Wollen abbilden und bewerten können.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass das Bundesministerium des Innern endlich damit begonnen hat, die gesetzlichen Regelungen zu den Auskunfteien zu überarbeiten und neue Regelungen zum Scoring zu schaffen.

Die vorgesehenen Regelungen zu den Auskunfteien verschlechtern die Rechtsposition der Betroffenen. Sie tragen dem sich ständig weiter entwickelnden Auskunfteimarkt und den dadurch hervorgerufenen Bedrohungen für das Recht auf informationelle Selbstbestimmung nicht hinreichend Rechnung. Ziel einer gesetzlichen Regelung muss es sein, den rasant wachsenden, branchenübergreifenden Datenaustausch zu beschränken. Es kann nicht hingenommen werden, dass Auskunfteidienste nur einseitig das Informationsinteresse der angeschlossenen Unternehmen bedienen. Sie müssen auch in stärkerem Maße die schutzwürdigen Belange der betroffenen Bürgerinnen und Bürgern berücksichtigen. Mit der im Entwurf vorgesehenen Möglichkeit, die Auskunftstätigkeit auf jegliche rechtliche und wirtschaftliche Risiken zu erstrecken, wäre zu befürchten, dass letztlich bei allen vertraglichen Beziehungen – also auch bei Versicherungs- und Arbeitsverträgen – vorab Auskunfteien eingeschaltet werden. Damit würden die allgemeinen Vertragsrisiken im Wirtschaftsleben in nicht mehr angemessener Weise einseitig auf die Kundinnen und Kunden verlagert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber auf, die Situation der Verbraucherinnen und Verbraucher deutlich zu verbessern und mit dem Gesetzesvorhaben einen fairen Ausgleich zwischen den Interessen der Wirtschaft und der betroffenen Verbraucherinnen und Verbraucher zu schaffen. Die Konferenz hält es für dringend erforderlich, die Auskunfteitätigkeit auf kreditorische Risiken zu begrenzen. Zudem fordert die Konferenz, Auskunfteidienste branchenspezifisch zu begrenzen.

Der vorgelegte Referentenentwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes sieht beim Scoring nun Ansätze für ein transparenteres Verfahren für die Betroffenen vor. Es muss jedoch darauf geachtet werden, dass dieser Ansatz auch vorbehaltlos umgesetzt wird. Das Scoring, bei dem mittels einer mathematischstatistischen Formel das zukünftige vertragstreue Verhalten eines Menschen durch einen Zahlenwert ausgedrückt wird, dringt seit Jahren in immer mehr Bereiche des Wirtschaftslebens vor. Den Betroffenen wurde jedoch bisher das Wissen darüber, wie sich der Score-Wert zusammensetzt, vorenthalten. Diese Praxis soll der Gesetzentwurf beenden. Die Betroffenen sollen Auskunft darüber erhalten, welche Daten mit welcher Gewichtung in den jeweiligen Score-Wert eingeflossen sind. Die vorgeschlagenen Regelungen gehen jedoch noch nicht weit genug. Unbedingt zu streichen ist etwa eine im Entwurf enthaltene Regelung, wonach die Auskunft mit der Begründung verweigert werden kann, es würden Geschäftsgeheimnisse offenbart.

2.4 Neuer Anlauf für ein bundesweites Datenschutzaudit

Die Diskussion um ein Datenschutzaudit bekam nach den Datenschutzskandalen des Jahres 2008 eine völlig neue Dynamik. Die Bundesregierung hat im Dezember 2008 auf Vorschlag des BMI einen neuen Entwurf für ein Datenschutzauditgesetz beschlossen.

Das als Teil eines umfassenderen Gesetzentwurfs vorgelegte Datenschutzauditgesetz (s. o. Nr. 2.2, vgl. auch 21. TB Nr. 2.4) folgt der Erkenntnis, dass durch die Förderung eines Datenschutzmanagements und die Schaffung wirtschaftlicher Anreize durch Zertifizierung Verstöße gegen datenschutzrechtliche Bestimmungen erschwert oder zumindest schneller offenbar werden. Auch wenn der vorgelegte Entwurf nur ein erster Schritt zu einer grundlegenden Modernisierung des Datenschutzes ist, enthält er doch eine Reihe positiver Aspekte.

Das vorgesehene Datenschutzaudit folgt einer – zumindest für den Datenschutz – völlig neuen Konzeption, die z. T. der Kennzeichnung von landwirtschaftlichen Erzeugnissen und Lebensmitteln nach dem Öko-Landbaugesetz, z. T. dem Umweltauditgesetz nachempfunden ist. Anders als bisherige Ansätze sollen Produkte oder Verfahren nicht einer einmaligen Zertifizierung unterworfen werden, die die zertifizierte Stelle berechtigt, ein befristetes Gütesiegel zu führen. Vielmehr ist ein Kontrollsystem vorgesehen, bei dem sich eine verantwortliche Stelle oder der Anbieter eines Datenverarbeitungssystems oder -programms der permanenten Kontrolle einer „Kontrollstelle“ unterwirft. Darüber hinaus muss eine dem Audit unterliegende Stelle weitere Anforderungen erfüllen. Dazu gehört neben der selbstverständlichen Einhaltung der datenschutzrechtlichen Vorschriften eine Anwendung von Richtlinien, die für die zu zertifizierenden Konzepte oder Einrichtungen besondere datenschutzrechtliche Anforderungen definieren.

Bei den „Kontrollstellen“ kann es sich um private oder öffentliche Stellen handeln. Sie bedürfen nach dem Gesetzentwurf meiner Zulassung, die sie unter der Voraussetzung erhalten, dass sie bestimmte Anforderungen an die Unabhängigkeit, Zuverlässigkeit und Fachkunde erfüllen. Die privaten „Kontrollstellen“ ihrerseits sollen von Landesbehörden überwacht werden.

Die besonderen Richtlinien sollen von einem Datenschutzauditausschuss erlassen werden, dem ehrenamtlich Vertreter von Datenschutzbehörden, Verwaltung und Wirtschaft angehören sollen. Der Ausschuss soll mit einer Geschäftsstelle bei meiner Dienststelle angesiedelt werden.

Der Entwurf hat zu einer kontroversen datenschutzpolitischen Diskussion geführt. Dabei wurden berechtigte Bedenken geäußert, aber auch Befürchtungen, die nach meiner Ansicht nicht zutreffen.

In meiner Stellungnahme habe ich darauf hingewiesen, dass er eine Reihe positiver Ansätze enthält: Das Audit ist freiwillig. Durch wettbewerbliche Anreize ist es geeignet, ein höheres Datenschutzniveau zu erreichen, gewährleistet durch die Anwendung der Richtlinien die Vergleichbarkeit der zertifizierten Gegenstände und weist angesichts zahlreicher Veröffentlichungspflichten eine erfreuliche Transparenz auf.

Ich halte auf dieser Grundlage auch die für die Akzeptanz des Datenschutzaudits unabdingbare Qualitätssicherung für möglich. Allerdings besteht die Gefahr, dass dieser Anspruch in der Praxis nicht umfassend eingelöst werden kann. Zum einen ist die im Gesetzentwurf vorgesehene Kontrolldichte zu gering. Zum anderen muss damit gerechnet werden, dass die für die Aufsicht über die Kontrollstellen zuständigen Landesbehörden ihre Aufgaben wegen einer nicht ausreichenden Ausstattung nicht angemessen ausführen können. Dies gilt umso mehr, als die Konzeption des Audits mit einem nicht unerheblichen personellen und organisatorischen Aufwand für die Behörden verbunden ist.

Abzuwarten bleibt außerdem, inwieweit allein der Wettbewerb zwischen den Kontrollstellen tatsächlich zu einer hohen Qualitätssicherung führt und Gefälligkeitszertifizierungen wirksam vermieden werden können.

Darüber hinaus ist die vorgesehene Stellung des Datenschutzauditausschusses verbesserungsbedürftig, da er trotz der im Entwurf geregelten Unabhängigkeit einer sehr weitgehenden Rechtsaufsicht des BMI unterliegen soll.

Den gelegentlich geäußerten Vorwurf, die europarechtlich zwingend vorgesehene unabhängige staatliche Datenschutzaufsicht werde durch den Entwurf beschränkt oder gar ersetzt, teile ich nicht. Das geplante Datenschutzaudit soll neben die staatliche Datenschutzaufsicht treten und tangiert diese nicht. Sie ist ein zusätzliches Instrument der Datenschutzkontrolle, das ergänzend zur staatlichen Aufsicht bestehen soll.

Schließlich habe ich darauf hingewiesen, dass der mit dem Gesetzentwurf verbundene erhebliche Aufgabenzuwachs für meine Dienststelle nur getragen werden kann, wenn mir die notwendigen personellen und sachlichen Ressourcen zur Verfügung gestellt werden. Dieser zusätzliche Aufwand wird von der Bundesregierung im Gesetzentwurf und dessen Begründung bereits konkret anerkannt. Ich erwarte, dass die entsprechenden Voraussetzungen im Haushaltsrecht und im Haushaltsvollzug so rechtzeitig geschaffen werden, dass das Audit mit Inkrafttreten des Gesetzes unmittelbar angewendet werden kann.

2.5 Datenschutz und Outsourcing – Ein neuer Ansatz

Die Auslagerung von Aufgaben einschließlich der damit zusammenhängenden Erhebung und Verarbeitung personenbezogener Daten auf Dritte verlangt es, die Möglichkeiten und Grenzen des Outsourcing im Bundesdatenschutzgesetz klar zu regeln.

Sowohl öffentliche Stellen als auch Unternehmen erledigen viele Arbeiten nicht mehr selbst, sondern beauftragen in zunehmendem Umfang Dritte („Outsourcing“). Auch

die Verarbeitung personenbezogener Daten durch die öffentliche Verwaltung ist von diesem Trend nicht ausgenommen. Das Spektrum reicht dabei von einfachen Hilfstätigkeiten (z. B. Datenerfassung) über die Abwicklung umfangreicher Datenverarbeitungsprozesse (Rechenzentrum) bis hin zur weitgehend selbständigen Wahrnehmung von Aufgaben durch den Auftragnehmer (Kundenbetreuung bei Krankenkassen, Gehaltsbuchhaltung). Dass bei der Auslagerung von Aufgaben besonderer Wert auf den Datenschutz gelegt werden muss, belegen einige spektakuläre Vorfälle im Berichtszeitraum (vgl. u. a. Nr. 10.2.1, 10.2.2), in denen technische und organisatorische Schwachstellen bei beauftragten Dritten zu Datenschutzpannen führten.

Die bei der Delegation von Aufgaben zu beachtenden organisations- und datenschutzrechtlichen Rahmenbedingungen habe ich bereits früher thematisiert (21. TB Nr. 2.5). Inzwischen hat die von mir geleitete Unterarbeitsgruppe des Arbeitskreises „Grundsatzfragen der Verwaltungsmodernisierung“ der Datenschutzbeauftragten des Bundes und der Länder ein Arbeitspapier zu den datenschutzrechtlichen Grundlagen der Auftragsdatenverarbeitung und des Outsourcing erstellt, das von der 76. Konferenz der Datenschutzbeauftragten von Bund und Ländern zustimmend zur Kenntnis genommen wurde. Das Arbeitspapier soll den öffentlichen Stellen als Orientierung und Handlungsempfehlung dienen, um die Einhaltung des Datenschutzes beim Outsourcing bestimmter Tätigkeiten sicherzustellen (s. Kasten zu Nr. 2.5 – der vollständige Text des Arbeitspapiers ist auf meiner Internet-Seite unter www.bfdi.bund.de abrufbar).

Outsourcing und die Verlagerung von Aufgaben machen weder vor den Landes- oder Bundesgrenzen halt, noch bleiben sie auf die jeweiligen Verwaltungsebenen beschränkt. Gerade bei solchen Konstellationen muss eine effektive Datenschutzaufsicht durch die Datenschutzkontrollinstanzen in Bund und Ländern gewährleistet werden, da die Datenschutzaufsicht bei unterschiedlichen Stellen liegen kann. Dies ist insofern eine große Herausforderung, da die Datenschutzgesetze in Bund und Ländern die Kontrollkompetenzen bei der Auftragsdatenverarbeitung unterschiedlich geregelt haben. Auch wenn geklärt ist, welche Kontrollinstanz insbesondere für den Auftragnehmer zuständig ist, müssen sich die jeweiligen Kontrollbehörden intensiv miteinander abstimmen.

Um auch hier ein bundesweit einheitliches Vorgehen zu gewährleisten, werden zurzeit durch die Unterarbeitsgruppe Empfehlungen ausgearbeitet, wie auch beim Outsourcing eine wirksame Datenschutzkontrolle ermöglicht werden kann. Wenn etwa eine Bundesbehörde einen privaten IT-Dienstleister beauftragt, gilt Folgendes:

Meine datenschutzrechtliche Kontrolle bei der Bundesbehörde erstreckt sich auch darauf, dass die in § 11 BDSG festgelegten Anforderungen eingehalten werden. Dafür ist sie mir gegenüber allein verantwortlich. Für die unmittelbare Kontrolle beim IT-Dienstleister, also beim Auftragnehmer, ist primär die Datenschutzaufsichtsbehörde des Landes zuständig, in dem der Auftragnehmer seinen Sitz hat.

Zu empfehlen ist deshalb, dass der Auftraggeber den Auftragnehmer vertraglich verpflichtet, sich im Zusammenhang mit dem Auftrag meiner Kontrolle zu unterwerfen. Damit wird sichergestellt, dass der Auftraggeber seiner Verantwortung gegenüber den Betroffenen gerecht werden und die Einhaltung des für ihn geltenden Datenschutzrechts wirksam überprüfen kann.

Die Unterwerfung kann sich aus kompetenzrechtlichen Gründen allerdings nur darauf beziehen, dass sich die für den Auftraggeber zuständige Kontrollbehörde beim Auftragnehmer Zutrittsrechte zusichern lässt und Feststellungen zum Sachverhalt treffen kann. Eine rechtliche Bewertung kann sie nur gegenüber dem gesetzlich ihrer Kontrolle unterliegenden Auftraggeber abgeben. Stellt die für den Auftraggeber zuständige Behörde beim Auftragnehmer Verstöße fest, muss sie die entsprechenden Empfehlungen oder Beanstandungen ebenfalls beim Auftraggeber anbringen. Hoheitliche Maßnahmen gegenüber dem Auftragnehmer können nur von der für ihn zuständigen Datenschutzkontrolle vorgenommen werden.

Kasten zu Nr. 2.5

Kernaussagen des Arbeitspapiers „Datenschutzrechtliche Grundlagen bei Auftragsdatenverarbeitung/ Outsourcing“:

1. Bedient sich eine öffentliche Stelle einer anderen öffentlichen oder nicht-öffentlichen Stelle zur rein technischen Abwicklung der Verarbeitung personenbezogener Daten, ist dies ein klassischer Fall der Auftragsdatenverarbeitung i. S. v. § 11 BDSG. Dies bezieht sich ausschließlich auf solche Fälle, bei denen alle Verarbeitungsschritte nach einem vom Auftraggeber vorgegebenen Algorithmus ablaufen, also z. B.:

   – Auslagerung rechentechnischer Vorgänge nach vorgegebenem Algorithmus auf externe Rechenzentren

   – Fernwartung

   – Entsorgung von Datenträgern

   – Technische Abwicklung einer virtuellen Poststelle

   Eine über § 11 BDSG hinausgehende materiell-rechtliche Befugnis ist für diese Form des Outsourcings nicht erforderlich.

2. Anders ist dies jedoch, wenn darüber hinausgehenden Aufgaben ganz oder teilweise auf eine andere Stelle übertragen werden sollen. In diesen Fällen bedarf es für die Übertragung immer einer rechtlichen Grundlage außerhalb des Datenschutzrechts. Solche organisationsrechtlichen Entscheidungen können nicht auf die rein datenschutzrechtliche Vorschrift des § 11 BDSG gestützt werden, da dieser nur die Auslagerung der Datenverarbeitung als Hilfsfunktion der Aufgabenerfüllung ermöglicht. Je nach Konstellation und (staats-)organisationsrechtlichen Anforderungen kommen hierfür Gesetze, Satzungen, Verwaltungsvereinbarungen, vertragliche Regelungen oder Organisationsentscheidungen in Betracht. Folgende Konstellationen sind denkbar:

   a) Die vollständige Verlagerung von Aufgaben auf eine andere öffentliche Stelle ist aufgrund Gesetzes oder eines Organisationserlasses möglich. Eine Übertragung auf eine nicht-öffentliche Stelle kann auf der Grundlage einer gesetzlichen Beleihung vorgenommen werden. Die damit einhergehende Übertragung der Datenverarbeitung ist als Datenübermittlung anzusehen; es handelt sich nicht um einen Fall der Datenverarbeitung im Auftrag. Beispiel:

      – Abrechnung von Reisekosten oder Festsetzung von Dienstbezügen durch eine zentrale Stelle für Beschäftigte mehrerer Dienststellen

   b) Bleibt die öffentliche Stelle Träger der Aufgabe und bedient sich lediglich für Teilaufgaben Dritter, muss zuerst die Zulässigkeit dieser teilweisen Aufgabenverlagerung geprüft werden. Bei der Ausgliederung hoheitlicher Aufgaben bedarf es eines gesetzlichen Übertragungsaktes. Beispiele:

      – Bearbeitung von Beihilfeangelegenheiten

      – Privatisierung des Maßregelvollzugs

      Bei sonstigen öffentlichen Aufgaben ist eine Übertragung auch auf vertraglicher Basis oder eine Unterstützung durch Verwaltungshelfer denkbar. Beispiele:

      – Call-Center mit bloßer Weiterleitungsfunktion

      – Inhaltliche Bearbeitung bei virtueller Poststelle

      Bei der Verlagerung rein fiskalischer Tätigkeiten genügt in der Regel eine vertragliche Vereinbarung mit dem Auftragnehmer. Beispiel:

      – Verwaltung von Liegenschaften

      Ist die Übertragung der (Teil-)aufgabe als solcher organisations- und verfassungsrechtlich zulässig, ist es möglich, die damit einhergehende Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Rahmen einer Auftragsdatenverarbeitung nach § 11 BDSG durchzuführen. Dies setzt voraus, dass die formellen Anforderungen der Vorschrift, wie z. B. strikte Weisungsgebundenheit, schriftliche Vereinbarung und Einhaltung des technisch-organisatorischen Datenschutzes erfüllt werden. Für den Betroffenen hat dies den Vorteil, dass unabhängig von der Einbindung Dritter ihm gegenüber nur eine Stelle dafür verantwortlich ist, dass mit seinen personenbezogenen Daten rechtmäßig umgegangen wird.

2.6 Outsourcing bei Trägern von Berufsgeheimnissen

Die von Ärzten, Rechtsanwälten, Steuerberatern oder anderen Berufsgeheimnisträgern eingesetzte Informations- und Kommunikationstechnik wird immer komplexer und aufwändiger. Eine Übertragung auf externe Dienstleister stößt auf datenschutz- und strafrechtliche Probleme.

Ein Fall, der sich so oder ähnlich in einer ärztlichen Praxis zutragen könnte: Ein diagnostisches Großgerät, z. B. ein MRT-Gerät, ist defekt. Der Radiologe kann den Defekt mangels Sachkenntnis nicht beheben und bestellt einen Techniker der Herstellerfirma. Um das Gerät zu reparieren, muss der Techniker auf die gespeicherten Bilder und die dazugehörigen Patientendaten zugreifen. Es erscheint auf den ersten Blick selbstverständlich, dass dies möglich sein muss. Ebenso wie in vielen vergleichbaren Fällen, bei denen Rechtsanwälte, Steuerberater oder andere Träger von Berufsgeheimnissen IT-Dienstleistungen auslagern wollen, trifft dies jedoch auf rechtliche Hindernisse.

Datenschutzrechtlich würde es genügen, die Auslagerung der rein technischen Vorgänge der Datenverarbeitung als klassische Form der Datenverarbeitung im Auftrag auf § 11 BDSG zu stützen (s. o. Nr. 2.5). Dies wird allerdings der besonderen rechtlichen Stellung der durch das Strafgesetzbuch (§ 203 StGB – s. Kasten zu Nr. 2.6) gesondert geschützten Berufsgeheimnisse, wie z. B. der ärztlichen Schweigepflicht, nicht gerecht. Anders als die datenschutzrechtlichen Anforderungen verpflichten die Berufsgeheimnisse nicht die für die Verarbeitung personenbezogener Daten verantwortliche Stelle, sondern den Träger des Berufsgeheimnisses persönlich, also beispielsweise

den einzelnen Arzt oder Rechtsanwalt. Dieser darf die vom Berufsgeheimnis geschützten Informationen grundsätzlich nur dann gegenüber Dritten offenbaren, wenn der Betroffene eingewilligt (d. h. von der Schweigepflicht entbunden) hat oder eine gesetzliche Offenbarungsbefugnis existiert. § 11 BDSG ermöglicht zwar eine Verarbeitung personenbezogener Daten durch Dritte, enthält aber keine Offenbarungsbefugnis für die vom Berufsgeheimnis geschützten Informationen.

Diese Situation ist unbefriedigend. Bedenkt man, dass – wie eingangs angedeutet – die meisten medizinischen Großgeräte eine Vielzahl sensitiver Patientendaten verarbeiten oder dass IT-gestützte Abrechnungssysteme hoch komplex sind, liegt es auf der Hand, dass den Berufsgeheimnisträgern häufig sowohl die Fachkompetenz wie auch die wirtschaftlichen Mittel fehlen, diese Systeme selbst zu betreuen. Deshalb lassen sich die Berufsgeheimnisträger im besten Falle regelmäßig von allen Kunden/Patienten/Mandanten usw. von der Schweigepflicht entbinden; im schlechteren Falle findet die Einbindung externer IT-Dienstleister in einer rechtlichen Grauzone mit dem Risiko einer Strafbarkeit nach § 203 StGB statt.

Die Unterarbeitsgruppe „Auftragsdatenverarbeitung/Outsourcing“ des Arbeitskreises „Grundsatzfragen der Verwaltungsmodernisierung“ der Datenschutzbeauftragten des Bundes und der Länder hat deshalb Lösungsmöglichkeiten diskutiert. Sie hat sich dabei fachlich auch mit dem BMJ beraten, dem seinerseits eine Studie vorliegt, die eine rein strafrechtliche Lösung vorschlägt. Diese würde aber nicht ausreichen, um das rechtliche Problem insgesamt zufrieden stellend zu regeln. Im Ergebnis der Diskussion hat sich gezeigt, dass die Mehrheit der Datenschutzbeauftragten eine Lösung favorisiert, bei der im BDSG eine möglichst eng umrissene Offenbarungsbefugnis geschaffen wird. Damit sollen die Berufsgeheimnisträger in die Lage versetzt werden, externe Anbieter mit der Durchführung und Wartung von IT-Dienstleistungen zu beauftragen. Diese Lösung ist aus meiner Sicht Regelungen in den einzelnen Berufsordnungen vorzuziehen. Bei solchen berufsspezifischen Regelungen besteht die Gefahr, dass angesichts der starken Zersplitterung des Berufsrechts kaum noch festzustellen wäre, welches Verhalten strafbar wäre. Voraussichtlich würde es zu einer Fülle sehr unterschiedlicher Regelungen kommen und möglicherweise sogar zu einem Wettstreit zwischen den Berufsgruppen um die großzügigste Befugnis zum Outsourcing.

Sofern diese Voraussetzungen für eine Regelung im BDSG geschaffen würden, müsste sichergestellt werden, dass sich die Berufsgeheimnisträger bei einer Auslagerung in dem zugelassenen Umfang nicht strafbar machen. Insofern halte ich die für sich genommen nicht ausreichende flankierende Änderung im Strafrecht für durchaus sinnvoll. Darüber hinaus müssten die strafprozessualen Rechte der Berufsgeheimnisträger – Zeugnisverweigerungsrechte und Beschlagnahmeschutz – auch für die Auftragnehmer gelten.

Kasten zu Nr. 2.6

§ 203 Strafgesetzbuch

Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,
3. Rechtsanwalt, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,
4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,

4a. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,

5. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder
6. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle

anvertraut worden oder sonst bekannt geworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2)…

2.7 Projekt D115 – Einheitliche Behördenrufnummer

Bei der geplanten Einführung einer bundesweiten Behördenrufnummer sind schwierige datenschutzrechtliche Fragen zu lösen. Insbesondere muss gewährleistet werden, dass die von verschiedenen Behörden zu unterschiedlichen Zwecken geführten personenbezogenen Daten nicht zusammengeführt werden.

Auch in Deutschland soll eine bundesweit einheitliche Rufnummer – die „115“ – eingeführt werden, die sowohl

für Bürgerinnen und Bürger als auch für die Wirtschaft als zentraler telefonischer Zugang zur öffentlichen Verwaltung in Bund, Ländern und Kommunen zur Verfügung steht (Projekt D115). Anrufer sollen unabhängig von lokalen und sachlichen Zuständigkeiten mit einer leicht zu merkenden Rufnummer schnelle und verlässliche Auskünfte von der öffentlichen Verwaltung erhalten. Bevor die „115“ zum selbstverständlichen Bestandteil unseres Kommunikationsverhaltens wird, sind nicht nur erhebliche organisatorische und technische Herausforderungen zu meistern, sondern auch datenschutzrechtliche Fragen zu lösen.

Zentraler Baustein der Infrastruktur von D115 sind die kommunalen Service-Center, die von den Kommunen selbst oder in ihrem Auftrag von privaten Anbietern betrieben werden sollen. In einigen Regionen sind solche Service-Center bereits in Betrieb, wie z. B. das Call-Center Köln/Bonn/Leverkusen oder das Berlin Telefon 900. Diese regional begrenzten Lösungen sollen in das bundesweite Verfahren integriert werden.

Sobald ein Anrufer die Nummer 115 wählt, geht der Anruf bei dem Service-Center in seiner Region ein. Deshalb werden die Anrufe zunächst vom jeweiligen Netzbetreiber (Festnetz, Mobilfunk oder Voice over IP) an den für D115 tätigen Netzbetreiber, die Deutsche Telekom AG (DTAG), übergeben. Die DTAG leitet die Anrufe an einen weiteren Dienstleister, die dtms GmbH, weiter. Die dtms GmbH verteilt die Anrufe an das regional zuständige Service-Center. Bei zu hohem Anrufaufkommen können Anrufe auch an ein anderes Service-Center gesteuert werden (vgl. Kasten zu Nr. 2.7).

Bei der geografischen Zuordnung der Anrufe an das örtliche Service-Center ist strikt darauf zu achten, dass nur die für die Zuordnung erforderlichen geografischen Angaben erhoben werden. Eine genaue adressscharfe Ortung der Anrufer muss auf jeden Fall unterbleiben. Die Projektleitung hat hierzu eine akzeptable Lösung entwickelt: Bei Anrufen aus dem Festnetz wird ausschließlich die Ortsnetzkennzahl, also die Vorwahl, genutzt. Bei Anrufen aus den Mobilfunknetzen wird die auf der Funkzelle basierende Standortinformation in eine Zielinformation (Amtlicher Gemeindeschlüssel oder Ortsnetzkennzahl) umgewandelt. Bei Anrufen aus internetbasierten Netzen soll eine geografische Zuordnung nicht vorgenommen werden. Damit ist sichergestellt, dass im Service-Center der genaue Aufenthaltsort der Anrufer nicht bekannt ist.

Der größte Teil der Anrufe soll bereits im Service-Center („First Level“) beantwortet werden und zwar unabhängig davon, ob die Kommune, die das Service-Center betreibt, hierfür zuständig ist oder nicht. Um die Fragen sachkundig, schnell und korrekt beantworten zu können, soll den Mitarbeitern der Service-Center eine Wissensdatenbank zur Verfügung stehen. Erst wenn sie die Fragen nicht beantworten können, etwa weil sie zu fachspezifisch sind oder ein konkretes Verwaltungsverfahren betreffen, wird der Anrufer an ein zentrales oder ressortspezifisches Service-Center eines Landes oder des Bundes oder ein anderes kommunales Service-Center weitergeleitet („Second Level“). Kann dem Anrufer auch hier nicht weitergeholfen werden, wird der Anruf an die zuständige Fachbehörde weitergegeben („Third Level“). Im Feinkonzept wird großer Wert darauf gelegt, dass in all diesen Fällen keine personenbezogenen Daten verarbeitet oder genutzt werden.

Neben der sofortigen Beantwortung oder der Weiterleitung der Anrufe sollen die Anliegen in elektronischer Form erfasst und an die jeweils zuständige Stelle weitergeleitet werden. Daher werden auch personenbezogene Daten erhoben und verarbeitet. Ich habe großen Wert darauf gelegt, dass in derartigen Fällen die ausdrückliche Einwilligung des Anrufers eingeholt wird. Ich halte hierfür eine mündliche Einwilligung für ausreichend, die nach § 4a BDSG aufgrund besonderer Umstände ausnahmsweise zulässig ist. Wichtig ist aber, dass sich die Anrufer eindeutig identifizieren und die Einwilligungen dokumentiert werden.

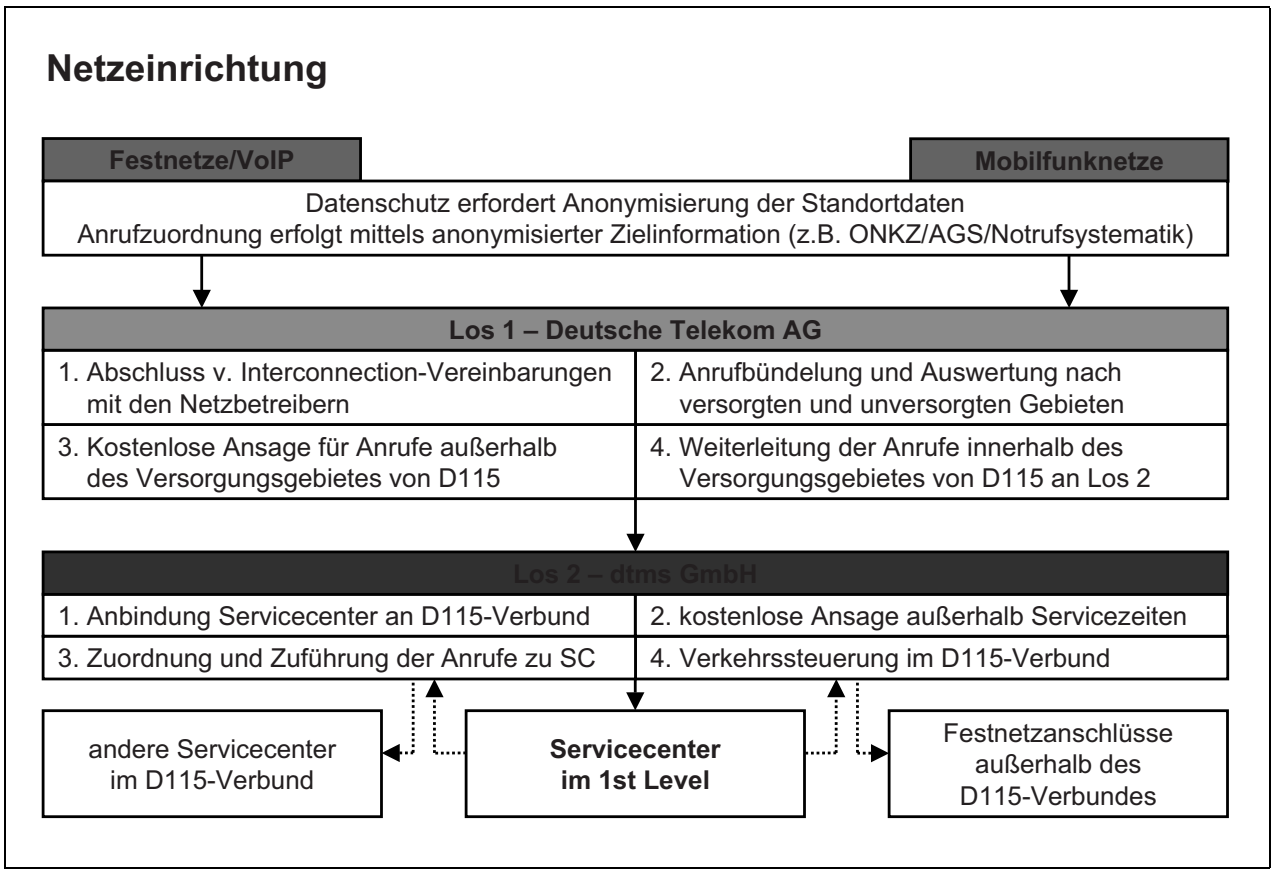
Sofern personenbezogene Daten zum Zwecke einer erneuten Auskunftserteilung oder der Weiterverfolgung eines Anliegens auf Wunsch der Anrufer gespeichert werden, erfolgt dies ausschließlich lokal im jeweiligen Service-Center. Die Daten sind zu löschen, wenn sie nicht mehr erforderlich sind. Auf meine Empfehlung wurde die maximale Speicherdauer nach abschließender Bearbeitung auf drei Monate begrenzt. Während der Test- und Pilotphase ist zu prüfen, inwieweit eine weitere Verkürzung möglich ist.

Falls eine Kommune das Service-Center nicht selbst betreibt, sondern hiermit ein privates Unternehmen beauftragt, sind weitere Anforderungen zu beachten. So muss zunächst geprüft werden, in welchem Umfang und auf welcher Grundlage eine Beauftragung überhaupt möglich ist, ohne dass dabei datenschutzrechtliche Belange beeinträchtigt werden (zu den Anforderungen bei der Auftragsdatenverarbeitung s. Nr. 2.5).

Datenschutzrechtlich problematisch war die ursprünglich vorgesehene Option, eingehende Drohanrufe aufzuzeichnen. Ich habe die Projektleitung darauf hingewiesen, dass es nicht zulässig wäre, zunächst alle eingehenden Anrufe automatisch aufzuzeichnen und durch eine entsprechende Signalisierung die Drohanrufe lediglich nachträglich von der Löschung auszunehmen. Diese generelle – wenn auch nur zeitweilige – Aufzeichnung wäre unverhältnismäßig und würde gegen das strafbewehrte Verbot des heimlichen Aufzeichnens von Telefongesprächen verstoßen. Anrufe dürfen deshalb nur aufgezeichnet werden, wenn aufgrund festgelegter Kriterien anzunehmen ist, dass Drohanrufe eingehen. Die Aufzeichnung von Anrufen muss die absolute Ausnahme bleiben.

Ich werde das Projekt D115 weiterhin intensiv begleiten.

Kasten zu Nr. 2.7



2.8 Datenschutz – bloß unnötige Bürokratie?

Seit dem Volkszählungsurteil ist der Datenschutz als Grundrecht anerkannt. Dennoch muss er immer wieder unter Beweis stellen, welch hohe Bedeutung er für ein demokratisches Gemeinwesen hat. Jüngstes Beispiel: Datenschutz als Bürokratiemonster.

Am 25. April 2006 hat das Bundeskabinett das Regierungsprogramm „Bürokratieabbau und bessere Rechtsetzung“ beschlossen. Mit dem Programm soll die Wirtschaft von überflüssigen Bürokratiekosten befreit werden. Dieses Ziel ist grundsätzlich zu begrüßen. Vorsicht ist allerdings geboten, wenn im Namen einer vermeintlichen Entlastung der Wirtschaft grundrechtliche Freiheiten beeinträchtigt werden. Der für die Betroffenen nachvollziehbare Umgang mit ihren persönlichen Daten ist eine Funktionsbedingung der demokratischen Informationsgesellschaft.

Unbestreitbar verursachen Informationspflichten Kosten bei den verantwortlichen Stellen. Entsprechend dem Regierungsprogramm wurde auch geprüft, in welchem Umfang die Transparenzanforderungen des BDSG Kosten verursachen. Nach Abschluss der Messungen wurden im Bundesdatenschutzgesetz 35 Informationspflichten identifiziert, deren Erfüllung die Wirtschaft jährlich mit mehr als 212 Mio. Euro belasten sollen. Dies ist gegenüber den ermittelten Gesamtbelastungen in Höhe von rund 47,6 Mrd. Euro zwar nur eine kleine Summe. Dennoch zählen drei zentrale Transparenzanforderungen sogar zu den 100 kostenaufwändigsten Informationspflichten:

– Hinweispflicht nach § 4a Absatz 1 Satz 2 BDSG

  Mehr als 58 Mio. Euro soll es Unternehmen jährlich kosten, die Betroffenen im Falle einer Einwilligung in eine Datenverarbeitung auf deren Zweck hinzuweisen. Dies ist die vermeintlich kostenaufwändigste Informationspflicht im Datenschutzrecht. Pro Jahr soll sie in geschätzten 6 046 000 Fällen erteilt werden, dies entspräche Kosten in Höhe von ca. 9,63 Euro pro Fall. Für die betroffenen Unternehmen ist die Einholung dieser Einwilligung jedoch ein standardisiertes Massengeschäft. In den allermeisten Fällen handelt es sich hierbei um die Unterschrift unter ein standardisiertes Formblatt. Gerade diese Einwilligung ermöglicht der Wirtschaft zudem erst eine umfangreiche Datenverarbeitung. Ansonsten wäre etwa ein Großteil der Datenverarbeitung für Werbemaßnahmen oder im Rahmen von Kundenbindungssystemen unzulässig.

– Unterrichtungspflicht, Unterrichtung des betrieblichen Datenschutzbeauftragten nach § 4g BDSG

  Fast 50 Mio. Euro soll die Umsetzung dieser Pflicht kosten, die es den betrieblichen Datenschutzbeauftrag-

ten ermöglicht, sich einen Überblick über die Datenverarbeitung in ihrem Betrieb zu verschaffen und dementsprechend zu beraten, Mitarbeiter zu schulen und Missbräuchen vorzubeugen.

– Werbewiderspruch nach § 28 Absatz 4 Satz 2 BDSG

  Diese Pflicht, die Betroffenen über ihre Rechte zu informieren, der Nutzung ihrer Daten für Werbemaßnahmen zu widersprechen, soll die Wirtschaft pro Jahr mehr als 45 Mio. Euro kosten. Zugrunde gelegt wurde eine Zahl von lediglich 460 000 Fällen im Jahr. Dies entspräche pro Fall Kosten in Höhe von 98,44 Euro. Dieses Verfahren ist jedoch standardisiert. Die Betroffenen werden nicht individuell angesprochen.

Der Datenschutz ist aber nicht nur Ausprägung eines Grundrechts; das BDSG setzt auch europarechtliche Vorgaben um, welche wiederum in engem Zusammenhang mit den Verbürgungen der Europäischen Menschenrechtskonvention und der Grundrechtecharta stehen. Eine reine Kostenmessung lässt auch außer acht, dass viele Formen der Datenverarbeitung ohne Transparenzpflichten gegenüber den Bürgerinnen und Bürgern gar nicht zulässig wären. Bei der Ermittlung der Bürokratiekosten fehlt die Gegenrechnung: Wie hoch sind die Gewinne der Wirtschaft durch die Datenverarbeitung? Demgegenüber fallen die vermeintlichen Kosten nicht ins Gewicht.

Obwohl im Rahmen der Bürokratiekostenmessung immer wieder betont wird, dass es nicht darum gehen kann, unverzichtbare rechtliche Anforderungen zu streichen, wird doch im Wege dieser scheinbar neutralen Kostenmessung gegenüber den betroffenen Sachbereichen ein Rechtfertigungsdruck aufgebaut. Dies ist im Falle des Datenschutzrechtes umso bedauerlicher, als eine Modernisierung und Vereinfachung des Bundesdatenschutzgesetzes seit Jahren überfällig ist. So ließe sich die Effizienz der Transparenzpflichten ggf. durch klarere Formulierungen der Datenschutzinformationen noch steigern. Hierzu hat etwa die Artikel-29-Gruppe einen Vorschlag erarbeitet, der bislang nur in wenigen Bereichen umgesetzt wurde (Stellungnahme zu einheitlicheren Bestimmungen über Informationspflichten 11987/04/DE vom 25. November 2004 – 10/2004, WP 100).

Ich begrüße jedoch, dass nunmehr im Vorabbericht 2008 zu den datenschutzrechtlichen Transparenzanforderungen – insbesondere zu den o. g. Pflichten – vermerkt wurde, dass die Prüfung abgeschlossen und keine Änderungen möglich seien.

2.9 Datenschutz bei Kindern – wer nimmt ihre Rechte wahr?

Ab welchem Alter und in welchem Umfang Kinder und Jugendliche eigenständig ihre Datenschutzrechte wahrnehmen können, ist nicht eindeutig geklärt.

Immer wieder stelle ich große Unsicherheit fest, wenn es um die Ausübung der Datenschutzrechte bei Kindern und Jugendlichen geht (vgl. hierzu Kasten zu Nr. 2.9). Das Bundesdatenschutzgesetz enthält keine Regelung, wann etwa ein Minderjähriger selbst Auskunft über die zu seiner Person gespeicherten Daten verlangen oder wirksam eine datenschutzrechtliche Einwilligung abgeben kann. Da das Recht auf informationelle Selbstbestimmung nach der Rechtsprechung des BVerfG Grundrechtscharakter hat, ist seine Ausübung in Form der vom BDSG eingeräumten Rechte Grundrechtswahrnehmung, die grundsätzlich den Betroffenen selbst unabhängig von ihrem Alter zukommt, soweit sie über die erforderliche Reife und Einsichtsfähigkeit verfügen. Anders sind Fälle zu beurteilen, in denen es um rechtsgeschäftliche Willenserklärungen geht; hier greifen die Vorschriften der §§ 104 ff. BGB. So wird sich z. B. bei Vertragsabschlüssen die damit verbundene Einwilligung in bestimmte Formen der personenbezogenen Datenverarbeitung nicht vom restlichen Vertrag trennen lassen. Nicht immer hat aber die Inanspruchnahme der durch das BDSG eingeräumten Rechte rechtsgeschäftlichen Charakter, so dass die Abgrenzung oft schwierig ist. Konflikte können auch dort entstehen, wo Jugendliche ihre Datenschutzrechte anders ausüben wollen als die Erziehungsberechtigten oder gesetzlichen Vertreter, etwa beim Einstellen von Fotos oder der Preisgabe persönlicher Angaben im Internet.

Eine vergleichbare Problematik stellt sich auch bei der Interpretation der Europäischen Datenschutzrichtlinie (Richtlinie 95/46/EG), die ebenfalls keine speziellen Bestimmungen zum Datenschutz bei Kindern und Jugendlichen enthält. Die Artikel-29-Gruppe hat deswegen diese Thematik aufgegriffen und am 18. Februar 2008 das „Arbeitspapier 1/2008 zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen)“ angenommen. Darin wird die Problematik in ihrer ganzen Bandbreite aufbereitet. Für die Ausübung der Datenschutzrechte betont das Papier die Bedeutung des Reifegrads des Kindes. Zudem werden die Rechte der gesetzlichen Vertreter für die Fälle erörtert, in denen die Offenlegung personenbezogener Daten dem Wohl des Kindes schaden würde. Die Bestimmungen der Europäischen Datenschutzrichtlinie sollen mit Rücksicht auf den Grundsatz des Kindeswohles angewandt werden. Wichtig ist auch, dass Kinder und Schüler zu mündigen Bürgern der Informationsgesellschaft erzogen werden. Den Datenschutzbehörden weist das Arbeitspapier im Zusammenhang mit dem Datenschutz für Kinder neben ihrer Kontrollfunktion als Aufgaben Aufklärung und Information, Einflussnahme auf die politischen Entscheidungsträger im Interesse der Kinder und Sensibilisierung der für die Datenverarbeitung Verantwortlichen für die besonderen Schutzbedürfnisse Minderjähriger zu (vgl. zum Schutz der Privatsphäre von Kindern im Internet Nr. 13.9; Anlage 8).

Ich hoffe, dass dieses Arbeitspapier, das ausdrücklich zu Kommentierung und Stellungnahme auffordert, weitere Diskussionen anstößt und dazu beiträgt, die vielfach noch unbefriedigende Situation zu verbessern, und – soweit nötig – auch zu gesetzlichen Präzisierungen führt.

Kasten zu Nr. 2.9

Beispiele für Konfliktsituationen:

- Auskunftsanspruch gegenüber der Schule:
  - Können Schülerinnen und Schüler den Anspruch eigenständig geltend machen und ab welchem Alter?
  - Kann ihnen entgegengehalten werden, ihre Eltern hätten bereits Auskunft erhalten?
  - Haben die Eltern einen Anspruch auf Auskunft, auch wenn der betroffene Jugendliche dies ausdrücklich nicht wünscht?
- Einwilligung in die Veröffentlichung von Fotos:
  - Bedarf es der Einwilligung sowohl der Eltern als auch des Jugendlichen?
  - Können die Eltern gegen den ausdrücklichen Willen des Jugendlichen wirksam einwilligen?
  - Kann umgekehrt der Jugendliche gegen den ausdrücklichen Willen der Eltern wirksam einwilligen?
- Einwilligung in die Verarbeitung personenbezogener Daten zu Werbezwecken:
  - Reicht die Einwilligung des Jugendlichen und gegebenenfalls ab welchem Alter?
  - Können die Eltern gegen den Willen des betroffenen Jugendlichen einwilligen?
  - Wem steht das Widerrufsrecht zu?

3 Wirtschaft

3.1 Gibt es eine Balance zwischen informationeller Selbstbestimmung und wirtschaftlichen Interessen?

Personenbezogene Daten sind die Währung der Informationsgesellschaft – wer diese nicht preisgeben will, muss auf viele Dienste und Bequemlichkeiten verzichten, erleidet sogar finanzielle Nachteile. Ohne Suchmaschinen lässt sich das Internet nicht mehr erschließen. Der Handel mit persönlichen Informationen scheint aus dem modernen Wirtschaftsleben nicht mehr wegzudenken zu sein. Und es gibt keine Flucht in ein Robinson'sches Paradies. Ist da noch Platz für eine Balance zwischen informationeller Selbstbestimmung und wirtschaftlichen Interessen?

Vor 25 Jahren stellte das Bundesverfassungsgericht im Volkszählungsurteil (1 BvR 209/83 u. a. vom 15. Dezember 1983) fest, dass eine Gesellschaftsordnung, in der Bürgerinnen und Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß, nicht mit dem informationellen Selbstbestimmungsrecht und damit dem Menschenbild des Grundgesetzes vereinbar wäre. Obwohl sich dieses Urteil unmittelbar nur auf staatliche Datensammlungen bezieht, gelten seine Grundsätze gleichfalls für die private Datenverarbeitungen. Doch dieses Recht auf informationelle Selbstbestimmung scheint im modernen Wirtschaftsleben keinen Platz zu haben. Die Vorfälle der letzten Zeit haben vor Augen geführt, welche Gefahren mit den großen Datensammlungen in der Privatwirtschaft einhergehen.

Wirtschaftsvertreter argumentieren bisweilen damit, dass sich die Einstellung der Menschen zur Privatsphäre und zum Datenschutz wesentlich geändert habe. Man sei heute eben freizügiger. Man könne sich nicht über Datenschutzskandale ereifern und gleichzeitig seine persönlichsten Daten, Vorlieben und Interessen bei Glücksspielen oder Kundenbindungsprogrammen freiwillig preisgeben (s. u. Nr. 7.3). Ich halte dies nicht für überzeugend. Auch diejenigen, die Kundenkarten oder soziale Netzwerke nutzen, haben einen Anspruch darauf, dass ihre Konto- oder Gesundheitsdaten vertraulich behandelt werden.

Erforderlich ist gleichwohl ein grundlegender Bewusstseinswandel. Dabei ist auch zu fragen, inwieweit der Einzelne angesichts der massenhaften Datenverarbeitung und den sich immer schneller entwickelnden technischen Möglichkeiten selbst noch in der Lage ist, die Gefahren für sein Recht auf informationelle Selbstbestimmung zu überblicken. Der eigenverantwortlich handelnde Mensch ist der Maßstab einer selbst bestimmten Informationsgesellschaft, doch setzt dies Verständnis und Bildung voraus – die oft beschworene digitale Spaltung der Gesellschaft in Computerkundige und -unkundige setzt sich auch hier fort (s. u. Kapitel 7, insb. Nr. 7.2, 7.3, 7.8 sowie Nr. 8.5 und 11.1). Ohne IT-Kenntnisse kein wirksamer Schutz der Privatsphäre mehr?

Für mich ist es vor diesem Hintergrund keine Frage, dass der Staat hier die Bürgerinnen und Bürger schützen muss. Auch der Präsident des Bundesverfassungsgerichts, Professor Dr. Papier, sieht den Staat in der Pflicht, ein „angemessenes Schutzregime“ zu schaffen. Noch sehe ich hier ein erhebliches Defizit. Der Staat hat zwar bei den Sicherheitsgesetzen erheblich aufgerüstet, der Datenschutz in der Privatwirtschaft und vor allem die Frage, wie die Bürgerinnen und Bürger vor zu viel Datensammelwut in der Wirtschaft geschützt werden können, ist in der Vergangenheit häufig vernachlässigt worden. Obwohl die als Reaktion auf aktuelle Missstände initiierten Gesetzesinitiativen durchaus zu begrüßen sind, können punktuelle Verbesserungen eine grundlegende Anpassung des Datenschutzrechts an die modernen Formen der Datenverarbeitung nicht ersetzen (s. u. Nr. 3.4.4 und Nr. 3.4.5).

Eine demokratische Informationsgesellschaft ist ohne eine Ethik der Selbstbegrenzung nicht denkbar: Nicht alles was möglich ist, darf auch gemacht werden. Informationen sind nicht das Maß aller Dinge, sonst wird der Mensch zum bloßen Objekt der Information, während die Information, das einzelne Datum zum objektiven, unbestechlichen Wert erhoben wird, dem der einzelne Mensch in seiner Subjektivität und Fehlbarkeit nichts mehr entgegensetzen kann.

Es gilt, den in § 3a BDSG bereits verankerten Grundsatz von der Datenvermeidung endlich ernst zu nehmen, und zwar im öffentlichen Bereich gleichermaßen wie bei den Unternehmen. Bereits beim Design technischer Systeme, bei der Verfügbarkeit und dem Umgang mit Daten, muss stärker nach den Auswirkungen auf das menschliche Miteinander gefragt werden. Hard- und Software müssen so gestaltet werden, dass in ihnen von vornherein der Datenschutz integriert ist. Bereits an dieser Stelle müssen datenschutzrechtliche Prinzipien wie Datenvermeidung, Datensparsamkeit, Transparenz und frühest mögliche Löschung der Daten einfließen.

3.2 Telekommunikations- und Teledienste

3.2.1 Vorratsdatenspeicherung: Das Bundesverfassungsgericht hat das letzte Wort

Die zum 1. Januar 2008 in Kraft getretene gesetzliche Verpflichtung zur Vorratsdatenspeicherung musste sogleich auf den Prüfstand des Bundesverfassungsgerichts (s. Kasten zu Nr. 3.2.1).

Bereits in meinem 21. TB (Nr. 10.1) hatte ich über die EG-Richtlinie zur Vorratsdatenspeicherung (RL 2006/24/EG vom 15. März 2006) berichtet. Parallel zur mittlerweile erfolgten Verabschiedung des die Richtlinie umsetzenden Gesetzes hat es massive öffentliche Kritik gegeben. So wurden gleich mehrere Beschwerden beim Bundesverfassungsgericht eingereicht, unter ihnen eine „Massenverfassungsbeschwerde“, an der sich ca. 34 000 Bürgerinnen und Bürger beteiligten.

Kasten zu Nr. 3.2.1

Vorratsdatenspeicherung

Seit dem 1. Januar 2008 sind Telekommunikationsunternehmen in Deutschland nach §§ 113a, 113b TKG gesetzlich verpflichtet, die Verkehrsdaten ihrer Kunden für einen Zeitraum von sechs Monaten zu speichern und bei Bedarf den Strafverfolgungsbehörden, den Polizeibehörden für präventiv-polizeiliche Aufgaben sowie den Nachrichtendiensten zur Verfügung zu stellen, soweit diese über entsprechende bundes- bzw. landesgesetzliche Auskunftsbefugnisse verfügen. Für sechs Monate gespeichert werden unter anderem die Rufnummern des anrufenden und des angerufenen Anschlusses, Beginn und Ende der Verbindung nach Datum und Uhrzeit sowie die Funkzellen, in denen sich die Gesprächspartner bei Beginn eines über Handy geführten Gespräches aufhalten. Ab dem 1. Januar 2009 müssen auch die bei der Internet- und E-Mail-Nutzung anfallenden Daten (insbesondere die IP-Adressen – vgl. hierzu auch Nummer 7.11) entsprechend vorgehalten werden. Im bundesweit geltenden § 100g StPO und einigen wenigen landesgesetzlichen Regelungen in den Polizeigesetzen von Bayern und Thüringen sowie im bayerischen Verfassungsschutzgesetz finden sich mittlerweile auch einige gesetzliche Ermächtigungen, wie sie in § 113b TKG für den Abruf von Verkehrsdaten vorausgesetzt werden.

In meiner vom BVerfG erbetenen Stellungnahme zu den Verfassungsbeschwerden habe ich meine verfassungsrechtlichen Bedenken unterstrichen. Ich halte die Verpflichtung zur Vorratsdatenspeicherung für verfassungswidrig, da sie eine Verpflichtung zur Datenspeicherung begründet, die weit überwiegend Personen trifft, die keinerlei zurechenbare Veranlassung für diesen Eingriff in ihr Grundrecht aus Artikel 10 GG (Fernmeldegeheimnis) sowie in das Grundrecht auf informationelle Selbstbestimmung gegeben haben.

Zweifel bestehen bereits im Hinblick auf die Geeignetheit. Insbesondere ist die als Hauptzweck angestrebte Verbesserung der Verfolgung von Straftaten im Bereich des Terrorismus und der organisierten Kriminalität fraglich. Die Tätergruppen in diesen Bereichen zeichnen sich in der Regel durch besonders gute Kenntnisse der elektronischen Kommunikation, professionelle Abschottung und Verschleierung der eigenen Kommunikation aus. Sie haben vielfältige Möglichkeiten, um die Vorratsdatenspeicherung zu umgehen und die Spuren bei der Tatvorbereitung und Tatausführung zu verwischen.

Gravierende Zweifel an der Verfassungswidrigkeit der Regelung ergeben sich auch unter dem Gesichtspunkt der Angemessenheit. Hier wird gleich an mehreren Stellen deutlich, dass die Vorratsdatenspeicherung massive, letztlich nicht zu rechtfertigende Eingriffe in das grundrechtlich geschützte Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung mit sich bringt. Mit der Vorratsdatenspeicherung wird jeder Nutzer von Telekommunikation und somit durchweg jede Bürgerin und jeder Bürger unter einen Generalverdacht gestellt. Der Grundsatz, dass intensive Grundrechtseingriffe stets an bestimmte, hinreichend konkrete Verdachts- oder Gefahrenstufen anknüpfen müssen, wird vollständig außer Acht gelassen. Statt dessen wird – unabhängig vom Vorliegen irgendeiner Gefahrenschwelle – anlass- und verdachtslos ein Grundrechtseingriff „ins Blaue hinein“ durchgeführt. Die einzelnen Telekommunikationsnutzer müssen ständig mit der Besorgnis leben, ihr gegenwärtiges und künftiges Kommunikationsverhalten könne jederzeit gegen sie verwendet werden, was wiederum zu einer ängstlich anpassenden Verhaltensänderung bei der Nutzung von Telekommunikationsmitteln und im Extremfall sogar zum gänzlichen Verzicht auf Kommunikation führen kann. Bereits im Volkszählungsurteil (1 BvR 209, 269, 362, 420, 440, 484/83) hat das BVerfG im Hinblick auf ein solches Szenario ausgeführt, dass eine staatliche Datenerhebung und -verarbeitung ohne hinreichend konkreten Anlass, die dazu führt, dass der Bürger keine Kenntnis mehr hat, wer, was, wann, bei welcher Gelegenheit über ihn weiß, im Ergebnis zu einer Einschüchterung des Bürgers bei der Ausübung seiner kommunikativen Grundrechte und damit zu einer Verkümmerung der gelebten Demokratie führen kann.

Durch die Speicherung von Verkehrsdaten werden Rückschlüsse auf Verhaltensweisen und Interessen des einzelnen Nutzers von Kommunikationsdiensten ermöglicht. So werden auch Anrufe bei Beratungsstellen oder Berufsgeheimnisträgern registriert. Mit Hilfe der Standortdaten der Funkzelle, in der sich der mobil Telefonierende bei Gesprächsbeginn aufhält, kann regelmäßig eine Lokali-

sierung erfolgen. Auch unabhängig von den Inhaltsdaten der Telekommunikation können umfassende Persönlichkeitsbilder, Soziogramme und Bewegungsprofile erstellt werden, die über verschiedenste Lebensbereiche Auskunft geben können. Nicht vergessen werden darf darüber hinaus, dass das Risiko sowohl des vorsätzlichen Missbrauchs aber auch das fahrlässiger Datenschutzverstöße mit zunehmender Quantität der Datenbestände stetig steigt. Das zeigen auch die jüngsten Fälle, vor allem aus dem Bereich der Telekommunikation.

Mit Blick auf die Verwendung der auf Vorrat gespeicherten Daten habe ich vor allem die unangemessen niedrig gehaltene Zugriffsschwelle des § 100g StPO für Strafverfolgungsbehörden kritisiert. Obwohl die Richtlinie als Zweck der Vorratsdatenspeicherung nur die Verfolgung von schweren Straftaten nennt, erlaubt § 100g StPO die Abfrage von Verkehrsdaten bereits zur Verfolgung von Straftaten von erheblicher Bedeutung oder sogar von nicht erheblichen Straftaten, sofern diese mittels Telekommunikation begangen wurden (s. auch Nr. 5.1).

Der weitere Verlauf der Verfahren in Karlsruhe ist zur Zeit noch nicht absehbar. Die mündliche Verhandlung war bei Redaktionsschluss noch nicht terminiert. Es ist allerdings davon auszugehen, dass das BVerfG die Entscheidung eines vor dem Europäischen Gerichtshof (EuGH) anhängigen Verfahrens abwarten wollte. Irland und Slowenien hatten hier gegen die Richtlinien-Kompetenz der Europäischen Gemeinschaft (EG) zur Regelung der Vorratsdatenspeicherung geklagt und argumentieren, dass die verabschiedete Richtlinie nicht der Angleichung der Datenspeicherungspflichten in den einzelnen Mitgliedstaaten diene und somit nicht dem europäischen Binnenmarkt, der sog. Ersten Säule, unterfalle. Vielmehr solle sie primär einen Zugriff der Ermittlungsbehörden auf Verkehrsdaten europaweit einheitlich ermöglichen. Eine solche Entscheidung würde aber in die Zuständigkeit der sog. Dritten Säule und somit der Europäischen Union fallen. Der EuGH hat inzwischen mit Urteil vom 10. Februar 2009 (C-301/06) festgestellt, dass die Richtlinie auf einer geeigneten Rechtsgrundlage erlassen wurde und entsprechend die Klage von Irland und Slowenien abgewiesen. Allerdings betonte er in diesem Zusammenhang auch, dass sich die Entscheidung ausschließlich auf die Wahl der Rechtsgrundlage bezieht und nicht auf eine eventuelle Verletzung der Grundrechte als Folge der mit der Richtlinie verbundenen Eingriffe in das Recht auf Privatsphäre.

Wenn auch die Hauptsacheentscheidung des BVerfG noch aussteht, hat es mit zwei Eilbeschlüssen im Frühjahr und Herbst 2008 zwar nicht die Vorratsdatenspeicherung als solche untersagt, den Strafverfolgern, den bayerischen und thüringischen Landespolizeien und dem bayerischen Verfassungsschutz beim Zugriff auf die Vorratsdaten aber bereits vorläufig deutliche Beschränkungen auferlegt. In der Entscheidung vom 11. März 2008 (1 BvR 256/08) wurde die Verwendung der gespeicherten Daten durch die Strafverfolgungsbehörden nur unter engen Vorraussetzungen für zulässig erklärt. So dürfen die Vorratsdaten nur dann an die Strafverfolgungsbehörden übermittelt werden, wenn Gegenstand des Ermittlungsverfahrens eine schwere Straftat im Sinne des § 100a Absatz 2 StPO ist, die auch im Einzelfall schwer wiegt, der Verdacht durch bestimmte Tatsachen begründet ist und die Erforschung des Sachverhalts auf andere Weise wesentlich erschwert oder aussichtslos wäre (§ 100a Absatz 1 StPO). Die Auskunftserteilung wurde damit – wenn auch nur vorläufig – erheblich eingeschränkt. Diese Linie wurde mit einem weiteren Beschluss vom 28. Oktober 2008 (1 BvR 256/08) bestätigt. Für den Abruf von Daten zur Gefahrenabwehr durch die Polizei in Bayern und Thüringen muss demnach eine dringende Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes vorliegen oder aber eine gemeine Gefahr drohen. Im Falle eines Abrufs durch den Verfassungsschutz müssen zwingend die Voraussetzungen der § 1 Absatz 1 und § 3 des Artikel-10-Gesetzes vorliegen. In jedem Fall gilt zudem der Grundsatz, dass die abgefragten Vorratsdaten nicht für weitere Zwecke verwendet werden dürfen.

Mit den beiden Beschlüssen hat das BVerfG einen wichtigen, aber aus prozessrechtlichen Gründen noch nicht abschließenden ersten Schritt getan. Die Hauptsacheentscheidung bleibt aber abzuwarten.

3.2.2 Fall Telekom/Lehren aus dem Missbrauch von Verkehrsdaten bei der Telekom

Der Missbrauch von Verkehrsdaten bei der Deutschen Telekom AG (DTAG) verdeutlicht, dass die Stellung der betrieblichen Datenschutzbeauftragten gestärkt, ihre Personalausstattung verbessert und die Kooperation zwischen Datenschutz und Daten verarbeitenden Stellen im Unternehmen intensiviert werden muss.

Ab Ende Mai 2008 wurde sukzessive bekannt, dass in der Vergangenheit bei der DTAG Verkehrsdaten von Mitarbeitern, Aufsichtsratsmitgliedern und unternehmensfremden Personen wie Journalisten und Gewerkschaftern, aus der regulären Datenverarbeitung „abgezweigt“ und diese Daten zur Analyse eventueller Telefonkontakte und damit von Verstößen gegen die Pflicht zur vertraulichen Behandlung der Konzernstrategie und anderer interner Vorgänge an externe „Datendetektive“ weitergegeben worden waren. Als es zu Differenzen wegen der Honorierung dieser gesetzeswidrigen Leistungen kam, wurde der Fall dem „SPIEGEL“ zugespielt und fand ein großes und anhaltendes Medienecho (vgl. auch u. Nr. 11.1). Die Diskussion um den Schutz der Daten von Kunden und Mitarbeitern wird seitdem äußerst lebhaft geführt.

Telekommunikationsverkehrsdaten (vgl. Kasten zu Nr. 7.8) werden vom Fernmeldegeheimnis aus gutem Grunde geschützt: Wer wann, von wo aus, wie lange und wie oft mit wem telefoniert – das sind Informationen, die vieles über den Anrufer und den Angerufenen aussagen können. Auch unabhängig von den Inhaltsdaten lassen sich allein aus Verkehrsdaten z. B. Bewegungsprofile gewinnen und berufliche und private Kontakte, Interessen und Probleme erschließen. Die Privatsphäre muss deshalb gegen die unbefugte Offenlegung des höchstpersönlichen Kommunikationsverhaltens auch mit den Mitteln des Strafrechtes geschützt werden. Die unbefugte Weitergabe von Verkehrsdaten an Dritte wird daher in § 206 StGB

unter Strafandrohung von maximal fünf Jahren Freiheitsstrafe gestellt. Die Staatsanwaltschaft Bonn ermittelt seit Mitte letzten Jahres mit Unterstützung des Bundeskriminalamts in einem sehr umfangreichen Verfahren zu den Vorgängen bei der DTAG, das bei Redaktionsschluss noch nicht abgeschlossen war.

Die Feststellung individueller Verstöße gegen strafrechtliche Normen und die Entscheidung über die Anklageerhebung ist Aufgabe der Strafverfolgung. Demgegenüber ist die Aufgabe des Datenschutzes eher präventiver und zukunftsgerichteter Art. Wegen der laufenden Ermittlungen der Staatsanwaltschaft Bonn habe ich meine Prüfungstätigkeit bei der DTAG darauf konzentriert, die Abläufe und die datenschutzrechtlichen Risiken bei der Verarbeitung von Verkehrsdaten zu analysieren, um auf eine Reduzierung der Risiken hinzuwirken.

Die Verarbeitung von Verkehrsdaten des Festnetzes erfolgt nicht zentralisiert, sondern dezentral an zahlreichen Standorten der DTAG. Erste Aufgabe bei meinen Kontrollen in Bonn war es deshalb, einen groben Überblick über die Strukturen und Abläufe bei der Verarbeitung von Verkehrsdaten zu gewinnen. Dieser Überblick musste gemeinsam mit den beteiligten Stellen und den Mitarbeitern des Konzerndatenschutzes erarbeitet werden. Aufgrund der Vielzahl der Systeme und der verteilten Zuständigkeiten bei der DTAG war es teilweise sehr mühsam, die notwendigen Struktur- und Prozessinformationen zur Verarbeitung von Verkehrsdaten, zum Rechtemanagment und zur Protokollierung zu erhalten. Auch beim Konzerndatenschutz bestand zu Anfang meiner Kontrolle noch kein vollständiger Überblick.

Der Zugriff auf Verkehrsdaten ist für betriebliche Zwecke, nämlich insbesondere für die Abrechnung gegenüber dem Kunden, aber auch gegenüber anderen Telekommunikationsunternehmen, ferner zur rechtzeitigen Erkennung von Störungen und Missbrauchsfällen erforderlich. Ein missbräuchliches „Abzweigen“ oder Kopieren von Verkehrsdaten kann also an mehreren Punkten ansetzen. Im Interesse optimierter Prävention müssen deshalb alle „risikogeneigten“ Datenverarbeitungen analysiert und bewertet werden.

Als wesentliches Ergebnis meiner Prüfungen hinsichtlich der Verarbeitung von Verkehrsdaten im Festnetzbereich lässt sich festhalten:

Die Daten werden mehrfach an verschiedenen Stellen gespeichert. Die Verkehrsdaten zu einem Gespräch können je nach Konstellation mehrfach vollständig und zusätzlich mit verkürzter Zielrufnummer erfasst werden. Dabei werden für die Missbrauchserkennung sogar Daten der Anrufversuche erhoben. Mit Blick auf das gesetzliche Gebot der Datensparsamkeit (§ 3a BDSG) sollte hier eine deutliche Reduzierung erfolgen, auch um Missbrauchsmöglichkeiten und Tatgelegenheiten zu verringern.

Verkehrsdaten werden teils auch zu lange gespeichert. Hier muss einerseits im Unternehmen die Speicherdauer an verschiedenen Stellen überprüft und reduziert werden. Andererseits sollte auch der Gesetzgeber sich dieser Thematik annehmen. Während die Speicherdauer und der Umfang der Daten für Zwecke der Abrechnung mit dem Kunden und bei der Vorratsdatenspeicherung minutiös geregelt sind, fehlen entsprechend klare Regelungen für andere Verwendungen von Verkehrsdaten.

Die DTAG hat auf meine Aufforderung damit begonnen, die erteilten Zugriffsrechte zu überprüfen. Für eine Anwendung, mit der nur in besonderen Fällen auf Verkehrsdaten zugegriffen wird, waren allein fast 4 000 Nutzer registriert. Auch wenn zur Gewährleistung eines effizienten Service die Erforderlichkeit von Zugriffsmöglichkeiten für eine nicht geringe Zahl unternehmensinterner Nutzer grundsätzlich plausibel erscheint, bedarf es zur Minderung von Missbrauchsrisiken gleichwohl einer Überprüfung und Aktualisierung mit dem Ziel einer Reduzierung von Zugriffsmöglichkeiten. Die „Rechtehistorie“, also die Dokumentation der Zuweisung von Zugriffsrechten einzelner Mitarbeiter auf bestimmte Anwendungen und Systeme, muss zudem sicher dokumentiert werden.

Die revisions-, also manipulationssichere Protokollierung von Zugriffen auf sensible Daten gehört zu den essentiellen Forderungen des Datenschutzes. Aus der Protokollierung muss erkennbar sein, ob der Zugriff durch einen Administrator, sonstige Mitarbeiter der DTAG oder externe Kräfte erfolgt ist. Die datenschutzrechtliche Kontrolle sollte durch zentrale Zugriffsmöglichkeiten (selbstverständlich in einem streng kontrollierten Verfahren) erleichtert werden.

Ein Teil der Missbrauchserkennungssysteme wurde von Mitarbeitern aus dem Bereich der Konzernsicherheit bedient. Hier bestand technisch die Möglichkeit, Verkehrsdaten zu erheben. Konzernsicherheit und Missbrauchserkennung sind zur Risikominimierung deutlich zu separieren. Aufträge an die Konzernsicherheit sind zudem präzise und nachvollziehbar zu erteilen und zu dokumentieren. Der Konzerndatenschutz muss bei „datenschutzsensiblen“ Maßnahmen der Konzernsicherheit frühzeitig und vor dem Zugriff auf Datenbestände beteiligt werden.

Das BDSG verpflichtet die Daten verarbeitenden Stellen zur Information und Unterstützung des betrieblichen bzw. behördlichen Datenschutzbeauftragten, damit dieser seine gesetzliche Informations- und Kontrollaufgabe wirksam erfüllen kann. Letztendlich bestand beim Konzerndatenschutz der DTAG jedoch kein vollständiger und ausreichend detaillierter Überblick über die Systeme zur Datenverarbeitung. Dieser Umstand war schließlich Grund einer Beanstandung.

Die DTAG hat seit Juni 2008 einiges aufgeholt, um ähnliche Vorfälle für die Zukunft so weit als möglich auszuschließen. Aus der Vielzahl der Maßnahmen möchte ich hier nur einzelne herausheben:

Die Aufwertung der zentralen Aufgabe „Datenschutz“ wird mit der Einrichtung des neuen Vorstandes für Recht und Datenschutz und der bereits 2008 eingeleiteten Personalverstärkung deutlich. Ermittlungsaufträge für die Konzernsicherheit sollen künftig kritisch geprüft und nachvollziehbar dokumentiert werden, um die Abzweigung und den Missbrauch sensibler Daten auszuschließen. Die Analyse und Behebung datenschutzrechtlicher

Schwachstellen bleibt angesichts der dislozierten Datenverarbeitung aber eine Daueraufgabe.

Erste positive Schritte sind festzustellen; es bleibt aber viel zu tun. Die Sensibilität für Fragen des Datenschutzes ist nicht nur bei der DTAG, sondern in der ganzen Branche gewachsen. Datenschutz ist weder Selbstzweck noch ausschließlich eine Frage der Technik. Gegen intelligente Innentäter wird es auch künftig keinen absoluten Schutz geben. Durch konsequente, aufeinander abgestimmte technische, organisatorische und auch rechtliche Maßnahmen lassen sich aber Tatgelegenheiten auch für intelligente Innentäter reduzieren.

Die aktuellen Vorgänge werfen Fragen jenseits der Verantwortlichkeit des einzelnen Unternehmens auf. Auch wenn es keine Kausalität zwischen den Vorgängen bei der DTAG und der erst nach diesen eingeführten Vorratsdatenspeicherung (s. Nr. 3.2.1) gibt, liegt doch die Frage nahe, ob sich mit der Vorratsdatenspeicherung das Missbrauchsrisiko nicht weiter erhöht. Die Forderung nach Datenminimierung zwecks Missbrauchsrisikominimierung bleibt deshalb unverändert aktuell.

Der „Fall Telekom“ gibt über den Einzelfall hinaus Anlass, eine präzisere Regelung der Befugnisse von Telekommunikationsunternehmen bei der Eingrenzung von Störungen und bei der Missbrauchserkennung zur Diskussion zu stellen. Die gegenwärtigen Regelungen in § 100 Absatz 1 und 3 TKG sind sehr knapp und zumindest „interpretationsfähig“. Eine ausdrückliche und präzise beschränkte Regelung der Nutzung von Verkehrsdaten für diese Zwecke fehlt derzeit.

3.2.3 Datenschutzgerechte Ausgestaltung der Auftragsdatenverarbeitung in Call-Centern

Eine Umfrage unter verschiedenen Telekommunikationsdiensteanbietern (TK-Anbietern) zeigt, dass bei der Auftragsdatenverarbeitung durch Call-Center der Datenschutz vielfach eine zu geringe Rolle spielt.

Ob Änderung des Handy-Vertrags oder technische Probleme mit dem Internet-Zugang – Call-Center sind heutzutage für Kunden wie TK-Anbieter aus dem täglichen Leben nicht mehr wegzudenken. Um so schlimmer ist es, dass der Missbrauch von personenbezogenen Daten, wie Name, Adresse, Telefonnummer oder gar Bankverbindung, in Call-Centern immer wieder ein aktuelles Thema ist. Aus diesem Grund habe ich verschiedene TK-Anbieter gebeten, ihre Rahmenverträge mit den von ihnen beauftragten Call-Centern vorzulegen. Das Ergebnis dieser Umfrage zeigt, dass die Anbieter sich vielfach um einen höheren Datenschutzstandard bemühen, gleichwohl ein beträchtlicher Optimierungsbedarf besteht. Eine datenschutzgerechtere Ausgestaltung der Auftragsdatenverarbeitung (vgl. Nr. 2.5) durch Call-Center kann durch Einhaltung der nachfolgend genannten Punkte erreicht werden (vgl. Kasten zu Nr. 3.2.3). Die Kunden der TK-Anbieter dürfen nicht durch fehlende oder halbherzige Datenschutzstandards dem Missbrauch ihrer Daten ausgesetzt werden. Ich werde die TK-Anbieter daher über meine Forderungen in Kenntnis setzen und die Umsetzung dieser konkreten Maßnahmen überprüfen.

Kasten zu Nr. 3.2.3

Datenschutzgerechte Ausgestaltung der Auftragsdatenverarbeitung in Call-Centern

- In den Rahmenverträgen zwischen TK-Anbietern und Call-Centern sollte explizit auf die Auftragsdatenverarbeitung und ihre rechtlichen Voraussetzungen verwiesen werden (§ 11 BDSG). Eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch das Call-Center ist hier nur im Rahmen ausdrücklicher Weisungen des TK-Anbieters zulässig. Dies schließt ein, dass alle typischerweise im Call-Center zu erwartenden Sachverhalte mit konkreten Handlungsanweisungen vorgegeben werden. Ein bloßer Verweis auf die bestehenden gesetzlichen Bestimmungen (§ 9 Satz 1 BDSG) ist nicht ausreichend.
- Eine datenschutzgerechte Auftragsdatenverarbeitung beginnt beim sicheren Transport der Datensätze zum Call-Center, erstreckt sich unter anderem auf die Festlegung der Zugriffsrechte sowie auf die Protokollierung der Zugriffe und endet schließlich mit der sofortigen, datenschutzgerechten Löschung der Datensätze nach Beendigung des Auftrags. Für den gesamten Ablauf der Auftragsdatenverarbeitung bedarf es unbedingt eines Datenschutzkonzeptes, welches vom Datenschutzbeauftragten des Call-Centers entwickelt und fortgeschrieben werden muss. Es ist dem TK-Anbieter bei Vertragsschluss vorzulegen.
- Da Call-Center häufig nicht nur für einen TK-Anbieter arbeiten, sind im Falle der gleichzeitigen Auftragsdatenverarbeitung entsprechende Vorkehrungen zur organisatorischen und technischen Trennung und Verarbeitung der unterschiedlichen Datensätze zu treffen und im Datenschutzkonzept präzise vorzugeben.
- Eine Beauftragung von Subunternehmen durch die Call-Center zur Auftragserledigung lehne ich ab. Auf jeden Fall müsste diese aber nach § 11 Absatz 2 Satz 2 BDSG vorab in der schriftlichen Vereinbarung mit dem Auftraggeber festgelegt werden.
- Die Mitarbeiterinnen und Mitarbeiter des Call-Centers müssen zudem über ein datenschutzkonformes Verhalten aufgeklärt werden. Schließlich sind sie bei ihrer täglichen Arbeit zur Wahrung des Fernmeldegeheimnisses (§ 88 TKG) und des Datengeheimnisses (§ 5 BDSG) verpflichtet.
- Über die Einhaltung dieser Bestimmungen muss ein sachkundiger Datenschutzbeauftragter des Call-Centers wachen. Zudem muss dem Datenschutzbeauftragten des TK-Anbieters ein zeitlich und räumlich uneingeschränktes Kontrollrecht eingeräumt werden. Ferner ist vertraglich sicherzustellen, dass der BfDI die Datenverarbeitung, für die der TK-Anbieter verantwortlich ist, bei Call-Center uneingeschränkt kontrollieren kann.
- Sollten Verstöße gegen das Datenschutzrecht festgestellt werden, so sind die Datenschutzbeauftragten des Call-Centers sowie des TK-Anbieters unverzüglich darüber zu informieren. Verstöße sollten mit Vertragsstrafen sanktioniert werden.

3.2.4 Nicht jeder will, doch mancher kommt auch gegen seinen Willen in das Telefonbuch

Immer wieder beklagen Telefonteilnehmer, gegen ihren Willen in öffentliche Verzeichnisse eingetragen zu werden.

Öffentliche Kundenverzeichnisse, also gedruckte und elektronische Telefonbücher, die telefonische und die „Internet-Auskunft", werden häufig gerne genutzt. Viele Telefonteilnehmer wollen so auch erreichbar sein – aber eben nicht alle. Oftmals gibt es gute Gründe, die Rufnummer und/oder Adresse nicht publik werden zu lassen. Gleichwohl ist häufig festzustellen, dass Daten gegen den erklärten Willen des Anschlussinhabers veröffentlicht werden.

Bei den Betroffenen, die sich wegen eines ungewollten Eintrags ihrer Daten an mich gewandt haben, handelte es sich – wie bereits im Berichtszeitraum meines 19. TB (Nr. 11.12) – im Wesentlichen um Kunden der Deutschen Telekom AG (DTAG). Darunter waren auch mehrere Polizeibeamte, die im sicherheitssensiblen Bereich tätig sind. Durch den ungewollten Eintrag mit Rufnummer und Anschrift sahen sie ihre eigene Sicherheit sowie die ihrer Familie gefährdet. In einem Fall wurde die DTAG mit einer nicht unerheblichen Schadensersatzforderung konfrontiert, da ein nicht zu vermeidender Umzug im Raum stand.

Auf meine Nachfragen hat die DTAG immer wieder angegeben, dass ein „individueller Arbeitsfehler" Ursache für die unerwünschten Einträge gewesen sei. Auffällig war, dass die betroffenen Kunden häufig keinen neuen Anschluss beantragt, sondern einen Produktwechsel (z. B. neuer Tarif) vorgenommen hatten. Geschah dies telefonisch, konnten die Kunden den Falscheintrag erst nach Erhalt der schriftlichen Auftragsbestätigung erkennen, die ihnen nach einigen Tagen per Post zuging. Gerade bei den Mitarbeitern des telefonischen Vertriebsweges bedarf es nach meiner Einschätzung intensiver Schulungsmaßnahmen, um die „individuellen Arbeitsfehler" zukünftig zu vermeiden.

Aber auch bei der Beauftragung in den Ladengeschäften der DTAG, kam es in der Folge immer wieder zu unerwünschten Telefonbucheinträgen. Bereits Anfang 2006 hatte ich deshalb die DTAG aufgefordert, den Kunden unmittelbar nach Auftragserteilung eine Auftragsbestätigung auszuhändigen. Denn nur so können Fehler sofort erkannt und Nachteile für den Kunden vermieden werden. Seitdem hat das Unternehmen mehrfach angekündigt, die technischen Systeme entsprechend umzustellen. Immer wieder wurden die angekündigten Einführungstermine nicht gehalten. Nunmehr wurde mir als Starttermin der Januar 2009 genannt.

Auch technische Fehler führten bei der DTAG zu ungewollten Einträgen. Aufgrund entsprechender Bürgereingaben hatte ich die DTAG um eine gründliche Prüfung von Vorgängen gebeten. Daraufhin wurde festgestellt, dass es insbesondere in Fällen, in denen externe Vertriebspartner involviert waren, zu systembedingten Falscheinträgen kam. Die Software für die Verwaltung der Bestandsdaten – einschließlich Einträgen in öffentliche Verzeichnisse – wurde inzwischen im Sommer 2008 durch eine modernere Version ersetzt, welche die Fehler zukünftig vermeiden soll.

Verbesserungsbedarf besteht auch bei der Bearbeitung von Kundenbeschwerden. So mussten Kunden, die schriftlich und/oder telefonisch die Korrektur ihrer fehlerhaft eingetragenen Daten erbeten hatten, wochenlang auf eine Reaktion warten. Offenbar war vielen Mitarbeitern nicht bekannt, an welche Stelle solche Kundeneingaben weiterzuleiten sind, nämlich an den Konzerndatenschutz. Erst nachdem sie sich wegen der mangelhaften Bearbeitung ihres berechtigten Anliegens an mich gewandt hatten, wurde auf meine Aufforderung dem Wunsch der Kunden entsprochen. Eine lange Bearbeitungszeit hat in diesen Fällen aber unter Umständen unangenehme Folgen. Denn fällt der Redaktionsschluss eines gedruckten Telefonbuchs in diesen Zeitraum, werden die falschen oder ungewollten Einträge aufgenommen und stehen für mindestens ein Jahr im Telefonbuch.

3.2.5 Bonitätsprüfung bei neuen Telefonkunden

Bei der Entscheidung über den Abschluss von Handy-Verträgen nutzen die Telekommunikationsunternehmen Informationen über die tatsächliche oder angenommene Zahlungsfähigkeit der Kunden, die sie bei Auskunfteien abfragen. Die Entscheidung erfolgt oftmals (weitgehend) automatisiert. Für den Interessenten ist dieses Verfahren vielfach nicht nachzuvollziehen.

Im Rahmen einer schriftlich durchgeführten datenschutzrechtlichen Prüfung bei 23 Telekommunikationsdiensteanbietern habe ich festgestellt, dass wichtige Vorgaben des BDSG bei einem nicht unerheblichen Anteil der Unternehmen nicht beachtet wurden. Die Antworten ergaben im Wesentlichen folgende Defizite:

1. Häufig wurden die Interessenten bei Vertragsablehnung an die Wirtschaftsauskunftei verwiesen, die entsprechende Negativmerkmale oder einen schlechten Score-Wert übermittelt hatte, ohne sich mit den Argumenten des Betroffenen auseinander zu setzen. Dies entspricht weder dem Wortlaut noch der Intention des BDSG. Automatisierte Einzelentscheidungen, die zur Ablehnung eines Antrages auf Abschluss eines Telekommunikationsvertrages führen, sind nur unter den Voraussetzungen von § 6a Absatz 2 Nummer 2 BDSG zulässig. Danach muss die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet werden, z. B. durch die Möglichkeit, sich noch einmal an die verantwortliche Stelle zu wenden, um seinen Standpunkt geltend zu machen. Dazu muss dem Betroffenen mitgeteilt werden, dass überhaupt eine automatisierte Ablehnung erfolgt ist. Die verantwortliche Stelle ist dann verpflichtet, ihre Entscheidung erneut zu prüfen. Einem abgelehnten Antragsteller muss also mitgeteilt werden, wie und an wen er sich in dem entsprechenden Unternehmen wenden kann. Dabei muss es sich um Mitarbeiter handeln,

die über entsprechende Kompetenzen verfügen, um die Darstellung der Betroffenen bewerten zu können, damit die vom Gesetz geforderte erneute Prüfung durchgeführt werden kann.

2. Die von den Wirtschaftsauskunfteien im Zusammenhang mit der Bonitätsprüfung übermittelten Daten, Negativmerkmale und Score-Werte wurden häufig viel zu lange in den unternehmenseigenen Datenbanksystemen der Telekommunikationsdiensteanbieter gespeichert (in vielen Fällen drei bis zwölf Monate, in einem Fall bis zu drei Jahre). Bei Berücksichtigung des Grundsatzes der Erforderlichkeit und der für die Integrität dieser Daten notwendigen Aktualität ist nach meiner Auffassung eine Speicherdauer von maximal einem Monat zulässig. Zwar verlangt z. B. die Schufa in Einzelfällen von ihren Vertragspartnern, dass sie das berechtigte Interesse einer Abfrage innerhalb Jahresfrist nachzuweisen haben. Hier würde es jedoch genügen, die Tatsache einer Vertragsanbahnung zu dokumentieren; die Speicherung der eigentlichen Bonitätsdaten hingegen ist nicht erforderlich.

3. Eine Reihe von Telekommunikationsunternehmen haben Auskunftsersuchen nicht beantwortet, sondern die Betroffenen an die Wirtschaftsauskunfteien verwiesen, obwohl die Daten in den eigenen Datenbanken der Telekommunikationsdiensteanbieter zur Verfügung standen. Dabei blieb unberücksichtigt, dass der Auskunftsanspruch nach § 34 Absatz 1 BDSG umfassend ist. Bittet also ein Betroffener um Auskunft und erfolgt sein Auskunftsersuchen eindeutig aufgrund einer durchgeführten Bonitätsprüfung, sind ihm sämtliche zu seiner Person gespeicherten Daten in diesem Zusammenhang mitzuteilen. Der Hinweis, man könne diese Daten von der Auskunftei erhalten, würde den Rechtsanspruch des Betroffenen missachten und hätte zudem die Konsequenz, dass der Betroffene entgegen § 34 Absatz 5 Satz 1 BDSG ein Entgelt zu entrichten hätte.

Im Zuge der weiteren Erörterungen habe ich die betroffenen Telekommunikationsunternehmen aufgefordert, die erforderlichen Verfahrensänderungen vorzunehmen. Die betroffenen Unternehmen haben mir zugesichert, meine Rechtsauffassung zum Umgang mit Bonitätsdaten künftig zu beachten.

3.3 Postunternehmen

3.3.1 Anlasslose Weitergabe von Sendungsdaten in die USA

Zu Beginn des Jahres 2008 berichteten Medien von Kontrollen des interkontinentalen Briefverkehrs durch US-Behörden. Ich habe dies zum Anlass genommen, den Umgang mit personenbezogenen Daten beim Postversand in die USA zu recherchieren.

Mit dem am 5. Dezember 2003 in Kraft getretenen „Trade Act of 2002“ regeln die USA die Ein- und Ausfuhr von Waren. Von diesen Bestimmungen werden alle Warensendungen erfasst, somit auch sämtliche Postsendungen wie Briefe, Päckchen und Pakete mit Wareninhalt. Bei der Beförderung von Postsendungen mit Wareninhalt ist zwischen Sendungen, die unter den Weltpostvertrag fallen (Beförderung nur durch die Deutsche Post AG), und solchen aus dem Expressbereich (Beförderung durch alle Dienstleister z. B. DHL, UPS, TNT, Federal Express) zu unterscheiden.

Bei dem unter den Postvertrag fallenden Sendungen mit Wareninhalt gibt der Absender bei der Aushändigung an die Deutsche Post AG eine Zollerklärung ab, deren Inhalt im Weltpostvertrag festgelegt ist. Anschließend erfolgt der Versand per Luft- oder Seeweg in die USA. Die Deutsche Post AG übermittelt vorab lediglich Informationen zum Gesamtgewicht der Ladung eines Flugzeuges oder Schiffes. Daten wie Absender, Empfänger, Inhalt und Gewicht der Sendung werden nicht erfasst und können somit nicht vorweg übermittelt werden. Diese Daten erhält der amerikanische Zoll (Bureau of Customs and Border Protection, CBP) erst mit dem Eintreffen der Sendungen in den USA anhand der Zollinhaltserklärungen. In den USA werden die Sendungen von der US-Post (USPS) entgegen genommen und dem CBP zugeführt, das über eine Zollpflicht entscheidet. Danach werden die Sendungen von USPS beim Empfänger zugestellt.

Die als Expresssendungen transportierten Pakete, Päckchen oder Briefe werden vom Dienstleister selbst oder einem Partnerunternehmen dem US-Empfänger zugestellt. Abhängig vom Transportweg werden die Sendungsdaten innerhalb einer bestimmten Frist, die sich aus dem „Trade Act of 2002“ ergibt, elektronisch an das Partnerunternehmen in den USA übermittelt, das die Daten an den amerikanischen Zoll weiterleitet.

Grundsätzlich sieht der „Trade Act of 2002“ auch die Erfassung von Daten aus dem reinen Briefverkehr ohne Wareninhalt vor. Eine Umsetzung ist jedoch nur mittels eines – noch nicht vorhandenen – Ergänzungsgesetzes möglich. Ein Vorstoß der US-Seite, die Datenerfassung auf alle Postsendungen (also auch ohne Wareninhalt) auszudehnen, blieb bislang glücklicherweise erfolglos.

Obwohl ich zunehmenden Kontrollen des internationalen Postverkehrs kritisch gegenüberstehe, sind die Maßnahmen nicht durch mich zu beanstanden. Der Zugriff amerikanischer Behörden auf die Daten aus den Zollerklärungen richtet sich nach amerikanischem Recht. Das CBP gehört zum Department of Homeland Security (DHS) und nimmt sowohl die Aufgaben der Grenzpolizei als auch des Zolls wahr. Nach einer Richtlinie des Datenschutzbeauftragten des DHS wird Ausländern ein Auskunfts- und Berichtigungsrecht bezüglich ihrer Daten eingeräumt, das jedoch nicht einklagbar ist. Nach Auskunft des DHS werden die personenbezogenen Daten aus einer vorab übermittelten Zollerklärung für eine Dauer von sechs Jahren aufbewahrt. Zugriff auf die Zollerklärungen von Postsendungen haben generell sowohl der US-Postdienst als auch das CBP. Dabei ist die gezielte Datenabfrage an eine „konkrete Notwendigkeit“ geknüpft; sie wird dokumentiert und kontrolliert.

Es bleibt festzuhalten, dass seit Inkrafttreten des „Trade Act of 2002“ die US-Zollbehörden bei der Wareneinfuhr

keine zusätzlichen Daten zu einer Sendung verlangen, sondern lediglich eine neue – elektronische – Form der Aufbereitung vornehmen. Elektronisch vorliegende Daten können jedoch zweifellos einfacher aufbewahrt, ausgewertet und – ggf. auch für andere Zwecke – genutzt werden. Ebenso sehe ich die Speicherungsdauer von sechs Jahren kritisch. Da die USA in der Gestaltung ihrer Einfuhrbestimmungen frei sind, ist dies eine zwar unerfreuliche, aber von europäischer Seite wohl kaum aufzuhaltende Entwicklung. Die Erweiterung der Meldepflicht und Speicherung der sendungsbezogenen Daten auch auf Briefe – wie im „Trade Act of 2002" prinzipiell vorgesehen – hielte ich für besonders problematisch. Deshalb erwarte ich von der Bundesregierung und den EU-Institutionen, weiterhin auf den Verzicht einer derartigen Ausweitung der elektronischen Erfassung hinzuwirken.

Auch die Europäische Kommission strebt die Ablösung der papierbasierten Zollabwicklung durch ein elektronisches System an. Daher arbeitet die Deutsche Post AG zusammen mit anderen Postunternehmen an einem Verfahren zum elektronischen Austausch zollrelevanter Daten (MEDICI – Mails Electronic Data Interchange & Cutoms Integration). Die Umstellung auf ein elektronisches Verfahren darf aber nicht zu einer verlängerten Speicherung von Daten führen.

3.3.2 Prüfungen bei Postunternehmen – Einzelfälle meiner Kontrolltätigkeit

Die Öffnung des Briefmarkts für private Anbieter brachte nicht nur mehr Wettbewerb, sondern auch mehr Beschwerden über Datenschutzverstöße.

Zum Ende des Jahres 2007 lief die vom Gesetzgeber der Deutschen Post AG eingeräumte Exklusivlizenz aus: Schon lange hatten sich Hunderte lizenzierte Wettbewerber auf die Öffnung des milliardenschweren Briefmarkts vorbereitet. Doch nicht immer gingen die Umstrukturierungen vom kleinen Postdienstleister zum konkurrenzfähigen Unternehmen mit den nötigen datenschutzrechtlichen Maßnahmen einher.

Auch im Zuge der Expansion der PIN AG kam es im Unternehmen zu datenschutzrechtlichen Defiziten. Viele Petenten beschwerten sich über eine mangelhafte Zustellungsqualität. Um diese Eingaben sachgerecht beantworten zu können, bin ich auf die Zusammenarbeit mit den Unternehmen angewiesen. Umso ärgerlicher war es, dass meine Anfragen unbeantwortet blieben. Folglich konnte ich den Petenten nicht in angemessener Zeit weiterhelfen. Möglicherweise war dies darauf zurückzuführen, dass die Verantwortlichen für den Datenschutz im Unternehmen häufig wechselten. Die fehlende Mitwirkung habe ich gemäß § 25 BDSG beanstandet.

Inzwischen wurde die insolvente PIN Group AG aufgelöst, einzelne Unternehmen werden aber unter dem ursprünglichen Namen weitergeführt. So auch die PIN Mail AG in Berlin.

Das Gründungsunternehmen der PIN-Gruppe versucht, seinen Qualitätsstandard wieder zu verbessern. Anfragen zu datenschutzrechtlichen Eingaben werden nun wieder zeitgerecht und in ausreichendem Maß beantwortet. Diesen Prozess werde ich durch regelmäßige Kontrollen und Beratungsgespräche begleiten.

Zahlreiche Kontrollbesuche bei Kurier-, Paket- sowie Briefdiensten zeigen, dass viele Postdienstleister ihr Geschäft grundsätzlich datenschutzgerecht betreiben. So habe ich im Berichtszeitraum den Briefdienst des Logistikkonzerns Thomas Nationwide Transport (TNT) TNT Post kontrolliert. Der betriebliche Ablauf ist so organisiert, dass datenschutzrechtlich relevante Vorschriften eingehalten werden. Das Qualitätsmanagement bindet den Datenschutz ein und sorgt für seine Einhaltung und Fortentwicklung. Gleiches gilt auch auf die Beförderung von Waren- und Expresssendungen durch den Paketdienst TNT Express.

Immer wieder erreichen mich Bürgeranfragen, woher der Absender die Anschrift bezogen hat. Hier muss man zwei wesentliche Aspekte unterscheiden: Zum einen befördern Postdienstleister Sendungen, die mit Anschriften aus dem Adresshandel beschriftet wurden, insbesondere bei Werbesendungen. Das Postunternehmen beschränkt sich auf das Einsammeln, Befördern und Zustellen der Sendungen. In diesem Falle müssen sich die Petenten direkt an den Absender bzw. die für diesen zuständige Aufsichtsbehörde wenden.

Zum anderen darf ein Postdienstleister im Adresshandel selber tätig sein, solange er die Daten für sein Geschäft nicht aus seiner Tätigkeit als Postdienstleister bezieht.

Recht komplex stellt sich diese Materie bei der Deutschen Post AG und ihren rechtlich selbständigen Tochtergesellschaften Deutsche Post Adress GmbH und Deutsche Post Direkt GmbH dar, da die Posttöchter nicht nur eigene Daten, sondern auch Daten aus Nachsendeaufträgen im Auftrag der Deutschen Post AG verarbeiten. Während die datenschutzgerechte Erhebung, Speicherung und Nutzung der Daten aus Nachsendeaufträgen unter meine Aufsicht fällt, obliegt die datenschutzrechtliche Prüfung der Datenverarbeitung durch die Posttöchter der Aufsichtsbehörde für den nicht-öffentlichen Bereich, hier der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW). Ebenso ist die Zuständigkeit für die Deutsche Post AG außerhalb der Postdienstleistungen mit Wegfall des Postmonopols zum 1. Januar 2008 auf die LDI übergegangen. Bei der datenschutzrechtlichen Kontrolle der Anschriftenweitergabe arbeite ich mit der LDI intensiv zusammen. Datenschutzrechtliche Verstöße oder einen kritischen Umgang mit Daten konnte ich bei gemeinsamen Kontrollen nicht feststellen.

3.4 Wirtschaft allgemein

3.4.1 Die Europäische Dienstleistungsrichtlinie und das Binnenmarktinformationssystem IMI

Die Umsetzung der Europäischen Dienstleistungsrichtlinie muss bis Ende 2009 abgeschlossen sein – datenschutzrechtliche Aspekte verdienen mehr Aufmerksamkeit.

Mit der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt (EU-DLRL) wurde der Bundesregierung aufgetragen, die Inhalte dieser Richtlinie bis zum 28. Dezember 2009 in nationales Recht umzusetzen. Dadurch wird ein europaweites Verfahren zur grenzüberschreitenden Erbringung von Dienstleistungen eingeführt. Künftig sollen Handwerker und andere Dienstleistungserbringer ohne hohe bürokratische Hürden alle notwendigen Informationen und Genehmigungen erhalten, die sie für die Ausübung ihres (Dienstleistungs-) Berufes im europäischen Ausland benötigen. Zu diesem Zweck soll sich der Dienstleistungserbringer elektronisch an einen sog. Einheitlichen Ansprechpartner (EA) wenden können, bei dem er alle wichtigen Informationen einholen und die notwendigen Verfahren einleiten kann. Der EA kann in dem Genehmigungsverfahren als Mittler und „Zuständigkeitsfinder“ agieren, aber auch selbst am Verfahren als verantwortliche Stelle teilnehmen.

In Artikel 43 der EU-DLRL wird zwar darauf hingewiesen, dass die Vorschriften zum Schutz personenbezogener Daten eingehalten werden müssen, diese jedoch auf nationaler Ebene definiert werden. Insbesondere sind der Übermittlungsumfang, die Empfänger der Daten, die Speicherdauer und die Löschungs-/Tilgungsregelungen, die Auskunfts- und Änderungsrechte von Betroffenen sowie die datenschutzrechtliche Kontrolle zu konkretisieren.

Mit dem Vierten Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften (4. VwVfÄndG, BGBl. I 2008 S. 2418) wurde die grundsätzliche Möglichkeit geschaffen, über einheitliche Stellen zu kommunizieren. Im Gesetz wird lediglich das Verfahren, nicht aber die Einrichtung einer einheitlichen Stelle geregelt. Hierfür ist es erforderlich, dass die Bundesländer zunächst festgelegen, welche Stelle(n) als EA eingerichtet wird/werden. Aller Voraussicht nach wird es unterschiedliche Modelle geben, von neu zu schaffenden Behörden bis hin zu Modellen, bei denen mehrere unterschiedliche Behörden diese Aufgabe übernehmen. Die Entscheidung über die Einrichtung und die Verortung der EA obliegt einzig und allein den Bundesländern, da dem Bund keine Gesetzgebungskompetenz zusteht. Es sind Regelungen zum datenschutzgerechten Umgang mit personenbezogenen, z. T. sensiblen Daten von Dienstleitungserbringern erforderlich.

Neben der Neuerung, dass potentielle Dienstleistungserbringer direkt elektronisch mit den zuständigen Stellen kommunizieren können, wird es im Zusammenhang mit der Umsetzung der EU-DLRL auch Neuerungen in den Verwaltungsstrukturen und deren Kommunikation geben. Das Binnenmarktinformationssystem (Internal Market Information System – IMI), das bereits zur Umsetzung der Richtlinie 2005/36/EG des Europäischen Parlaments und des Rates vom 7. September 2005 über die Anerkennung von Berufsqualifikationen (Berufsanerkennungsrichtlinie) eingesetzt wird, soll um ein Modul „Dienstleistungsrichtlinie“ erweitert werden (vgl. Kasten zu Nr. 3.4.1).

Kasten zu Nr. 3.4.1

Binnenmarktinformationssystem IMI

Bei IMI handelt es sich um ein elektronisches System für den Informationsaustausch, das den Mitgliedstaaten eine effizientere Zusammenarbeit in ihren laufenden Aktivitäten erlauben und die Kommunikation unter den Verwaltungen der Mitgliedstaaten der Europäischen Union verbessern soll. Die Datenbank wird auf einem Server der Europäischen Kommission in Luxemburg gespeichert. Der gesamte Datenaustausch wird über diesen Server erfolgen, auf dem auch die ausgetauschten Daten gespeichert werden sollen. Auf europäischer, nationaler bis hin zur Benutzerebene müssen sog. IMI-Akteure und IMI-Nutzer festgelegt werden. Die Kommunikation zwischen den Behörden soll über einen in jeder Amtssprache der Europäischen Union vorformulierten Fragenkatalog weitgehend schematisiert erfolgen.

Neben dem Basismodul zum Informationsaustausch soll das IMI-Modul „Dienstleistungsrichtlinie“ noch zwei weitere Funktionen enthalten: Zum einen ein System zur Verwaltungszusammenarbeit bei Ausnahmen im Einzelfall, bei dem die Mitgliedstaaten ausnahmsweise und unter engen Voraussetzungen aus Gründen der Sicherheit der Dienstleistung Maßnahmen gegenüber einem in einem anderen Mitgliedstaat niedergelassenen Dienstleistungserbringer ergreifen können. Zum anderen der Vorwarnmechanismus, der die Mitgliedstaaten zu einer Unterrichtung von Amts wegen und ohne Anfrage im Rahmen des Basismoduls bei ernsten Gefahren für die Gesundheit oder Sicherheit von Personen oder Umwelt verpflichtet.

Seit Ende Februar 2008 befindet sich IMI im Hinblick auf die Berufsanerkennungsrichtlinie in der Pilotphase für einige Gesundheitsberufe (Ärzte, Apotheker, Physiotherapeuten) sowie Steuerberater/Wirtschaftsprüfer. Bis Ende August 2008 wurde IMI EU-weit für knapp 150 Anfragen genutzt. Deutsche Behörden haben in diesem Zeitraum 25 Anfragen über IMI versandt und sieben Anfragen erhalten. Der Großteil der Anfragen bezog sich auf die Anerkennung von ärztlichen Qualifikationen. Die meiner Kontrolle unterliegende Wirtschaftsprüferkammer in Berlin hat in diesem Zeitraum noch keine IMI-Anfrage erhalten und selbst nur eine Anfrage allgemeiner Art und ohne Personenbezug an Großbritannien gestellt. Für das Jahr 2009 ist ein Pilotprojekt für das IMI-Modul Dienstleistungsrichtlinie unter Einbeziehung von Dienstleistungen im Baugewerbe (incl. Architekten), Dienstleistungen von Immobilienmaklern, Reiseagenturen, Reiseveranstaltern und Fremdenführern, Catering und Gastronomie sowie Tierärzten vorgesehen. Anschließend soll der vollständige Betrieb für das gesamte System beginnen.

Die Artikel-29-Gruppe der europäischen Datenschutzbehörden hat zu den Datenschutzaspekten des IMI Stellung genommen (Stellungnahme Nr. 7/2007, WP 140). Die Gruppe schlägt vor, für den Datenaustausch innerhalb des

IMI eine spezifische Rechtsgrundlage zu schaffen. Die Europäische Kommission ist diesem Wunsch nur zum Teil nachgekommen (Entscheidung 2008/49/EG), denn sie hat die Verantwortung für die Datenverarbeitungsmaßnahmen weitgehend offen gelassen und sieht eine „gemeinsame Wahrnehmung der IMI-Akteure je nach Zuständigkeit in IMI“ vor.

Deshalb ist die Forderung nach Schaffung einer eigenständigen umfassenden Rechtsgrundlage immer noch aktuell. Sie muss neben der präzisen Beschreibung von Funktionen, Rechten und Pflichten der IMI-Akteure auch Aussagen zu den datenschutzrechtlichen Verantwortlichkeiten, Betroffenenrechten, Sicherheitsmaßnahmen und Kontrollen enthalten. Die Schaffung des elektronischen Zentralsystems IMI birgt zudem das Risiko, dass mehr Daten gemeinsam und in größerem Umfang genutzt werden können, als dies für den Zweck einer effizienten Zusammenarbeit unbedingt erforderlich ist. Die Speicherdauer in diesem System ist genau festzulegen. Fraglich ist, ob die in der EU-DLRL vorgesehene Aufbewahrungsfrist von sechs Monaten nach Abschluss des Informationsaustausches tatsächlich erforderlich ist. Es muss gewährleistet werden, dass IMI nicht routinemäßig für Zuverlässigkeitsprüfungen bei zuwandernden Selbständigen, sondern nur dann verwendet wird, wenn dies im Einzelfall erforderlich ist.

Noch ungeklärt ist die in der EU-DLRL vorgesehene Pflicht zur Registeröffnung. Die Mitgliedstaaten müssen hiernach sicherstellen, dass die Register, in die die Dienstleistungserbringer eingetragen sind, sowohl von den zuständigen Behörden in ihrem Hoheitsgebiet als auch von den Behörden der anderen Mitgliedstaaten unter den selben Bedingungen eingesehen werden können.

Die Europäische Kommission und der europäische Datenschutzbeauftragte haben sich inzwischen in einem Schriftwechsel dahingehend verständigt, zunächst „guidelines“ zur datenschutzgerechten Anwendung von IMI für die EU-DLRL zu erarbeiten. Während einer Erprobungsphase sollen praktische Erfahrungen mit der Anwendbarkeit von IMI gesammelt und ausgewertet werden. Erst danach ist beabsichtigt, über die Notwendigkeit der Schaffung einer Rechtsgrundlage zur Einrichtung und zum Betrieb von IMI abschließend zu entscheiden.

Vor dem Hintergrund dieses getroffenen Kompromisses bin ich mir mit meinen Länderkollegen einig, dass hier Bundes- und Landesgesetzgeber gefordert sind, kurzfristig Anpassungen in den einschlägigen Fachgesetzen vorzunehmen.

3.4.2 Neuer Energieausweis führt zu Ärger bei Hauseigentümern

Seit einiger Zeit müssen Hauseigentümer einen Energieausweis erstellen lassen. An den Datenschutz haben Gesetz- und Verordnungsgeber dabei nicht gedacht – mit Folgen für die Eigentümer.

Am 1. Oktober 2007 ist die „Verordnung über energiesparenden Wärmeschutz und energieeinsparende Anlagentechnik (Energieeinsparverordnung – EnEV)“, BGBl. I 2007, S. 1519, in Kraft getreten, mit der ein Energieausweis für neue und bestehende Gebäude eingeführt wurde. Dieser ist entweder auf der Grundlage des Energiebedarfs oder auf der Grundlage des Energieverbrauchs des Gebäudes zu erstellen. Bei der Berechnung des Energiebedarfs sind bautechnische Werte und Berechnungsmethoden heranzuziehen, während zur Berechnung des Energieverbrauchs Daten des tatsächlich erfassten Energieverbrauchs der letzten drei Jahre benötigt werden. Unmittelbar nach dem Inkrafttreten der Verordnung haben sich viele Betroffene an mich gewandt und die Problematik bei der Erhebung von Verbrauchsdaten geschildert, insbesondere für den Fall, dass dem Eigentümer die Verbrauchsdaten des Mieters nicht vorliegen.

Weder die EnEV noch das ihr zugrunde liegende Energieeinspargesetz (EnEG) enthalten Regelungen für die Erhebung der Verbrauchsdaten. Auch ist keine Verpflichtung des Mieters vorgesehen, die im Rahmen seines Vertrages mit dem Energieversorgungsunternehmen entstandenen Verbrauchsdaten an den Vermieter oder den Aussteller des Energieausweises herauszugeben. Der Eigentümer darf auch nicht die Verbrauchsdaten des Mieters direkt beim Energieversorger anfordern. Nur in den Fällen, in denen der Energieversorger in der Lage ist, dem Eigentümer eine Auflistung der Gesamtverbrauchsdaten eines Mehrfamilienhauses ohne Aufschlüsselung der Daten der einzelnen Mietparteien zu übermitteln, ist ein direkter Rückschluss auf das persönliche Energieverbrauchsverhalten Einzelner nicht möglich und somit eine Datenübermittlung zulässig.

Das Fehlen gesetzlicher Vorgaben zur Verarbeitung personenbezogener Verbrauchsdaten hat zur Konsequenz, dass dieses energiepolitisch positive Vorhaben in der praktischen Umsetzung mit unvermeidbaren Problemen verbunden ist. Eine Nachregelung durch den Gesetz- bzw. Verordnungsgeber sollte deshalb erwogen werden. Der Gesetzgeber kann nicht einerseits den Eigentümer zur Erstellung eines Energieausweises verpflichten und gegen ihn bei Missachtung ein Ordnungswidrigkeitenverfahren einleiten, ihm andererseits aber keine eindeutigen rechtlichen Möglichkeiten einräumen, seiner gesetzlichen Verpflichtung nachzukommen.

3.4.3 Die neue Publizitätspflicht im elektronischen Unternehmensregister und E-Bundesanzeiger

Die neue Form der Veröffentlichung von Bilanzen im Internet erregt Unmut bei Unternehmen, ist aber datenschutzrechtlich nicht zu beanstanden. Es gibt jedoch vereinzelten Korrekturbedarf.

Mit dem Inkrafttreten des Gesetzes über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister (EHUG) am 1. Januar 2007 wurden die Publikationspflichten offenlegungspflichtiger Unternehmen aufgrund von EU-Richtlinien (Richtlinien 2003/58/EG und 68/151/EWG) neu geregelt. Unterlagen zum Jahres- und Konzernabschluss für die Geschäftsjahre ab 2006 müssen nicht mehr beim Handelsregister, sondern elektronisch bei der Bundesanzeiger Verlagsge-

sellschaft mbH als Betreiberin des elektronischen Bundesanzeigers eingereicht werden. Der Kreis der offenlegungspflichtigen Unternehmen sowie Art und Umfang der einzureichenden Unterlagen sind hingegen unverändert geblieben.

Hierzu haben mich viele Eingaben von Unternehmern erreicht, die mit der Veröffentlichung ihrer Unternehmensdaten über die Internet-Plattformen www.unternehmensregister.de und www.ebundesanzeiger.de nicht einverstanden waren. Der freie Zugang für jedermann ist jedoch datenschutzrechtlich nicht zu beanstanden. Die Angaben über juristische Personen und Personenmehrheiten hat der Gesetzgeber aus dem Anwendungsbereich des BDSG bewusst ausgenommen. Während für den Einzelnen die informationelle Selbstbestimmung den Ausgangspunkt bildet, unterliegen juristische Personen insbesondere aus Gründen des Verbraucher-, Anleger- und Gläubigerschutzes vielfältigen Pflichten zur Publizität und Rechnungslegung. Datenschutzregeln sind auf derartige Regeln – zumindest nach deutschem Recht – nicht anwendbar.

Durch einige Eingaben bin ich darauf hingewiesen worden, dass bei der Suche z. B. nach einem Namen eines Wirtschaftprüfers oder Steuerberaters nicht nur die von ihm zu publizierenden Unternehmensdaten, sondern auch die aller Unternehmen als Suchergebnis angezeigt wurden, bei denen er in seiner Funktion als Wirtschaftsprüfer oder Steuerberater mitgewirkt hat. Das Bundesministerium der Justiz hat inzwischen die Bundesanzeiger Verlagsgesellschaft mbH angewiesen, diese Volltextsuche in den Jahresabschlüssen so abzuschalten, dass lediglich noch nach den Firmenbezeichnungen der veröffentlichenden Unternehmen bzw. nach Teilen hiervon recherchiert werden kann. Seit August 2008 ist der Suchmodus beider Plattformen entsprechend angepasst worden.

3.4.4 Der Mensch ist kein Score-Wert

Bereits in meinen zurückliegenden Tätigkeitsberichten habe ich auf die Gefahren der Profilbildung hingewiesen und ein gesetzgeberisches Handeln angemahnt (vgl. 20. TB Nr. 11.4 ff.; 21. TB Nr. 9.1). Den nun im Berichtszeitraum vorgelegten Gesetzentwurf (Bundestagsdrucksache 16/10529), der die Tätigkeit von Auskunfteien regeln und Score-Verfahren transparenter machen will, begrüße ich. Ich wünsche mir jedoch ein klareres Bekenntnis zum Schutz des Einzelnen vor einer ausufernden Profilbildung.

Der Entwurf der Bundesregierung sieht eine ausdrückliche Rechtsgrundlage für die Einmeldung von personenbezogenen Daten in ein Auskunfteisystem vor. Dabei handelt es sich um Daten über nicht-vertragsgemäßes Verhalten. Hiervon gibt es zwei wichtige Ausnahmen: Kreditinstitute dürfen auch Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung eines Vertragsverhältnisses an eine Auskunftei weitergeben. Zudem bleibt es einem Unternehmen unbenommen, im Wege einer Einwilligung vom Betroffenen die Erlaubnis zu erhalten, weitere Daten an eine Auskunftei zu übermitteln. Der Gesetzentwurf regelt zudem die Durchführung von Scoring-Verfahren und verschärft das Auskunftsrecht der Betroffenen: So müssen alle Auskunfteien zukünftig einmal jährlich kostenlos Auskunft zu den bei ihnen gespeicherten Daten und Score-Werten geben.

Doch dies ist noch nicht ausreichend. Der Entwurf hat drei entscheidende Schwachstellen, die sich in der Praxis zum Nachteil des Einzelnen, aber auch der zuständigen Datenschutzaufsichtsbehörde auswirken werden:

Es fehlt eine wirksame Beschränkung des Auskunfteienmarktes. Derzeit erlaubt das Gesetz eine Abfrage bei einer Auskunftei, wenn das abfragende Unternehmen ein berechtigtes Interesse geltend machen kann. Dieses wird allzu oft in der Praxis im Sinne eines wirtschaftlichen Risikos ausgelegt. Dadurch wird das Risiko der Nicht-Leistung einseitig auf die schwächere Vertragspartei abgewälzt. So könnten in Zukunft auch Arbeitgeber vor einer Einstellung die Bonität ihrer Arbeitnehmerinnen und Arbeitnehmer überprüfen. Die Schwierigkeit liegt in der Praxis gerade darin, die aus allgemeinen wirtschaftlichen Erwägungen heraus begründeten Anfragen auf diejenigen zu reduzieren, bei denen tatsächlich ein besonderes, weil kreditorisches Risiko im Hintergrund steht. Hier fehlt eine klare Beschränkung des Auskunfteienmarktes. Deswegen sollte im Gesetz ein unmittelbares finanzielles Ausfallrisiko als Voraussetzung für eine Bonitätsauskunft festgeschrieben werden.

Außerdem gehen die Auskunftsrechte an einer entscheidenden Stelle noch nicht weit genug. Zwar soll der Score-Wert zukünftig einzelfallbezogen und nachvollziehbar erläutert werden, doch bei dieser sehr flexiblen und auslegbaren Bestimmung besteht die Gefahr, dass der Betroffene nur mit einer allgemeinen Erklärung abgespeist wird. Bereits heute erfährt der Betroffene bei einigen Auskunfteien auf Nachfrage, wie ein Score-Wert generell zustande kommt. Für den Betroffenen kommt es aber darauf an zu erfahren, welche Bedeutung eine bestimmte Information für die Kreditentscheidung hat. Zum Schutz der Betriebs- und Geschäftsgeheimnisse würde es genügen, die genutzten Datenarten in absteigender Reihenfolge ihrer Bedeutung für das im Einzelfall berechnete Ergebnis zu beauskunften. Dies böte die Möglichkeit sowohl den Interessen der Wirtschaft nach einem Schutz der Score-Formel als auch den Transparenzanforderungen der Bürgerinnen und Bürger gerecht zu werden.

Schließlich ist eine Beurteilung der Kreditwürdigkeit anhand der Wohnanschrift („Geo-Scoring“) diskriminierend und unseriös, da sie die Bewertung der Kreditwürdigkeit an ein Merkmal anknüpft, das der Einzelne nicht beeinflussen kann (s. u. Nr. 7.1). Genau dies soll nach dem Gesetzentwurf aber möglich bleiben: Es ist gesellschaftlich nicht hinnehmbar, dass man generell mehr für einen Kredit bezahlt, wenn man in einer schlecht beleumundeten Gegend wohnt. Daher sollte die Verwendung von Anschriftendaten zur Bonitätsbewertung nicht zugelassen werden.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Nachbesserungen angemahnt. Ich habe die Hoffnung, dass am Ende der zu Redaktionsschluss noch andauernden Beratungen im Deutschen

Bundestag die Rechte der Betroffenen weiter gestärkt sein werden.

3.4.5 Informationelle Selbstbestimmung ernst nehmen – Neue Anforderungen an Werbewirtschaft und Adresshandel

Die Bundesregierung hat am 10. Dezember 2008 eine weitere Novelle des Bundesdatenschutzgesetzes im Adresshandel beschlossen, die den illegalen Datenhandel eindämmen soll (vgl. Nr. 2.3). Die bereits im Vorfeld des Kabinettsbeschlusses heftig geführte Debatte, insbesondere befeuert durch die Werbewirtschaft, dürfte sich in den nun anstehenden Beratungen in Bundesrat und Bundestag noch intensivieren.

Besonders umstritten ist dabei der Vorschlag, das sog. Listenprivileg für bestimmte Datenverarbeitungen für Werbezwecke abzuschaffen. Nach § 28 Absatz 3 Nummer 3 BDSG dürfen bestimmte personenbezogene Daten für Zwecke der Werbung genutzt und übermittelt werden, solange die Betroffenen nicht widersprechen. Dieses Listenprivileg ist mit erheblichen Gefahren für die Betroffenen verbunden, denn die auf diesem Weg privilegierten personenbezogenen Daten lassen sich nicht ohne weiteres von weiteren Datensammlungen isolieren. Mit ihrer Übermittlung können daher Zusatzinformationen verbunden sein, die weit über das vom Gesetzgeber akzeptierte Informationsspektrum hinausreichen. Insbesondere lässt sich der Informationsgehalt mit Hilfe der Angabe steuern und variieren, die es ermöglicht, die Zugehörigkeit zu einer bestimmten, den Übermittlungsadressaten interessierenden Personengruppe zu konkretisieren. Vor diesem Hintergrund halte ich allein die konsequente Abschaffung des Listenprivilegs und die Einführung der Einwilligungslösung für folgerichtig. Damit wäre Werbung gegenüber Privatpersonen grundsätzlich nur mit Einwilligung möglich.

Flankiert werden soll die Abschaffung des Listenprivilegs von im wesentlichen fünf weiteren Maßnahmen:

- Stärkung des betrieblichen Datenschutzbeauftragten
- Einführung eines Koppelungsverbots, d. h. der Abschluss eines Vertrages darf nicht davon abhängig gemacht werden, dass die Betroffenen in die Weitergabe ihrer persönlichen Daten an Dritte zu Werbezwecken einwilligen, es sei denn, die Datenweitergabe ist gerade Gegenstand des Vertrages
- Erweiterung des Bußgeldkatalogs, da die Ordnungswidrigkeitentatbestände des § 43 BDSG nicht unerhebliche Lücken aufweisen, so dass eine Reihe von Datenschutzverstößen gar nicht sanktioniert werden können
- Schaffung einer Möglichkeit zur Abschöpfung unrechtmäßiger Gewinne aus illegaler Datenverwendung
- Einführung einer Informationspflicht bei Datenschutzverstößen in der Privatwirtschaft

Diese Maßnahmen sind notwendig, aber noch nicht hinreichend. Personenbezogene Daten haben für die Wirtschaft einen hohen Wert. Um diesen hohen Wert zu schützen, müssen die Aufsichtsbehörden angemessen ausgestattet sein. Ich meine hiermit nicht nur eine angemessene personelle und finanzielle Ausstattung, auch das Instrumentarium der Aufsichtsbehörden muss erweitert werden. Gefahrenabwehr können Datenschutzbehörden bislang nur bei festgestellten technischen und organisatorischen Mängeln nach § 9 BDSG, nicht aber bei den oftmals erheblich schwerwiegenderen materiell rechtlichen Datenschutzverstößen treffen. Erforderlich ist daher, § 38 Absatz 5 BDSG um die Möglichkeit zu erweitern, Anordnungen und Untersagungen auch in Bezug auf materiell rechtswidrige Datenverarbeitungen treffen zu können.

Notwendig ist zudem die Einführung einer Kennzeichnungspflicht für personenbezogene Daten (s. dazu Nr. 8.5). Die Verpflichtung der Stelle, die die personenbezogenen Daten ursprünglich erhoben hat, bei Weitergabe des Datenbestandes zu Werbezwecken diesen mit einer Herkunftsbezeichnung zu versehen, die jederzeit auch bei mehrfacher Weitergabe und Vermischung mit anderen Datenbeständen die Quelle identifizierbar macht, würde es den Betroffenen sehr erleichtern, ihre Datenschutzrechte wahrzunehmen.

Nach wie vor bedarf das Datenschutzrecht – gerade wenn es um den Schutz des Einzelnen gegenüber Datensammlungen in der Privatwirtschaft geht – einer grundlegenden Überarbeitung.

3.4.6 Datenschutz bei Rechtsanwälten weiterhin nicht gesichert

Der Streit, ob auch Rechtsanwaltskanzleien dem Bundesdatenschutzgesetz und seinen Kontrollmechanismen unterliegen, konnte noch immer nicht gelöst werden.

Nach wie vor bestreiten die Rechtsanwaltskammern die Anwendbarkeit des BDSG auf die von Rechtsanwälten verarbeiteten mandatsbezogenen Daten. Anwaltskanzleien verweigern in vielen Fällen die Zusammenarbeit mit den zuständigen Datenschutzaufsichtsbehörden. Hierüber habe ich bereits in meinem letzten Tätigkeitsbericht (21. TB Nr. 9.7) ausführlich berichtet. Eine Lösung in dieser wichtigen Frage steht leider immer noch aus.

Kasten zu Nr. 3.4.6

Aus der Stellungnahme der Bundesregierung zum 21. TB zu Nr. 9.7:

„Die Bundesregierung teilt die Rechtsauffassung des BfDI, dass die Erhebung und Verwendung personenbezogener – auch mandatsbezogener – Daten durch Rechtsanwälte den Vorschriften des BDSG unterliegt und dass die Datenschutzaufsichtsbehörden der Länder zuständig sind, die Datenschutzkontrolle durchzuführen. …“

Zwar hat sich die Bundesregierung in ihrer Stellungnahme zum 21. TB meiner Rechtsauffassung angeschlos-

sen (s. Kasten zu Nr. 3.4.6). Es ist aber noch nicht gelungen, eine gesetzliche Klarstellung zu erreichen, so dass das Grundrecht der betroffenen Bürgerinnen und Bürger auf informationelle Selbstbestimmung bei Datenverarbeitung durch Rechtsanwälte vielfach gar nicht oder nur sehr eingeschränkt geltend gemacht werden kann. Dies gilt nicht nur für die gesetzlichen Ansprüche auf Auskunft, Benachrichtigung, Sperrung und Löschung von personenbezogenen Daten, sondern auch für die Möglichkeit, den Umgang mit personenbezogenen Daten in Rechtsanwaltskanzleien durch die unabhängige Datenschutzaufsicht überprüfen zu lassen.

Die Rechtsanwaltskammern vertreten die Meinung, dass die Aufsicht in Bezug auf die mandatsbezogene Informationsverarbeitung bei Rechtsanwälten ausschließlich bei ihnen liege. Unabhängig davon, dass weder das BDSG noch die Europäische Datenschutzrichtlinie eine entsprechende Einschränkung der allgemeinen Regelungen enthalten, wäre ein solches Verfahren auch mit Artikel 28 Absatz 1 der Richtlinie unvereinbar, da die datenschutzrechtlichen Kontrollstellen ihre Aufgabe in völliger Unabhängigkeit wahrnehmen müssen. Diese Unabhängigkeit ist bei den Rechtsanwaltskammern als Selbstverwaltungsorganisation schon insoweit nicht gegeben, als die Verantwortlichen von den Mitgliedern gewählt werden, die zu Kontrollierenden also ihre Kontrolleure aussuchen und gegebenenfalls auch durch Abwahl sanktionieren können.

Ein weiteres Argument der Rechtsanwaltskammern hat größeres Gewicht: Es besteht die Sorge, die Aufsichtsbehörden könnten verpflichtet sein, bei ihren Kontrollen gewonnene Informationen, etwa über strafbare Handlungen eines Mandanten, an andere staatliche Stellen weiterzugeben. Insofern bestehe auch kein Zeugnisverweigerungsrecht und Beschlagnahmeverbot für die Aufsichtsbehörden. Auch wenn mir in der Praxis noch kein Fall bekannt geworden ist, in dem sich dieses Problem konkret gestellt hätte, kann dieses Argument rein rechtlich betrachtet nicht völlig von der Hand gewiesen werden. Die Konsequenz kann allerdings nur sein, für die Datenschutzaufsichtsbehörden entsprechende Schutzvorschriften zu schaffen, durch die die Weitergabe entsprechender Erkenntnisse ausgeschlossen wird. Eine vergleichbare Problematik bestand auch hinsichtlich der Beschäftigung externer Datenschutzbeauftragter durch Berufsgeheimnisträger. Hier hat der Gesetzgeber im Ersten Mittelstandsentlastungsgesetz vom 22. August 2006 (BGBl. I 2006 S. 2970) u. a. in § 4f BDSG einen neuen Absatz 4a zum Zeugnisverweigerungsrecht und Beschlagnahmeschutz und in § 203 StGB einen neuen Absatz 2a zur Strafbarkeit unbefugten Offenbarens durch Datenschutzbeauftragte eingefügt. Ich hoffe, dass durch eine entsprechende Stärkung der Rechtstellung der Datenschutzaufsichtsbehörden auch hier eine für alle Seiten zufrieden stellende Lösung gefunden werden kann.

Die in der Gegenäußerung der Bundesregierung zu meinem 21. TB angekündigte Prüfung durch BMI und BMJ hat offensichtlich auch nach zwei Jahren noch zu keinem konkreten Ergebnis geführt. Dies bedauere ich um so mehr, als der Streit für die Bürgerinnen und Bürger ganz konkrete Konsequenzen hat. So habe ich bereits in meinem letzten TB über den Fall einer Rechtsanwaltskanzlei berichtet, die in großem Stil von der Deutschen Telekom AG für das Beitreiben ihrer Forderungen eingesetzt wird und jede Zusammenarbeit mit der zuständigen Datenschutzaufsichtsbehörde verweigert, obwohl es immer wieder Beschwerden wegen nicht ordnungsgemäßer Datenverarbeitung gibt. Auch hier ist es trotz einer Vielzahl von Gesprächen, die u. a. von mir als zuständiger Aufsichtsbehörde für die Deutsche Telekom AG mit dieser geführt wurden, noch zu keinem befriedigenden Ergebnis gekommen. Nach meiner Überzeugung kann es im Schutzbereich des BDSG und der Europäischen Datenschutzrichtlinie keine datenschutz- und kontrollfreien Räume geben. Es stellt sich deswegen die Frage, ob ein Unternehmen wie die Deutsche Telekom AG im großen Umfang personenbezogene Daten an einen Dritten übermitteln darf, wenn es nicht gewährleisten kann, dass die Betroffenen dort den gleichen Datenschutz genießen, der für das Unternehmen selber gilt.

3.4.7 Dringend notwendige Verbesserungen beim Datenschutz in der Versicherungswirtschaft lassen weiter auf sich warten

Die Verhandlungen zwischen Datenschutzaufsichtsbehörden und Versicherungswirtschaft über eine datenschutzgerechte Ausgestaltung der Datenverarbeitung bei den Versicherungsunternehmen sind nur mühsam vorangekommen, befinden sich aber nun auf einem Erfolg versprechenden Weg. Ein Durchbruch konnte indes noch nicht erzielt werden.

Die Beratungen der AG Versicherungswirtschaft des Düsseldorfer Kreises, einem Koordinierungsgremium der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, mit dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) wurden fortgesetzt. Gegenstand waren datenschutzrechtliche Fragen bei der Verarbeitung personenbezogener Daten für Zwecke der Antrags-, Vertrags- und Leistungsabwicklung durch die Versicherungsunternehmen. Im Vordergrund standen der Entwurf für eine neue einheitliche Einwilligungs- und Schweigepflichtentbindungserklärung, die Umgestaltung des früher unter dem Namen „Uniwagnis“ bekannten Hinweis- und Informationssystems (HIS) und der Entwurf des GDV für Verhaltensregeln für den Umgang mit personenbezogenen Daten im Sinne von § 38a BDSG.

Über Struktur, Erscheinungsbild und Inhalt der Einwilligungs- und Schweigepflichtentbindungserklärung sowie des dazu gehörenden Merkblatts zur Datenverarbeitung besteht zwischen der Versicherungswirtschaft und den Datenschutzaufsichtsbehörden seit langem Dissens. Hierüber habe ich bereits im 20. TB (Nr. 17.1.9) und 21. TB (Nr. 9.6) berichtet. Die Datenschutzaufsichtsbehörden fordern seit geraumer Zeit eine Änderung und Überarbeitung der Einwilligungserklärung, weil die bisher verwendete Klausel nicht transparent genug ist und nicht den Vorschriften des § 4a BDSG entspricht. Insbesondere unterscheiden sich die Auffassungen zu der Frage, welche

Datenverarbeitungen bereits nach den gesetzlichen Vorschriften zulässig sind und welche einer Einwilligung bedürfen. Ziel sollte es sein, die Einwilligungsklausel auf die Sachverhalte zu beschränken, bei denen keine gesetzlichen Erlaubnistatbestände vorhanden sind (z. B. im Fall der Nutzung und Übermittlung für Werbezwecke).

Die Entscheidung des Bundesverfassungsgerichts vom 23. Oktober 2006 zur Unzulässigkeit formularmäßiger Einwilligungserklärungen in Versicherungsverträgen (1 BvR 2027/02, vgl. 21. TB Nr. 9.6) sowie das Inkrafttreten von § 213 Versicherungsvertragsgesetz (VVG), in der die Erhebung von Gesundheitsdaten durch Versicherungsunternehmen geregelt wird, brachten endlich Bewegung in die Diskussion und unterstützten die Datenschutzaufsichtsbehörden bei ihren Forderungen. Die im Berichtszeitraum geführten Verhandlungen mit dem GDV gestalteten sich dennoch schwierig und gingen nur mühsam voran. Grund hierfür waren auch die parallel dazu laufenden Gespräche über die Verhaltensregeln der Versicherungswirtschaft (s. u.) sowie die in unmittelbarem Zusammenhang mit dem Umfang und Inhalt der Einwilligungsklausel stehende Frage der Umgestaltung des Hinweis- und Informationssystems (HIS). Bei Redaktionsschluss zeichnete sich jedoch ein erfolgreicher Abschluss der Verhandlungen ab, so dass in Versicherungsverträgen demnächst die neue datenschutzgerechte Einwilligungs- und Schweigepflichtentbindungserklärung nebst Merkblatt verwendet werden kann.

Über datenschutzrechtliche Bedenken gegen das Hinweis- und Informationssystem (HIS) der Versicherungswirtschaft, das der Risikoprüfung und Aufdeckung bzw. Prävention von Versicherungsbetrug dient, habe ich im letzten TB (Nr. 9.5) berichtet. Eine Bestandsaufnahme des Düsseldorfer Kreises hat diese Bedenken bestätigt und die Datenschutzaufsichtsbehörden darin bestärkt, eine datenschutzkonforme Umgestaltung des Systems zu fordern. Nachdem der GDV Anfang 2007 erfreulicherweise seine Bereitschaft zu einer Neukonzeption erklärt hatte, haben ihm die Datenschutzaufsichtsbehörden mitgeteilt, dass sie die weitere Nutzung des bisherigen HIS für einen Übergangszeitraum bis Ende 2008 tolerieren würden. Um zumindest vorläufig mehr Transparenz über das bisherige Verfahren zu schaffen, haben der GDV und die AG Versicherungswirtschaft eine gemeinsame Verfahrensbeschreibung erstellt und im Internet unter www.gdv.de oder www.datenschutzzentrum.de veröffentlicht.

Im November 2007 stellte der GDV seine Pläne zur Neustrukturierung des Hinweis- und Informationssystems vor, die als Grundkonzept eine Weiterführung als Auskunftei nach § 29 BDSG vorsehen. Seitens der AG Versicherungswirtschaft wurde signalisiert, dass dieses Grundkonzept akzeptabel sei, jedoch noch zahlreiche Detailfragen geklärt werden müssten. Im September 2008 wies der GDV erstmals darauf hin, dass eine Inbetriebnahme des neuen HIS Anfang 2009 unrealistisch sei. Im November 2008, also knapp zwei Jahre nach dem Hinweis der Datenschutzaufsichtsbehörden auf die Rechtswidrigkeit des bisherigen HIS, wurde schließlich mitgeteilt, die Umsetzung des neuen Konzepts könne nicht vor April 2011 abgeschlossen werden.

Es ist sehr zu bedauern, dass sich der GDV nun außer Stande sieht, die von den Datenschutzaufsichtsbehörden festgelegte Frist für die Aufnahme des dem Grunde nach begrüßenswerten neuen HIS einzuhalten. Mit einer weiteren Nutzung des bisherigen Systems wird ein datenschutzwidriger Zustand fortgeführt. Die Bereitschaft des GDV zu datenschutzrechtlichen Verbesserungen in Bezug auf die Benachrichtigung der Betroffenen bei Einmeldung in das System und auf eine Auskunftserteilung nach § 34 BDSG ändert nichts an der grundsätzlichen Rechtswidrigkeit des derzeitigen Systems. Die AG Versicherungswirtschaft hat den GDV im Dezember 2008 nochmals ausdrücklich auf den anhaltenden rechtswidrigen Zustand hingewiesen, der sowohl die einzelnen Versicherungsunternehmen als auch die zuständigen Aufsichtsbehörden im Falle der Weiternutzung des bisherigen HIS vor große Probleme stellt. Wie die Aufsichtsbehörden im einzelnen auf eine weitere Nutzung reagieren, war bei Redaktionsschluss noch nicht absehbar. Einzelne Aufsichtsbehörden haben Versicherungsunternehmen aber bereits darauf hingewiesen, dass sie einen fortgesetzten rechtswidrigen Datenaustausch über HIS mit Sanktionen belegen würden.

Positiv bewerte ich die Absicht des GDV, einen so genannten Code of Conduct für alle angeschlossenen Versicherungsunternehmen zu erstellen. Hierbei handelt es sich um Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen im Sinne von § 38a BDSG. Eine solche Verhaltensrichtlinie schafft weitestgehend einheitliche Standards für die Verarbeitung personenbezogener Daten beim Abschluss und bei der Abwicklung von Versicherungsverträgen und fördert die Einhaltung der zu beachtenden Datenschutzbestimmungen. Sie wirkt zwar in erster Linie nach innen und richtet sich an die Versicherungsunternehmen selbst. Sie ist aber auch geeignet, dem Versicherungsnehmer einen Eindruck zu vermitteln, wie und auf welcher gesetzlichen Grundlage mit seinen persönlichen Daten verfahren wird. Die Verhaltensregeln können zwar eine umfassende Unterrichtung des Betroffenen nach § 4 Absatz 3 BDSG über die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Kategorien von Empfängern nicht ersetzen, bieten jedoch eine gute Möglichkeit, zusätzlich zur neuen Einwilligungsklausel und zum Merkblatt die erforderliche Transparenz der Datenverarbeitung zu erhöhen.

Der GDV hat der AG Versicherungswirtschaft Ende 2007 den Entwurf für den Code of Conduct zur Abstimmung vorgestellt. Wegen des engen Zusammenhangs wurden gemeinsame Gespräche hierüber zeitgleich mit den Beratungen über den Inhalt der neuen Einwilligungs- und Schweigepflichtentbindungserklärung geführt. Eine Endfassung der Verhaltensregeln lag bei Redaktionsschluss noch nicht vor.

Freiheit und Sicherheit

In den folgenden beiden Kapiteln berichte ich über Themen aus den Bereichen „Innere Sicherheit“ und „Recht und Verwaltung“. Schwerpunkte waren hier die Erweiterung der Befugnisse der Sicherheitsbehörden und insbesondere der heimliche Zugriff auf ein informationstechnisches System durch eine Sicherheitsbehörde (Nr. 4.1 ff.), die Neuregelung der Telekommunikationsüberwachung nach §§ 100a ff. StPO (Nr. 5.1), die geplante Einführung eines Zentralregisters im Bundesmeldegesetz (Nr. 5.2) und die Vorbereitungen für die Volkszählung im Jahr 2011 (Nr. 5.5).

4 Innere Sicherheit

4.1 Online-Durchsuchungen durch Sicherheitsbehörden

Online-Durchsuchungen sind schwerwiegende Grundrechtseingriffe und nur zur Abwehr existenzieller Bedrohungen zulässig.

Seit der Einführung der akustischen Wohnraumüberwachung 1998 (vgl. hierzu 20. TB Nr. 7.1) wurde keine einzelne Überwachungsmaßnahme so intensiv und kontrovers diskutiert wie der heimliche, d. h. vom Betroffenen unbemerkte, Zugriff auf ein informationstechnisches System (Personalcomputer, Mobiltelefon etc.) durch eine Sicherheitsbehörde, die sog. „Online-Durchsuchung“. Es handelt sich dabei regelmäßig um einen schwerwiegenden Grundrechtseingriff, wie das Bundesverfassungsgericht in seiner Entscheidung vom 27. Februar 2008 (1 BvR 370/07) festgestellt hat (s. o. Nr. 2.1). Der Begriff „Online-Durchsuchung“ umfasst nicht nur den einmaligen Zugriff auf ein System, um dort vorhandene Daten anzuschauen, zu kopieren oder auszuleiten. Er ermöglicht auch eine längerfristige Überwachung und damit die Erfassung aller während des Überwachungszeitraums erzeugten Daten (s. Kasten zu Nr. 4.1).

Kasten zu Nr. 4.1

Technische Voraussetzung für eine **Online-Durchsuchung** ist das Aufspielen einer entsprechenden Software in das zu überwachende System. Dies kann entweder über einen Datenträger (Diskette, CD-ROM, USB-Stick etc.) oder online, d. h. über eine bestehende Internet-Verbindung, z. B. als Anhang an eine E-Mail, geschehen. Der Betroffene merkt nichts hiervon. Er kann sich auch durch sog. Firewalls oder Virenschutzsoftware nicht hiergegen schützen.

Mit einer Online-Durchsuchung hat eine Sicherheitsbehörde Zugriff auf sämtliche in dem infiltrierten System vorhandene – auch höchst persönliche – Daten. Angesichts des gewandelten gesellschaftlichen Kommunikations- und Nutzungsverhaltens besteht damit regelmäßig nicht nur Zugriff auf gespeicherte E-Mail, sondern auch auf Gesundheits-, Bank-, Finanz-, Steuer- und privateste Daten. Hierzu zählen beispielsweise auch Tagebücher, die zunehmend nicht mehr in Papierform, sondern elektronisch geführt werden. Aus der Zusammenschau dieser Daten entstehen weit reichende Persönlichkeitsprofile der Betroffenen.

Die für eine Online-Durchsuchung eingesetzte Software kann technisch bedingt auch höchst persönliche Daten erfassen, die zum Kernbereich der privaten Lebensgestaltung gehören. In diesen Kernbereich, der durch die in Artikel 1 des Grundgesetzes geschützte Menschenwürde garantiert wird, darf der Staat nicht eingreifen. Dies hat das BVerfG in mehreren Entscheidungen nachdrücklich betont.

Sollen mit der eingeschleusten Software ausschließlich Daten aus einem laufenden Kommunikationsvorgang (E-Mail-Verkehr, Internet-Telefonie) erfasst und ausgeleitet werden, spricht man von einer „Quellen-Telekommunikationsüberwachung“. Sie betrifft in erster Linie das durch Artikel 10 Grundgesetz geschützte Fernmeldegeheimnis. Ich halte es für zweifelhaft, ob technisch sichergestellt werden kann, dass bei einer Quellen-Telekommunikationsüberwachung ausschließlich die laufende Telekommunikation überwacht und aufgezeichnet wird und es zu keiner Erhebung weiterer personenbezogener Daten, z. B. auf der Festplatte des betreffenden Rechners, kommt (s. u. Nr. 4.1.1; 8).

Das BVerfG hat in seinem Urteil zur Online-Durchsuchung den heimlichen Zugriff auf informationstechnische Systeme nur unter sehr engen Voraussetzungen für zulässig erklärt (s. u. Nr. 4.1.1; 8). So müssen bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Hierzu zählen Leib, Leben und Freiheit einer Person sowie die Güter der Allgemeinheit, welche die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen betreffen. Erforderlich ist mithin eine existenzielle Bedrohungslage. Nur dann kann diese Maßnahme gerechtfertigt sein. Der Gesetzgeber muss zudem den Grundrechtsschutz der Betroffenen durch geeignete Verfahrensvorkehrungen sicherstellen.

4.1.1 Verfassungsbeschwerde erfolgreich

Online-Durchsuchungsbefugnis im Landesverfassungsschutzgesetz Nordrhein-Westfalen ist verfassungswidrig.

In seinem Urteil zur Online-Durchsuchung vom 27. Februar 2008 hat das Bundesverfassungsgericht die im Verfassungsschutzgesetz des Landes Nordrhein-Westfalen neu aufgenommene Befugnis zur Durchführung von Online-Durchsuchungen für verfassungswidrig erklärt. Mit diesem Gesetz hatte der Gesetzgeber zum ersten Mal einer Sicherheitsbehörde diese Befugnis gewährt.

Angesichts des schwerwiegenden Grundrechtseingriffs ist diese Maßnahme nur unter sehr engen Voraussetzungen zur Abwehr existenzieller Bedrohungen zulässig (s. o. Nr. 4.1). In meiner Stellungnahme gegenüber dem BVerfG habe ich nicht nur auf die gravierenden verfassungsrechtlichen Mängel dieser gesetzlichen Befugnis, sondern auch auf meine generellen verfassungsrechtlichen Bedenken und die praktischen Probleme hingewiesen, die unvermeidbar mit der Durchführung von Online-Durchsuchungen verbunden sind. Ich begrüße es deshalb, dass das Gericht diese Bedenken aufgenommen und die Online-Durchsuchung nur in eng begrenzten Fällen und unter hohen Hürden für zulässig erklärt hat.

Kasten zu Nr. 4.1.1

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008

Vorgaben des Bundesverfassungsgerichts bei der Online-Durchsuchung beachten

1. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass das Bundesverfassungsgericht die Regelung zur Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen für nichtig erklärt hat. Hervorzuheben ist die Feststellung des Gerichts, dass das allgemeine Persönlichkeitsrecht auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst. 25 Jahre nach dem Volkszählungsurteil hat das Bundesverfassungsgericht damit den Datenschutz verfassungsrechtlich weiter gestärkt und ihn an die Herausforderungen des elektronischen Zeitalters angepasst.

2. Ein solches Grundrecht nimmt auch den Staat in die Verantwortung, sich aktiv für die Vertraulichkeit und Integrität informationstechnischer Systeme einzusetzen. Das Bundesverfassungsgericht verpflichtet den Staat, im Zeitalter der elektronischen Kommunikation Vertraulichkeit zu gewährleisten. Nunmehr ist der Gesetzgeber gehalten, diesen Auftrag konsequent umzusetzen. Dazu müssen die Regelungen, welche die Bürgerinnen und Bürger vor einer „elektronischen Ausforschung“ schützen sollen, gemäß den Vorgaben des Gerichts insbesondere im Hinblick auf technische Entwicklungen verbessert werden. Hiermit würde auch ein wesentlicher Beitrag geleistet, Vertrauen in die Sicherheit von E-Government- und E-Commerce-Verfahren herzustellen.

3. Die Konferenz unterstützt die Aussagen des Gerichts zum technischen Selbstschutz der Betroffenen. Ihre Möglichkeiten, sich gegen einen unzulässigen Datenzugriff zu schützen, etwa durch den Einsatz von Verschlüsselungsprogrammen, dürfen nicht unterlaufen oder eingeschränkt werden.

4. Die Konferenz begrüßt außerdem, dass das Bundesverfassungsgericht das neue Datenschutzgrundrecht mit besonders hohen verfassungsrechtlichen Hürden vor staatlichen Eingriffen schützt. Sie fordert die Gesetzgeber in Bund und Ländern auf, diese Eingriffsvoraussetzungen zu respektieren. Die Konferenz spricht sich in diesem Zusammenhang gegen Online-Durchsuchungen durch die Nachrichtendienste aus.

5. Das Bundesverfassungsgericht hat den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung auch bei Eingriffen in informationstechnische Systeme zu gewährleisten. Unvermeidbar erhobene kernbereichsrelevante Inhalte sind unverzüglich zu löschen. Eine Weitergabe oder Verwertung dieser Inhalte ist auszuschließen.

6. Auch wenn Online-Durchsuchungen innerhalb der durch das Bundesverfassungsgericht festgelegten Grenzen verfassungsgemäß sind, fordert die Konferenz die Gesetzgeber auf, die Erforderlichkeit von Online-Durchsuchungsbefugnissen kritisch zu hinterfragen. Sie müssen sich die Frage stellen, ob sie den Sicherheitsbehörden entsprechende Möglichkeiten an die Hand geben wollen. Die Konferenz bezweifelt, dass dieser weiteren Einbuße an Freiheit ein adäquater Gewinn an Sicherheit gegenüber steht.

7. Sollten gleichwohl Online-Durchsuchungen gesetzlich zugelassen werden, sind nicht nur die vom Bundesverfassungsgericht aufgestellten verfassungsrechtlichen Hürden zu beachten. Die Konferenz hält für diesen Fall zusätzliche gesetzliche Regelungen für erforderlich. Zu ihnen gehören vor allem folgende Punkte:

   – Soweit mit der Vorbereitung und Durchführung von Online-Durchsuchungen der Schutzbereich von Artikel 13 GG (Unverletzlichkeit der Wohnung) betroffen ist, bedarf es dafür jedenfalls einer besonderen Rechtsgrundlage.

   – Der vom Bundesverfassungsgericht geforderte Richtervorbehalt ist bei Online-Durchsuchungen mindestens so auszugestalten wie bei der akustischen Wohnraumüberwachung. Ergänzend zu einer richterlichen Vorabkontrolle ist eine begleitende Kontrolle durch eine unabhängige Einrichtung vorzuschreiben.

   – Gesetzliche Regelungen, welche Online-Durchsuchungen zulassen, sollten befristet werden und eine wissenschaftliche Evaluation der dabei gewonnenen Erkenntnisse und Erfahrungen anordnen.

   – Informationstechnische Systeme, die von zeugnisverweigerungsberechtigten Berufsgruppen genutzt werden, sind von heimlichen Online-Durchsuchungen auszunehmen.

   – Für die Durchführung von „Quellen-Telekommunikationsüberwachungen“, die mit der Infiltration von IT-Systemen einhergehen, sind die gleichen Schutzvorkehrungen zu treffen wie für die Online-Durchsuchung selbst.

8. Schließlich sind die Gesetzgeber in Bund und Ländern aufgrund der Ausstrahlungswirkung der Entscheidung des Bundesverfassungsgerichts gehalten, die sicherheitsbehördlichen Eingriffsbefugnisse in Bezug auf informationstechnische Systeme, z. B. bei der Überwachung der Telekommunikation im Internet sowie der Beschlagnahme und Durchsuchung von Speichermedien, grundrechtskonform einzuschränken.

Von besonderer Bedeutung für das BVerfG war auch die Frage der Abgrenzbarkeit der Online-Durchsuchung von einer Quellen-Telekommunikationsüberwachung. Das Gericht hat gefordert, dass im Falle einer Quellen-Telekommunikationsüberwachung durch technische und rechtliche Vorgaben absolut sicher gewährleistet werden muss, dass außer der laufenden Kommunikation keine sonstigen personenbezogenen Daten erfasst werden. Ob diese Vorgabe technisch umsetzbar ist, konnten die vom Gericht geladenen technischen Sachverständigen nicht zweifelsfrei beantworten.

Der Gesetzgeber ist aufgerufen, die Entscheidung des BVerfG zu beachten (vgl. Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008 in Berlin – s. Kasten zu Nr. 4.1.1) und dessen Vorgaben z. B. im Rahmen des aktuellen Entwurfs zur Novellierung des Gesetzes über das Bundeskriminalamt (s. u. Nr. 4.1.2; 4.3.1) umzusetzen. Die Anwendung der Befugnis zur Online-Durchsuchung durch die Sicherheitsbehörden ist ein wesentlicher Bestandteil meiner zukünftigen Kontrolltätigkeit. Entsprechendes gilt für die Beachtung der Vorgaben des BVerfG zum Kernbereichsschutz. Auch insoweit werde ich darauf achten, dass der absolut geschützte Kernbereich der Privatsphäre der Bürgerinnen und Bürger von den Sicherheitsbehörden strikt gewahrt wird.

4.1.2 Neue Befugnisse zur Online-Durchsuchung für das BKA

Die Diskussion über die dem BKA eingeräumte sog. Online-Durchsuchung zur Abwehr von Gefahren des internationalen Terrorismus (s. u. Nr. 4.3.1) kam erst nach Einschaltung des Vermittlungsausschusses zu einem (vorläufigen) Ergebnis. Jetzt wird sich wahrscheinlich das BVerfG damit befassen müssen.

An der Verfassungskonformität der Befugnisregelung zur Online-Durchsuchung in § 20k BKAG (Kasten zu Nr. 4.1.2) habe ich Zweifel. So verkürzt die hier vorgesehene Kernbereichsregelung die verfassungsgerichtlichen Vorgaben zum Schutz des Kernbereichs privater Lebensgestaltung in nicht akzeptabler Weise.

In seinem Urteil vom 27. Februar 2008 (s. o. Nr. 4.1.1) berücksichtigt das BVerfG den Umstand, dass die Automatisierung des Datenzugriffs im Rahmen einer Online-Durchsuchung das Erkennen kernbereichsrelevanter Daten erschwert, indem es ein zweistufiges Verfahren zum Schutz des Kernbereichs vorsieht. Anknüpfend an die bisherige Rechtsprechung zum Kernbereichsschutz gibt es dem Gesetzgeber auf, darauf hinzuwirken, dass in der ersten Stufe Maßnahmen zu treffen sind, welche die Erhebung kernbereichsrelevanter Daten soweit wie möglich verhindern. Nur in Fällen, in denen dennoch Daten mit Bezug zum Kernbereich erhoben wurden, hat der Gesetzgeber in einer zweiten Stufe durch Verfahrensvorschriften sicherzustellen, dass die Intensität der Kernbereichsverletzung so gering wie möglich bleibt.

Diesen Vorgaben entspricht es nicht, wenn nach dem Gesetz der verdeckte Eingriff in informationstechnische Systeme nur unzulässig sein soll, wenn *allein* kernbereichsrelevante Kommunikationsinhalte erfasst werden. Da diese Fälle in der Praxis kaum vorkommen werden, liefe ein derartiges Erhebungsverbot und damit der erforderliche Kernbereichsschutz ins Leere.

Zwar begrüße ich es, dass im Laufe des parlamentarischen Gesetzgebungsverfahrens Änderungen beschlossen wurden, wonach nunmehr die Anordnung der Online-Durchsuchung ausnahmslos dem Richtervorbehalt unterstellt wird und die Durchsicht der durch diese Maßnahme erlangten Daten auf kernbereichsrelevante Inhalte ebenfalls nur dem Richter obliegt. Der verfassungsrechtlich gebotene Schutz kernbereichsrelevanter Informationen auf der ersten Stufe schon bei der Datenerhebung bleibt jedoch weiterhin defizitär.

Auch wenn in dem Gesetz im Übrigen die Vorgaben des BVerfG zur Ausgestaltung der Online-Durchsuchung nominell umgesetzt zu sein scheinen, habe ich weiterhin Zweifel, inwieweit eine derartige, tief in die Privatsphäre eingreifende Befugnis im Hinblick auf den damit verfolgten Zweck vertretbar ist. Ausweislich der Begründung soll dem BKA mittels der Eingriffsbefugnisse die Möglichkeit gegeben werden, im Falle hoher terroristischer Bedrohung zeitnah entsprechende Gefahrenabwehrmaßnahmen durchführen zu können. Gegen die Eignung der Online-Durchsuchung spricht, dass sie in jedem Einzelfall die Entwicklung maßgeschneiderter Software erforderlich macht und damit technisch sehr aufwendig ist. Damit sind Zweifel angebracht, dass das BKA hiermit entsprechenden Gefahrenlagen rasch begegnen kann. Außerdem bleibt fraglich, ob die mit der Online-Durchsuchung verbundenen Risiken für die informationstechnischen Systeme, z. B. im Zusammenhang mit der Aufbringung entsprechender Software auf dem Zielsystem, wirksam zu beherrschen sind. Angesichts der nicht ausgeräumten verfassungsrechtlichen Zweifel sind von verschiedener Seite Verfassungsbeschwerden gegen das BKA-Gesetz angekündigt worden, so dass sich das BVerfG voraussichtlich erneut mit der Online-Durchsuchung beschäftigen muss.

Unabhängig davon müssen die Erfahrungen mit dieser neuen Befugnis sorgfältig beobachtet werden. Im Mittelpunkt steht dabei die Frage, ob mit dieser Maßnahme ein adäquater Gewinn an Sicherheit erzielt werden kann und ob die gesetzlich vorgegebenen Schutzvorkehrungen die erforderliche Wirkung entfalten. Ich begrüße es zwar grundsätzlich, dass die Geltung der Befugnis zur Online-Durchsuchung informationstechnischer Systeme bis 31. Dezember 2020 befristet worden ist. Eine Angleichung der Befristung an dem im Gesetz auch vorgesehenen Evaluationszyklus von fünf Jahren nach Inkrafttreten der Gesetzesnovelle wäre aber sinnvoller gewesen.

Kasten zu Nr. 4.1.2

§ 20k BKA-Gesetz

Verdeckter Eingriff in informationstechnische Systeme

(1) Das Bundeskriminalamt darf ohne Wissen des Betroffenen mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass eine Gefahr vorliegt für

1. Leib, Leben oder Freiheit einer Person oder
2. solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

Eine Maßnahme nach Satz 1 ist auch zulässig, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass ohne Durchführung der Maßnahme in näherer Zukunft ein Schaden eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für eines der in Satz 1 genannten Rechtsgüter hinweisen. Die Maßnahme darf nur durchgeführt werden, wenn sie für die Aufgabenerfüllung nach § 4a erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre.

(2) Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(3) Bei jedem Einsatz des technischen Mittels sind zu protokollieren

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,
2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit, die die Maßnahme durchführt.

Die Protokolldaten dürfen nur verwendet werden, um dem Betroffenen oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme nach Absatz 1 rechtmäßig durchgeführt worden ist. Sie sind bis zum Ablauf des auf die Speicherung folgenden Kalenderjahres aufzubewahren und sodann automatisiert zu löschen, es sei denn, dass sie für den in Satz 2 genannten Zweck noch erforderlich sind.

(4) Die Maßnahme darf sich nur gegen eine Person richten, die entsprechend § 17 oder § 18 des Bundespolizeigesetzes verantwortlich ist. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(5) Die Maßnahme nach Absatz 1 darf nur auf Antrag des Präsidenten des Bundeskriminalamtes oder seines Vertreters durch das Gericht angeordnet werden.

(6) Die Anordnung ergeht schriftlich. In ihr sind anzugeben

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
2. eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sowie
4. die wesentlichen Gründe.

Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Anordnungsvoraussetzungen unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(7) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erhobene Daten sind unter der Sachleitung des anordnenden Gerichts nach Absatz 5 unverzüglich vom Datenschutzbeauftragten des Bundeskriminalamtes und zwei weiteren Bediensteten des Bundeskriminalamtes, von denen einer die Befähigung zum Richteramt hat, auf kernbereichsrelevante Inhalte durchzusehen. Der Datenschutzbeauftragte ist bei Ausübung dieser Tätigkeit weisungsfrei und darf deswegen nicht benachteiligt werden (§ 4f Absatz 3 des Bundesdatenschutzgesetzes). Daten, die den Kernbereich privater Lebensgestaltung betreffen, dürfen nicht verwertet werden und sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

4.1.3 Online-Durchsuchungen durch Nachrichtendienste

Die Vorgaben des Bundesverfassungsgerichts (s. o. Nr. 4.1) gelten auch für Nachrichtendienste. Online-Durchsuchungen ohne gesetzliche Grundlage sind rechtswidrig.

Nachrichtendienste sind weitgehend im „Vorfeldstadium" tätig, in dem noch keine konkreten Gefahren erkennbar sind. Innerhalb ihrer gesetzlich zugewiesenen Aufgaben beobachten sie Vorgänge und Verhaltensweisen, sofern ein tatsächlicher Anhaltspunkt für ihre Zuständigkeit besteht. Diese Schwelle ist vergleichsweise niedrig. Oftmals ist dieser Anhaltspunkt diffus, d. h. er kann auf den Beginn einer möglichen Gefahrenlage hindeuten oder in harmlosen Zusammenhängen verbleiben. Dies hat zur Folge, dass auch vollkommen unbescholtene Bürgerinnen und Bürger in den Fokus der Nachrichtendienste geraten können. Im Gegensatz zur Polizei ist die Tätigkeit der Nachrichtendienste im Regelfall gerichtlich nicht kontrollierbar.

Die Bundesregierung hatte die Befugnis der Nachrichtendienste zur Durchführung von Online-Durchsuchungen auf § 8 Absatz 2 Satz 1 und Absatz 2 Satz 2 Bundesverfassungsschutzgesetz i. V. m. einer entsprechenden Dienstvorschrift gestützt. Die Durchführung von Online-Durchsuchungen auf dieser Basis ist nach der Entscheidung des BVerfG vom 27. Februar 2008 unzulässig. Auch die Nachrichtendienste dürfen Online-Durchsuchungen nur durchführen, soweit sie dazu ausdrücklich gesetzlich ermächtigt sind. Die gesetzliche Grundlage muss den verfahrensrechtlichen Vorgaben entsprechen. Dabei ist zu beachten, dass eine Online-Durchsuchung nur unter sehr engen Voraussetzungen durchgeführt werden darf. So darf den Nachrichtendiensten eine Befugnis zur Online-Durchsuchung nicht auf der Grundlage ihrer ansonsten zulässigen Tätigkeitsschwelle gewährt werden. Soweit den Nachrichtendiensten eine Befugnis zur Online-Durchsuchung eingeräumt werden soll, müssen nach der ausdrücklichen Vorgabe des BVerfG vielmehr für die Nachrichtendienste zugeschnittene gesetzliche Voraussetzungen für den Eingriffsanlass entwickelt werden, die dem Gewicht und der Intensität der Grundrechtsgefährdung in vergleichbarem Maße Rechnung tragen, wie es der im Polizeirecht verwendete Gefahrenbegriff leistet.

Es ist zumindest fraglich, ob die Normierung einer Online-Durchsuchungsbefugnis zugunsten der Nachrichtendienste unter diesen Voraussetzungen überhaupt zulässig sein kann oder diese Befugnis allenfalls der Polizei vorbehalten bleiben muss, deren Tätigkeit im Übrigen gerichtlich kontrollierbar ist.

4.2 Veränderungen der Sicherheitsarchitektur des Bundes

Die Bundesregierung arbeitet weiter am Aus- und Umbau der Sicherheitsarchitektur von Polizeibehörden und Nachrichtendiensten.

Mit dem im Dezember 2006 vom Deutschen Bundestag verabschiedeten Gemeinsame-Dateien-Gesetz und dem Terrorismusbekämpfungsergänzungsgesetz wurden bereits wesentliche gesetzliche Grundlagen für eine neue Sicherheitsarchitektur (vgl. 21. TB Nr. 5.1) geschaffen. Zentrale Elemente dieser neuen Sicherheitsarchitektur sind z. B. die Aufnahme des Wirkbetriebs der Anti-Terror-Datei im März 2007 (s. u. Nr. 4.2.2.2), des Gemeinsamen Terrorismusabwehrzentrums – GTAZ – (vgl. 21. TB Nr. 5.1.4), des Gemeinsamen Analyse- und Strategiezentrums Illegale Migration – GASIM – (s. u. Nr. 4.2.3), des seit Beginn des Jahres 2007 betriebenen Gemeinsamen Internet-Zentrums – GIZ – sowie die Einrichtung weiterer verschiedener behördenübergreifender Informations- und Kooperationsformen.

Das Reformkonzept erstreckt sich auch auf die Weiterentwicklung der IT-gestützten Datenverarbeitung der Sicherheitsbehörden. So sind sowohl bei der technischen Infrastruktur der Polizeibehörden als auch im Bereich der Nachrichtendienste Entwicklungen zu beobachten, die darauf abzielen, alle bei den Sicherheitsbehörden vorhandenen Erkenntnisse nicht nur für die jeweilige Behörde, sondern auch für den Verbund der Sicherheitsbehörden und damit umfassend nutzbar zu machen. Das BKA beginnt beispielsweise, seine IT-Landschaft zu vereinheitlichen und personenbezogene Erkenntnisse stärker zu verknüpfen (s. u. Nr. 4.2.4). Bei den Nachrichtendiensten erfolgt eine Abkehr vom bisherigen Prinzip „Need to know" („Kenntnis nur wenn nötig") zum Prinzip „Need to share", wogegen im Hinblick auf den datenschutzrechtlichen Erforderlichkeitsgrundsatz erhebliche Bedenken bestehen. Zudem soll das nachrichtendienstliche In-

formationssystem der Verfassungsschutzbehörden des Bundes und der Länder (NADIS) durch die Aufnahme weiterer gemeinsamer Textdateien und multimedialer Dateien zu einer noch umfassenderen Informationsplattform für alle deutschen Verfassungsschutzbehörden ausgebaut werden.

Die Intensivierung der Zusammenarbeit zwischen Polizei und Nachrichtendiensten wirft bedeutsame datenschutzrechtliche Fragen auf. So ist jeweils zu klären, ob die Änderung von Zuständigkeiten, die Zuweisung neuer Befugnisse oder die Einrichtung neuer technischer Infrastrukturen das verfassungsrechtliche Trennungsgebot von Polizei und Nachrichtendiensten beeinträchtigt. Auch die angestrebte Optimierung der Zusammenarbeit darf nicht dazu führen, dass unklare oder überlappende Zuständigkeiten entstehen oder dass es zur unzulässigen Beeinträchtigung von Persönlichkeitsrechten kommt. Hierauf werde ich auch zukünftig weiterhin strikt achten.

4.2.1 Bündelung der Telekommunikationsüberwachung beim Bundesverwaltungsamt

Das Vorhaben des BMI, Einrichtungen zur Telekommunikationsüberwachung durch Polizeien und Nachrichtendienste des Bundes und der Länder beim Bundesverwaltungsamt (BVA) zusammenzufassen, begegnet datenschutzrechtlichen Bedenken.

Das Vorhaben, die Telekommunikationsüberwachung zu bündeln, in dem gemeinsame technische Anlagen zur Durchführung dieser verdeckten Datenerhebungsmaßnahme in einem Servicezentrum beim BVA bereitgestellt werden, sehe ich angesichts der unterschiedlichen Aufgaben und Befugnisse von Polizei und Nachrichtendiensten kritisch. Es besteht die Gefahr, dass dabei die Grenzen dieser unterschiedlichen Befugnisse überschritten werden und das Trennungsgebot verletzt wird. Zumindest würden derartige Infrastrukturen es erleichtern, die unterschiedlichen Maßnahmen und die dabei gewonnenen Informationen zu verknüpfen. Sollte dieses Projekt weitergeführt werden, wäre daher darauf zu achten, dass die Maßnahmen der verschiedenen Bedarfsträger von Polizei und Nachrichtendiensten organisatorisch und technisch strikt voneinander zu trennen sind. Zudem halte ich eine parlamentarische Begleitung des Projekts für unerlässlich.

Zwar begrüße ich es, dass das BMI beabsichtigt, die Aufgaben und Befugnisse des BVA im Zusammenhang mit der technischen Unterstützung von Maßnahmen der Telekommunikationsüberwachung auf eine gesetzliche Grundlage zu stellen. Der Gesetzentwurf enthält bisher aber keine akzeptablen Vorschläge zur Separierung der Unterstützungsleistungen des BVA für die verschiedenen Bedarfsträger von Polizei und Nachrichtendiensten. Vorgesehen ist eine lediglich logische Trennung der Speichermedien über die Speichersoftware. Rein logische Trennungen von Daten lassen sich aber ohne großen technischen Aufwand wieder aufheben. Angesichts der Bedeutung des Trennungsgebots für die polizeiliche und nachrichtendienstliche Datenerhebung und -verarbeitung reicht die allein über die Vergabe von Zugriffsrechten gesteuerte Trennung der erhobenen und verarbeiteten Telekommunikationsüberwachungsdaten von Polizei- und Strafverfolgungsbehörden einerseits sowie Nachrichtendiensten andererseits nicht aus. Hier bedarf es einer weitergehenden technischen Separierung, etwa auf Betriebssystemebene. Zudem muss ausgeschlossen werden, dass die im Rahmen der technischen Unterstützungsleistung eingesetzten Mitarbeiter des BVA doppelfunktional, d. h. gleichzeitig für polizeiliche und nachrichtendienstliche Bedarfsträger tätig werden. Rein fiskalische Erwägungen dürfen bei der Organisation und Durchführung von Telekommunikationsüberwachungen, die tief in den Schutzbereich des Artikel 10 GG eingreifen, nicht ausschlaggebend sein.

Daneben müssen noch weitere Fragen einer Lösung zugeführt werden.

Klärungsbedürftig ist u. a., in welchem Umfang das BVA im Rahmen seiner Beauftragung gegenüber dem jeweiligen Bedarfsträger weisungsgebunden ist. Ich halte es für problematisch, wenn nach dem Gesetzentwurf das BVA zwar den fachlichen und gesetzlichen Anforderungen des jeweiligen Auftraggebers Rechnung zu tragen hat, der einzelne Bedarfsträger jedoch keinen Anspruch darauf haben soll, dass das BVA seine technischen Einrichtungen nach dessen Wünschen konfiguriert. Im Hinblick auf die beim jeweiligen Bedarfsträger verbleibende Verantwortlichkeit bezüglich der Rechtmäßigkeit der Überwachungsmaßnahme sowie der dabei zu beachtenden Anforderungen an Datenschutz und Datensicherheit muss klar geregelt werden, dass das BVA den Weisungen des jeweiligen Bedarfsträgers zur Ausgestaltung der technischen Unterstützung, die dieser zur Wahrung seiner jeweiligen gesetzlichen Verpflichtungen für erforderlich hält, uneingeschränkt unterliegt. Entsprechende Vorkehrungen können, je nachdem auf welcher Rechtsgrundlage eine Telekommunikationsüberwachung durchgeführt wird, unterschiedlich hoch sein, so dass ein entsprechendes Auftragsverhältnis in jedem Einzelfall entsprechend ausgestaltet sein muss. Der Bedarfsträger muss zudem die Möglichkeit haben, in einem laufenden Auftragsverhältnis ergänzende Maßnahmen vom BVA zu verlangen, etwa aufgrund geänderter Rechtsprechung, oder wegen neuer technologischer Entwicklungen.

Offen ist auch, in welchem Umfang die technischen Unterstützungsmaßnahmen des BVA protokolliert werden und wie meine Beteiligungs- und Kontrollrechte bezüglich der Tätigkeit des BVA, etwa wenn das BVA Unterstützung bei Telekommunikationsüberwachungsmaßnahmen nach dem G 10-Gesetz oder für Landesbehörden leistet, gewährleistet werden.

Bei Redaktionsschluss waren die Ressortberatungen zu dem Gesetzentwurf noch nicht abgeschlossen.

4.2.2 Anti-Terror-Datei-Gesetz

Im Berichtszeitraum habe ich mich mit der Umsetzung des Ende 2006 in Kraft getretenen Anti-Terror-Datei-Gesetzes (ATDG) (vgl. 21. TB Nr. 5.1.1) befasst. Im Mittelpunkt stand dabei das Protokollierungsverfahren gemäß

§ 9 ATDG (Nr. 4.2.2.1). Schließlich habe ich auch im BKA eine Schwerpunktkontrolle der polizeilichen Datenverarbeitung in der Anti-Terror-Datei (ATD) durchgeführt (Nr. 4.2.2.2).

4.2.2.1 Die Protokollierung in der Anti-Terror-Datei gestaltet sich schwierig

Zwischen dem BMI und mir besteht ein Dissens hinsichtlich des Umfangs der nach § 9 ATDG erforderlichen Protokollierung sowie der Reichweite meiner datenschutzrechtlichen Kontrollbefugnis gemäß § 10 ATDG bezüglich dieser Protokolldaten.

Nach Auffassung des BMI wird bei einer Abfrage, die auf eine verdeckte Speicherung in der ATD trifft, kein Treffer protokolliert. Andernfalls würde dies – so die Argumentation des BMI – zu einer Offenlegung einer verdeckten Speicherung führen, was der Regelung des § 4 Absatz 1 ATDG widerspräche. Gemäß § 9 ATDG müsse nur jeder Zugriff auf die ATD protokolliert werden. Ein „Zugriff" im Sinne von § 5 ATDG liege nur vor, wenn die Daten für die abfragende Behörde auch sichtbar würden. Der Nachweis über einen Treffer auf eine verdeckte Speicherung erfolge durch die Dokumentation bei der beteiligten Behörde, die die jeweiligen Daten verdeckt gespeichert hat. Protokolldaten, die durch Datenbanktransaktionen beteiligter Landesbehörden in der ATD entstanden sind, würden zudem im datenschutzrechtlichen Verantwortungsbereich dieser Behörden stehen und dürften von mir nicht eingesehen werden.

Im Rahmen der Ressortberatungen zum ATDG hatte ich stets für eine systemseitige Vollprotokollierung, d. h. eine automatisierte, beweissichere und lückenlose Protokollierung aller Datenbanktransaktionen auf der Grundlage von Auswerteprogrammen in der ATD zu datenschutzrechtlichen Kontrollzwecken plädiert. Das BMI hat diesem Petitum entsprochen und meinen Formulierungsvorschlag in die Gesetzesbegründung wortidentisch übernommen. Diese Begründung konkretisiert inhaltlich die Regelungen des § 9 Absatz 1 ATDG. Demnach ist das BKA verpflichtet, in der ATD alle Datenbanktransaktionen lückenlos und auswertbar zu Datenschutzkontrollzwecken zu protokollieren. Hierzu zählen auch die verdeckt erfolgten Speicherungen im Sinne von § 4 Absatz 1 Satz 1 2. Alt. ATDG sowie die durch eine Anfrage ausgelösten Treffer auf verdeckt gespeicherte Daten. Die strenge Zweckbindung des § 9 Absatz 1 Satz 1 ATDG gewährleistet, dass keine Offenlegung von verdeckt erfolgten Speicherungen gegenüber den an der ATD beteiligten Stellen erfolgt. Die umfassende Protokollierung und Auswertbarkeit der Protokolldaten ist eine zentrale Verfahrenssicherung und damit ein adäquater Ausgleich zu dem mit dem ATDG erstmals gesetzlich legitimierten Informationspool von Polizeien und Nachrichtendiensten, der in besonders schwerwiegender Weise in das Recht der Betroffenen auf informationelle Selbstbestimmung eingreift und mit erheblichen verfassungsrechtlichen Risiken behaftet ist. Eine Beschränkung der nach § 9 Absatz 1 ATDG bestehenden umfassenden Protokollierungsverpflichtung durch bzw. im Hinblick auf die Regelungen des § 4 Absatz 1 ATDG ist weder dem Wortlaut dieser Regelung noch den jeweiligen Gesetzesbegründungen zu entnehmen. Bei der Durchführung datenschutzrechtlicher Kontrollen verdeckter Speicherungen in der ATD bin ich jedoch gegenwärtig auf die Vorlage entsprechender Dokumentationen durch die jeweilige Behörde angewiesen, ohne die Möglichkeit zu haben, diese Angaben durch Auswertung der Protokolldaten zu verifizieren. Dies entspricht nicht den Erfordernissen einer unabhängigen und effizienten Datenschutzkontrolle.

Für eine Beschränkung meiner Kontrollbefugnisse bezüglich der durch Datenbanktransaktionen beteiligter Landesbehörden in der ATD generierten Protokolldaten sehe ich ebenfalls keine Rechtsgrundlage. Das BKA hat die Aufgabe, für Zwecke der Datenschutzkontrolle die Zugriffe auf die ATD zu protokollieren. Die Durchführung dieser Aufgabe wird von meiner Behörde gemäß § 10 ATDG datenschutzrechtlich kontrolliert. Lediglich die datenschutzrechtliche Kontrolle der Eingabe und Abfrage von Daten durch eine Landesbehörde richtet sich nach dem jeweiligen Datenschutzgesetz des betreffenden Landes. Der Umfang der datenschutzrechtlichen Verantwortung wird im Übrigen durch § 8 ATDG festgelegt. Protokolldaten, die durch Datenverarbeitungsmaßnahmen in der ATD entstehen, werden durch diese Regelung nicht erfasst. Keinesfalls darf ein datenschutzrechtlich kontrollfreier Raum entstehen. Ich bin darauf angewiesen, dass ich z. B. bei einer Auswertung von Protokolldaten zu einer bestimmten, in der ATD gespeicherten Person auch erkennen können muss, welche Landesbehörden Daten zu dieser Person verarbeitet haben, um den zuständigen Landesdatenschutzbeauftragten entsprechend einbinden bzw. informieren zu können. Die Sichtweise wird von den Datenschutzbeauftragten der Länder geteilt.

Das BMI hat vorgeschlagen, dass die Landesdatenschutzbeauftragten die Protokolldaten, die durch Datenbanktransaktionen der jeweils ihrer Kontrollbefugnis unterliegen Landesstellen entstanden sind, im BKA selbst einsehen und auswerten können. Ich habe dieses Verfahren vorerst akzeptiert. Die nächsten Jahre werden zeigen, inwieweit dadurch eine effiziente Kontrolle der Datenverarbeitung in der ATD durch die daran beteiligten Bundes- und Landesbehörden gewährleistet werden kann.

4.2.2.2 Kontrolle der Anti-Terror-Datei beim Bundeskriminalamt

Bei der Datenverarbeitung in der ATD habe ich einige datenschutzrechtliche Mängel festgestellt. Dies gilt insbesondere für die Problematik der Speicherung von „Randpersonen".

Als ein zentraler Bestandteil der neuen Sicherheitsarchitektur des Bundes (vgl. 21. TB Nr. 5.1) wurde im März 2007 die Anti-Terror-Datei (vgl. 21. TB Nr. 5.1.1) durch den Bundesminister des Innern offiziell „freigeschaltet". Zu Beginn wurden Informationen über rund 13 000 Personensätze in der ATD gespeichert; bis Ende Mai 2008 wuchs diese Zahl auf 17.745 an. Die Zahl der tatsächlich erfassten Betroffenen dürfte aber niedriger liegen, da einzelne Personen von verschiedenen Stellen

(mehrfach) gespeichert worden sein können. Dies ist bedingt durch die Struktur der Datenbank.

Im März 2008 führte ich eine datenschutzrechtliche Kontrolle der Datenverarbeitung in der ATD durch das BKA durch. Zu diesem Zeitpunkt hatte das BKA dort ca. 3 000 Datensätze eingegeben. Einen Schwerpunkt meiner Kontrolle bildete die Problematik der Speicherung von Kontaktpersonen und weiterer Randpersonen in der ATD, besonders unter dem Aspekt der Hinzuspeicherung von erweiterten Grunddaten. Hierbei wurden im Einzelnen die Kriterien „besuchte Orte oder Gebiete“, „Kontaktperson“ und „Bemerkungen/Hinweise“ sowie die Einstufung einer Person als „dolose“ Kontaktperson betrachtet.

„Besuchte Orte oder Gebiete“ nach § 3 Absatz 1 Nummer 1 lit. b) nn) ATDG dürfen als erweiterte Grunddaten in der ATD gespeichert werden, sofern sich dort die in § 2 Satz 1 Nummern 1 und 2 ATDG genannten Personen treffen. Ich habe bemängelt, dass in vielen der geprüften Fälle aus der Speicherung und den dazu vorgelegten Unterlagen nicht erkennbar war, ob die gespeicherten Örtlichkeiten tatsächlich als Treffpunkte in diesem Sinne dienten.

Hingegen war die Speicherung von „Kontaktpersonen“ als erweitertes Grunddatum gemäß § 3 Absatz 1 Nummer 1 lit. b) oo) ATDG in den geprüften Fällen nicht zu beanstanden. Die Voraussetzungen, dass zwischen der Kontaktperson und der Zielperson nicht nur flüchtige oder zufällige Verbindungen bestehen und dass es sich bei der Zielperson um eine „Hauptperson“ handelt, also um ein Mitglied einer terroristischen Vereinigung oder um einen Befürworter von Gewalt als Mittel zur Durchsetzung international ausgerichteter politischer oder religiöser Belange, waren bei den geprüften Datensätzen für die Erfassung in der ATD erfüllt.

Bei den Speicherungen von „Bemerkungen/Hinweisen“ im Sinne von § 3 Absatz 1 Nummer 1 lit. b) rr) ATDG war nur in seltenen Fällen nachvollziehbar, warum dies – wie der Gesetzgeber voraussetzt – im Einzelfall nach pflichtgemäßem Ermessen geboten und zur Aufklärung oder Bekämpfung des internationalen Terrorismus unerlässlich war. Die Problematik bestand darin, dass bei der automatischen Befüllung der ATD mit einem Datensatz aus einer Quelldatei des polizeilichen Staatsschutzes auch das dort gespeicherte Freitextfeld mit übertragen wurde, ohne dass die vom Gesetzgeber geforderte Einzelfallprüfung hinsichtlich der ATD-Relevanz zuvor durchgeführt worden war. Nach Feststellung dieses schwerwiegenden Mangels ist das Verfahren insofern geändert worden, als das BKA vor Überführung eines ATD-relevanten Datensatzes alle Freitextfelder in der Quelldatei der geforderten Einzelfallüberprüfung unterziehen wird und vom BKA eine Löschung aller bisher in der ATD gespeicherten Freitextfelder vorgenommen worden ist. Meines Erachtens bedarf es eines solchen Verfahrens auch bei der Speicherung „besuchter Orte oder Gebiete“ im Sinne von § 3 Absatz 1 Nummer 1 lit. b) nn) ATDG. Die Möglichkeiten, Angaben über Örtlichkeiten in einer Quelldatei des polizeilichen Staatsschutzes speichern zu dürfen, sind weniger restriktiv als im Zusammenhang mit der Speicherung in der ATD, da die Tatbestandsvoraussetzung, dass sich dort die in § 2 Satz 1 Nummern 1 und 2 ATDG genannten Personen treffen, nicht besteht. Es bedarf also auch insofern einer Einzelfallbetrachtung, inwieweit Angaben zu einem besuchten Ort oder zu einer Örtlichkeit in der Quelldatei die einschränkenden Voraussetzungen des ATDG erfüllen.

Die Speicherung „doloser“ Kontaktpersonen in der ATD sehe ich nach wie vor kritisch. Dolos bedeutet in diesem Zusammenhang, dass bei diesen Personen tatsächliche Anhaltspunkte dafür vorliegen, dass sie von der Planung oder Begehung einer terroristischen Straftat oder der Ausübung, Unterstützung oder Vorbereitung von rechtswidriger Gewalt im Sinne des ATDG Kenntnis haben. Zu diesen „dolosen“ Kontaktpersonen können auch erweiterte Grunddaten in der ATD gespeichert werden. Dies sehe ich insbesondere in Bezug auf Randpersonen kritisch.

Im Rahmen der Kontrolle erwies es sich als schwierig, aussagefähige Belege oder tatsächliche Anhaltspunkte für eine belastbare Aussage zu einer entsprechend positiven Kenntnis zu eruieren. Insofern mangelte es an einer soliden Grundlage für die Speicherung der erweiterten Grunddaten. Damit bestätigte sich meine Befürchtung, dass eine gesetzeskonforme Qualifizierung einer Kontaktperson als „dolos“ auf der Grundlage objektiver Verhaltensumstände in der Praxis kaum möglich sein dürfte. Die hierfür herangezogenen Umstände und Erkenntnisse sind meist von vager oder ambivalenter Natur und rechtfertigen deshalb einen derartigen Eingriff in das Recht auf informationelle Selbstbestimmung des Einzelnen vielfach nicht.

Die Kontrolle der Datenverarbeitung in der ATD durch die Polizeien und Nachrichtendienste des Bundes wird auch im kommenden Berichtszeitraum ein Schwerpunkt meiner Tätigkeit sein.

4.2.3 Gemeinsames Analyse- und Strategiezentrum Illegale Migration (GASIM)

Das gemeinsame Analyse- und Strategiezentrum Illegale Migration (GASIM) soll die Zusammenarbeit der beteiligten öffentlichen Stellen des Bundes bei der Bekämpfung der illegalen Migration intensivieren. Seine Arbeitsweise ist Gegenstand einer datenschutzrechtlichen Prüfung.

Gegen Ende des Berichtszeitraums habe ich im GASIM einen Beratungs- und Kontrollbesuch durchgeführt. Gegenstand des Besuchs war die Erhebung und Verarbeitung personenbezogener Daten durch die am GASIM beteiligten Behörden des Bundes. Insbesondere habe ich untersucht, in welchem Umfang die Sicherheitsbehörden innerhalb des GASIM miteinander kooperieren.

Das GASIM hat am 2. Mai 2006 in Berlin seine Arbeit aufgenommen. An ihm sind das Bundeskriminalamt, die Bundespolizei, das Bundesamt für Migration und Flüchtlinge, die Finanzkontrolle Schwarzarbeit der Zollverwaltung, der Bundesnachrichtendienst, das Bundesamt für Verfassungsschutz und das Auswärtige Amt beteiligt. Das GASIM soll die Fachkompetenzen der beteiligten Behör-

den und Stellen bei der Bekämpfung der illegalen Migration und ihrer Begleit- und Folgekriminalität intensivieren und bündeln. Insoweit ist es eine behördenübergreifende Informations- und Kooperationsplattform. Die Zuständigkeiten und Entscheidungskompetenzen der beteiligten Behörden und Stellen bleiben unberührt. Bestehende rechtliche Rahmenbedingungen werden nicht verändert. Das GASIM ist daher keine eigenständige Behörde oder Organisation. Die Erhebung und Verarbeitung personenbezogener Daten durch die jeweiligen Behörden hat nach den für sie geltenden Rechtsvorschriften zu erfolgen. In Anlehnung an die Organisation des gemeinsamen Terrorismusabwehrzentrums (vgl. 21. TB Nr. 5.1.4) erfolgt im GASIM die Zusammenarbeit und der Informationsaustausch in den verschiedenen Arbeitsfeldern in Kooperationsforen unter verschiedener, sich aus der jeweiligen Zuständigkeit ergebenden Geschäftsführung einer der am GASIM beteiligten Behörden.

Im Rahmen meines Beratungs- und Kontrollbesuchs habe ich vor allem den personenbezogenen Datenaustausch im Forum 4 („Nachrichtendienstlich-taktische und -strategische Lage“) unter der Geschäftsführung des BND sowie im Forum 7 („Operative Maßnahmen im Zusammenhang mit der illegalen Migration“) unter der Geschäftsführung der Bundespolizei näher untersucht. Es ist zu überprüfen, inwieweit die am GASIM beteiligten Behörden im Rahmen der bestehenden Übermittlungsregelungen in zulässiger Weise personenbezogene Daten ausgetauscht haben. In diesem Zusammenhang sind die im Bundesverfassungsschutzgesetz, im BND-Gesetz, im Bundespolizeigesetz, im BKA-Gesetz, im SGB X sowie im Asylverfahrensgesetz enthaltenen Übermittlungsvorschriften, die Möglichkeiten und Grenzen dieser Zusammenarbeit regeln, zu beachten.

Bis Redaktionsschluss hatte ich das umfangreiche Material, welches ich im Rahmen meines Beratungs- und Kontrollbesuchs eingesehen habe, noch nicht abschließend ausgewertet. Das Ergebnis der Kontrolle werde ich im nächsten Tätigkeitsbericht erörtern.

4.2.4 Neugestaltung der IT-Landschaft in der Abteilung Staatsschutz des Bundeskriminalamts

Das BKA richtet in der Abteilung Staatsschutz neue Dateien ein und nutzt hierfür das Programm rsCASE. Dadurch sollen Informationen besser verarbeitet und verknüpft werden.

Das BKA als Zentralstelle der deutschen Polizei sowie als Ermittlungsorgan für besondere Verfahren hat mit unterschiedlichsten Phänomenbereichen der Kriminalität und mit entsprechend vielen speziellen Datenverarbeitungssystemen zu tun. Im Laufe der Zeit ist die Dateienlandschaft immer weiter angewachsen. Die Applikationsvielfalt und die Verwendung unterschiedlicher technischer Plattformen lässt die Anzahl erforderlicher Schnittstellen exponentiell ansteigen. Letztlich besteht nach Auffassung des BKA die Gefahr, dass wichtige Informationen nicht erkannt werden oder verloren gehen. Daher hat das BKA im Berichtszeitraum ein Projekt eingesetzt, in dessen Rahmen die Dateienlandschaft in der Abteilung Staatsschutz neu gestaltet und vereinheitlicht werden soll. Als zentrales Eingangssystem für die spätere Weiterleitung von Erkenntnissen und Informationen in die jeweilige Fachdatei dient hierbei das Vorgangsbearbeitungssystem des BKA. Die neue Struktur der Fachdateien folgt den Aufgaben des BKA als Zentralstelle sowie als ermittlungsführende Behörde und orientiert sich zugleich an bestimmten Phänomenbereichen der Kriminalität. Für die Abteilung Staatsschutz des BKA werden beispielsweise für die Bereiche „Spionage/Technologietransfer“, „Politisch Motivierte Kriminalität“ und „Internationaler Terrorismus und Extremismus“ eigene Dateien eingerichtet, die analog den BKA-Funktionen als Zentralstelle und Strafverfahrens- bzw. Ermittlungsorgan als zwei getrennte Varianten „Z“ und „S“ existieren.

Für die neu eingerichteten Dateien der Abteilung Staatsschutz wird als systemtechnische Grundlage das Programm rsCASE verwendet, das bereits bei verschiedenen Polizeien der Länder genutzt wird. Das Programm rsCASE ermöglicht es, Verknüpfungen von Daten und Beziehungen zwischen beteiligten Personen – auch komplizierter Art – zu erkennen und grafisch aufzubereiten.

Aus datenschutzrechtlicher Sicht kritisch zu werten ist die Praxis des BKA, auch in den neuen Dateien solche Angaben zu speichern, die als sog. Prüffall qualifiziert worden sind. Dabei handelt es sich um Informationen, die nicht nach § 8 BKA-Gesetz (BKAG) kategorisierbar sind, d. h. die nicht z. B. einer beschuldigten oder verdächtigen Person zugeordnet werden können. Die Speicherung personenbezogener Daten kann hier nur auf die Generalermächtigungsklausel des § 7 BKAG gestützt werden. Dadurch entsteht jedoch die Gefahr, dass auch die Daten von unbeteiligten oder ggf. nur zufällig angetroffenen Personen gespeichert werden. Deshalb hatte ich bei den bisher geführten Auswertedateien (vgl. 20. TB Nr. 5.2.5) erreicht, dass die Daten von derartigen „Prüffällen“ nur für zwei Jahre gespeichert werden dürfen und danach, falls in diesem Zeitraum keine weiteren einschlägigen Erkenntnisse hinzutreten, gelöscht werden müssen. Zudem dürfen diese Daten nicht an Dritte, z. B. anfragende Behörden, übermittelt werden. Zwar begrüße ich, dass diese Regelungen für die neuen Dateien der Abteilung Staatsschutz übernommen werden. Dennoch besteht weiterhin die Gefahr, dass in einer Vielzahl von Fällen Informationen zu Personen, die an der Begehung von Straftaten nicht beteiligt oder ggf. nur zufällig an bestimmten Orten anwesend sind, gespeichert werden oder diese gar in den Fokus von Ermittlungen geraten.

Auch in der Zukunft werde ich darauf achten, dass das BKA bei verbesserten technischen Datenverarbeitungsmöglichkeiten den durch das BKA-Gesetz gesteckten Rechtsrahmen einhält.

4.3 Bundeskriminalamt

Schwerpunkte meiner Tätigkeit im Berichtszeitraum waren die Novellierung des BKA-Gesetzes (s. u. Nr. 4.3.1) sowie die Fortentwicklung des polizeilichen Informationssystems INPOL (s. u. Nr. 4.3.2).

4.3.1 BKA-Gesetzesnovelle

Durch die Novellierung des BKA-Gesetzes werden dem BKA erstmals umfassende polizeiliche Befugnisse zur Abwehr des internationalen Terrorismus eingeräumt. Datenschutzrechtliche Kritik wurde dabei nur zum Teil berücksichtigt.

Die durch die Föderalismusreform vorgezeichnete Aufgabenzuweisung an das BKA bedeutet eine Zäsur in der bundesdeutschen Sicherheitsarchitektur (vgl. Kasten a zu Nr. 4.3.1). Die deutsche Polizei war in der Bundesrepublik Deutschland von Beginn an Ländersache. Die Zuweisung präventiver Befugnisse an das BKA verändert diese Kompetenzaufteilung, die letztlich auch öffentliche Gewalt begrenzende Ziele verfolgte.

Die BKA-Gesetzesnovelle begegnet vor allem zwei wesentlichen Kritikpunkten:

Ich habe weiterhin erhebliche Zweifel, inwieweit die vorgesehenen Datenerhebungs- und -verarbeitungsbefugnisse für die Erfüllung der dem BKA zugewiesenen Aufgaben wirklich angemessen, erforderlich und geeignet sind. Neben polizeilichen Standardbefugnissen, z. B. Platzverweis oder Personalienfeststellung, erhält das BKA zusätzlich besondere Ermittlungsbefugnisse bis hin zur Online-Durchsuchung informationstechnischer Systeme. Schon im Hinblick auf die weiterhin bestehende Zuständigkeit der Länder bei der Abwehr von Gefahren des internationalen Terrorismus ist fraglich, ob für die wenigen Fälle, in denen das BKA selbst tätig werden wird, diese Fülle neuer Befugnisse wirklich angemessen ist. So sind Eingriffsmaßnahmen mit großem zeitlichen Vorlauf, etwa die Rasterfahndung, nicht geeignet, um auf terroristische Bedrohungslagen schnell zu reagieren. Schutzpolizeiliche Standardbefugnisse setzen eine flächendeckende Präsenz des Amtes voraus, die faktisch nicht gegeben ist. Das Nebeneinander von Zuständigkeiten des BKA und der Landespolizeibehörden für die Gefahrenabwehr sehe ich auch insofern kritisch, als es dazu führt, dass sowohl das BKA als auch die Länder parallele Abwehrmaßnahmen ergreifen können und dabei gleich mehrfach personenbezogene Daten verarbeiten.

Die dem BKA eingeräumten heimlichen Eingriffsbefugnisse greifen in einer Weise in die Persönlichkeitsrechte ein, die bislang ganz wesentlich den Nachrichtendiensten vorbehalten waren. Waren bei den Nachrichtendiensten diese sog. nachrichtendienstlichen Mittel deshalb vertretbar, weil die Dienste keinerlei exekutive Befugnisse besitzen, so verhält sich dies hier anders: Wenden Polizeibehörden heimliche Ermittlungsmethoden an, können diese mit exekutiven Befugnissen verbunden werden. Dies erhöht die Eingriffsintensität und die Folgen für den Betroffenen ganz erheblich.

Schließlich geht es auch um das Verhältnis zwischen Prävention und Strafverfolgung. Bereits vor der Novelle hatte das BKA die Befugnis, in bestimmten Deliktsbereichen Ermittlungen vorzunehmen, allerdings unter der Verfahrensleitung der Generalbundesanwaltschaft und nach den Regeln der Strafprozessordnung. Zu diesen Deliktsbereichen zählt auch die Bildung terroristischer Vereinigungen. In diesen Fällen wäre das BKA also auf Gefahren abwehrende Befugnisse nicht angewiesen.

Kasten a zu Nr. 4.3.1

Ergebnis der Förderalismusreform

Mit dem Gesetz zur Änderung des Grundgesetzes vom 28. August 2006 (BGBl. I 2006 S. 2034) wurde u. a. eine neue ausschließliche Bundeskompetenz zur Regelung präventiver Befugnisse des BKA bei der Abwehr von Gefahren des internationalen Terrorismus geschaffen.

Artikel 73 GG wurde dazu wie folgt geändert:

cc) Nach Nummer 9 wird folgende Nummer 9a eingefügt:

„9a. die Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalpolizeiamt in Fällen, in denen eine länderübergreifende Gefahr vorliegt, die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist oder die oberste Landesbehörde um eine Übernahme ersucht;“.

Der andere wesentliche Kritikpunkt an dem Gesetz betrifft die Gewährleistung des Kernbereichs privater Lebensgestaltung. Das Bundesverfassungsgericht hat in mehreren Entscheidungen in den letzten Jahren dem Gesetzgeber aufgegeben, diesen Kernbereich bei heimlichen Datenerhebungsbefugnissen abzusichern, insbesondere indem Eingriffe in diesen Bereich soweit möglich von vornherein unterbleiben. Dieses Erhebungsverbot muss zudem durch Regelungen über die sofortige Löschung intimer Informationen und der Nicht-Verwertbarkeit ergänzt werden, wenn es ausnahmsweise doch zu einer Kernbereichsverletzung gekommen ist. Das BKA-Gesetz weist insofern Defizite auf. So verbleiben verfassungsrechtliche Zweifel daran, dass die Online-Durchsuchung informationstechnischer Systeme (s. o. Nr. 4.1.2) sowie die Überwachung der Telekommunikation nur unzulässig sein sollen, wenn aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass *allein* kernbereichsrelevante Inhalte erfasst werden. Da diese Fälle in der Praxis kaum vorkommen werden, läuft das Gebot, Eingriffe in den Kernbereich privater Lebensgestaltung grundsätzlich zu unterlassen, weitgehend ins Leere. Auch ist es aus meiner Sicht unzureichend, wenn im Zusammenhang mit der Erhebung von Daten mit besonderen Mitteln gemäß § 20g BKAG, wie z. B. längerfristige Observationen oder der Einsatz verdeckter Ermittler, von Regelungen zum Schutz des Kernbereichs völlig abgesehen wurde.

Diese Kritik wird von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder geteilt (vgl. Kasten b zu Nr. 4.3.1).

Im Zuge des Gesetzgebungsverfahrens wurden aber auch – gemessen an den Vorentwürfen – einige Verbesserungen vorgenommen. So wurde die Gefahrenschwelle als Voraussetzung für die Durchführung einer Rasterfahn-

Kasten b zu Nr. 4.3.1

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008

Mehr Augenmaß bei der Novellierung des BKA-Gesetzes

Der vom Bundesministerium des Innern erarbeitete Referentenentwurf eines Gesetzes zur Abwehr des internationalen Terrorismus durch das Bundeskriminalamt hat zum Ziel, das Bundeskriminalamt mit umfassenden polizeilichen Befugnissen zur Verhütung von terroristischen Straftaten und zur Abwehr von Gefahren für die öffentliche Sicherheit in diesem Zusammenhang auszustatten. Insbesondere sind Befugnisse zur Durchsuchung, Rasterfahndung, Wohnraumüberwachung und Telekommunikationsüberwachung vorgesehen. Außerdem will das Bundesinnenministerium eine Befugnis zum heimlichen Zugriff auf informationstechnische Systeme („Online-Durchsuchung“) in das BKA-Gesetz aufnehmen.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dagegen aus, dass dem Bundeskriminalamt nach dem Gesetzentwurf mehr Befugnisse eingeräumt werden sollen, als einzelnen Landespolizeien zur Erfüllung ihrer eigenen Gefahrenabwehraufgaben zustehen. Sie halten es daher für geboten, im weiteren Gesetzgebungsverfahren die Befugnisse des BKA auf die zur Aufgabenerfüllung zwingend notwendigen Kompetenzen zu beschränken.

Die bisherige informationelle Gewaltenteilung zwischen den Polizeien der Länder und dem BKA diente auch dem Datenschutz. Die Konferenz fordert deshalb eine klare, d. h. hinreichend trennscharfe Abgrenzung der spezifischen Befugnisse des Bundeskriminalamts einerseits zu denen der Landespolizeien und Verfassungsschutzbehörden andererseits.

Dem Referentenentwurf zufolge soll die Aufgabenwahrnehmung durch das Bundeskriminalamt die Zuständigkeit der Landespolizeibehörden auf dem Gebiet der Gefahrenabwehr unberührt lassen. Dies führt zu erheblichen datenschutzrechtlichen Problemen, da nach geltendem Recht auch die Länder bei Abwehr einer durch den internationalen Terrorismus begründeten Gefahr parallele Abwehrmaßnahmen ergreifen können. Angesichts der Weite der für das Bundeskriminalamt vorgesehenen und den Landespolizeibehörden bereits eingeräumten Datenerhebungs- und Datenverarbeitungsbefugnisse steht zu befürchten, dass es zu sich überlappenden und in der Summe schwerwiegenderen Eingriffen in das informationelle Selbstbestimmungsrecht Betroffener durch das Bundeskriminalamt und die Landespolizeibehörden kommen wird.

Ebenso stellt sich die grundsätzliche Frage der Abgrenzung von Polizei und Verfassungsschutz. In den vergangenen Jahren sind die Polizeigesetze des Bundes und der Länder zunehmend mit Befugnissen zur verdeckten Datenerhebung (z. B. heimliche Video- und Sprachaufzeichnungen, präventive Telekommunikationsüberwachung) ausgestattet worden. Zudem wurden die Eingriffsbefugnisse immer weiter ins Vorfeld von Straftaten und Gefahren erstreckt. Damit überschneiden sich die polizeilichen Ermittlungsbefugnisse zunehmend mit denen des Verfassungsschutzes.

Das Bundesverfassungsgericht hat in seinem Urteil zur „Online-Durchsuchung“ vom 27. Februar 2008 den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung zu gewährleisten. Diese Vorgabe des Gerichts gilt nicht nur für eine etwaige gesetzliche Regelung zur „Online-Durchsuchung“, sondern für alle Eingriffsmaßnahmen. Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber deshalb auf, im Rahmen der Novellierung des BKA-Gesetzes den Schutz des Kernbereichs privater Lebensgestaltung für alle Eingriffsmaßnahmen zu regeln.

dung gemäß § 20j BKAG entsprechend den verfassungsgerichtlichen Vorgaben konkretisiert. Die Anordnung der Rasterfahndung unterliegt jetzt dem Richtervorbehalt. Die ursprünglich vorgesehene Eilfallregelung wurde gestrichen, so dass in jedem Fall ein Richter über die Durchführung von Online-Durchsuchungen zu entscheiden hat. Auch die Verwertung der bei einer solchen Maßnahme anfallenden Daten soll, sofern sie möglicherweise den Kernbereich privater Lebensgestaltung betreffen, nur mit richterlicher Genehmigung erfolgen. Auch konnte erreicht werden, dass die Bedingungen für die zulässige Übermittlung von Erkenntnissen des BKA an die Nachrichtendienste verschärft wurden.

Positiv ist schließlich, dass der Gesetzgeber eine Verpflichtung zur Evaluierung der neuen Aufgabenzuweisung für das BKA sowie der Befugnisse zur Rasterfahndung und zum verdeckten Eingriff in informationstechnische Systeme (s. o. Nr. 4.1.2) nach Ablauf von fünf Jahren beschlossen hat.

Ob die neue Aufgabe des BKA zu dem versprochenen „Mehr“ an Sicherheit führen wird, dürfte jedenfalls erst in einigen Jahren abschätzbar sein, wenn das Gesetz entsprechend evaluiert worden ist.

Das novellierte BKA-Gesetz ist am 1. Januar 2009 in Kraft getreten (BGBl. I 2008 S. 3083).

4.3.2 Polizeiliches Informationssystem INPOL

INPOL wird laufend fortentwickelt.

Auch im Berichtszeitraum haben sich Bund-Länder-Gremien insbesondere mit der konzeptionellen Weiterentwicklung des polizeilichen Informationssystems INPOL befasst. Als vorläufiges Ergebnis wurde der Bedarf nach einem einheitlichen „polizeilichen Informationsmodell“ mit dem Grundsatz „Einmalerfassung und Mehrfachnutzung“ formuliert, das den INPOL-Dateien zugrunde liegen und von allen INPOL-Teilnehmern angewandt werden soll. Im November 2008 hat die Ständige Konferenz der Innenminister und -senatoren der Länder das Ergebnis der Arbeitsgruppe zustimmend zur Kenntnis genommen. Im Rahmen einer Projektgruppe und ggf. eines Pilotbetriebes sollen unter Federführung des BKA im Weiteren nähere Einzelheiten des polizeilichen Informationsmodells und dessen Anwendung in der Praxis erarbeitet werden.

Ein weiteres Vorhaben im Rahmen des polizeilichen Informationssystems hat das Ziel, die bisherigen sog. INPOL-Fall-Dateien durch einen polizeilichen Informations- und Analyseverbund (PIAV) abzulösen, in welchem übergreifende, auf bestimmte Kriminalitätsphänomene bezogene Dateien – nach Relevanzprüfung – einschlägige Informationen und personenbezogene Daten zusammenfassen. Zu beiden Projekten liegen lediglich erste Überlegungen vor, so dass es für eine abschließende datenschutzrechtliche Bewertung noch zu früh ist.

Daneben waren eine Reihe anderer Aspekte zu beachten, die sich auf den aktuellen Betrieb von INPOL beziehen. Dies betraf den erforderlichen Umfang der Protokollierung von Zugriffen (vgl. Nr. 4.3.2.1) sowie die Zulässigkeit der Speicherung personenbezogener Daten von Minderjährigen (vgl. Nr. 4.3.2.2).

4.3.2.1 Protokollierung im polizeilichen Informationssystem (INPOL)

Die Vorgabe der BKA-Gesetzesnovelle, dass jeder Zugriff auf das polizeiliche Informationssystem INPOL zu protokollieren ist, wirft die Frage auf, inwieweit auch die Inhalte von Datenfeldern protokolliert werden sollen.

Die am 1. Januar 2009 in Kraft getretene Novelle des BKA-Gesetzes (vgl. Nr. 4.3.1) beinhaltet auch eine grundlegende Änderung der Protokollierungsregelungen im polizeilichen Informationssystem INPOL. Durch die Neufassung von § 11 Absatz 6 Satz 1 BKA-Gesetz (BKAG) entfällt die Beschränkung, lediglich jeden zehnten Abruf zu protokollieren. Künftig hat das BKA „bei jedem Zugriff für Zwecke der Datenschutzkontrolle den Zeitpunkt, die Angaben, die die Feststellung der aufgerufenen Datensätze ermöglichen, sowie die für den Zugriff verantwortliche Dienststelle zu protokollieren“. Zudem ist die Auswertung der Protokolldaten nach dem Stand der Technik zu gewährleisten. Mit der Gesetzesänderung wird ein seit langem bestehendes und wiederholt von den Datenschutzbeauftragten des Bundes und der Länder vorgebrachtes Anliegen (zuletzt 19. TB Nr. 13.8) berücksichtigt. Die Protokollierung sämtlicher Abrufe aus INPOL ermöglicht eine effektivere Kontrolle der polizeilichen Datenverarbeitung.

Im Zusammenhang mit der Änderung der Protokollierung stellte sich aber auch die Frage, inwieweit eine inhaltliche Protokollierung von Änderungen und Zugriffen auf Daten erfolgen soll, ob also nur die Tatsache einer Änderung selbst oder auch die Inhalte der Datenfelder, die geändert werden, in den Protokollen festgehalten werden.

Anlässlich eines Informationsbesuches im Juli 2008 hat mir das BKA die Protokollierungspraxis beim polizeilichen Informationssystem INPOL vorgestellt. Hier existieren drei Varianten der Protokollierung von Datenabrufen: die Nachrichtenprotokollierung, die fachliche Protokollierung und die technische Protokollierung (s. Kasten a zu Nr. 4.3.2.1).

Kasten a zu Nr. 4.3.2.1

Verfahren zur Protokollierung von Datenabrufen im polizeilichen Informationssystem INPOL:

- Die Nachrichtenprotokollierung dient der Sicherstellung der Nachvollziehbarkeit des Austausches von Nachrichten oder Anfragen und korrespondierenden Antworten in INPOL zwischen dem Zentralsystem des BKA und den Landessystemen der INPOL-Teilnehmer. Diese Variante der Protokollierung erfolgt auf der Grundlage des § 9 BDSG.
- Die fachliche Protokollierung geschieht innerhalb des BKA-spezifischen Teils von INPOL. Hier werden die Abrufe und Transaktionen, die beim BKA erfolgen, systemseitig vollständig erfasst. Durch technische Maßnahmen – Auflegen eines „Viewers“ – wurde jedoch bis 31. Dezember 2008 der für datenschutzrechtliche Kontrollzwecke vorgesehene Datenbestand gemäß der bis dahin geltenden Fassung des § 11 Absatz 6 Satz 1 BKAG auf 10 Prozent reduziert.
- Die technische Protokollierung verfolgt allein Zwecke zur Gewährleistung der Datensicherheit, z. B. zur Ermöglichung der Fehlersuche. Hierbei werden in der Regel nur systemtechnische Angaben, aber keine personenbezogenen Daten gespeichert.

Sowohl bei der fachlichen als auch bei der Nachrichtenprotokollierung werden auch die Inhalte der geänderten oder aufgerufenen Datenfelder erfasst. Hieran möchte das BKA auch festhalten, wenn künftig alle Zugriffe auf INPOL protokolliert werden.

Bei der Beurteilung der Erforderlichkeit einer Inhaltsprotokollierung der Datenbanktransaktionen sind die Möglichkeiten einer effektiveren Datenschutzkontrolle sowie die Wahrung des Rechtsschutzinteresses der Betroffenen gegen die Entstehung paralleler Datenbestände und der damit einhergehenden Missbrauchsgefahren abzuwägen. Dabei ist nicht auszuschließen, dass ohne inhaltliche Protokollierung bei zwischenzeitlich gelöschten oder geän-

derten Datensätzen eine datenschutzrechtliche Überprüfung wesentlich erschwert wird. Hinzu kommt, dass im Hinblick auf den im BKA begrenzten Personenkreis, der Zugriff auf die Protokolldaten erhalten soll, das Missbrauchsrisiko sehr begrenzt ist. Zu bedenken ist allerdings auch, dass die protokollierten Daten gemäß § 11 Absatz 6 BKAG nicht ausschließlich zu Datenschutzkontroll- oder Datensicherungszwecken, sondern auch ausnahmsweise zur Verhinderung oder Verfolgung einer schwerwiegenden Straftat gegen Leib, Leben oder Freiheit einer Person verwendet werden dürfen. Das BKA hat mir hierzu allerdings mitgeteilt, dass bisher nur in einem Fall – einem Tötungsdelikt – die INPOL-Protokolldaten zu kriminalpolizeilichen Zwecken genutzt worden sind.

Da INPOL ein von Bund und Ländern gemeinsam betriebenes System ist, werde ich auf eine gemeinsame Position mit den Datenschutzbeauftragten der Länder hinwirken (Regelungen zur Protokollierung s. Kasten b zu Nr. 4.3.2.1).

Kasten b zu Nr. 4.3.2.1

Gesetzliche Regelungen zur Protokollierung von Datenabrufen aus Informationssystemen:

– Bundeskriminalamtsgesetz:

§ 11 Polizeiliches Informationssystem

(6) Das Bundeskriminalamt hat bei jedem Zugriff für Zwecke der Datenschutzkontrolle den Zeitpunkt, die Angaben, die die Feststellung der aufgerufenen Datensätze ermöglichen, sowie die für den Zugriff verantwortliche Dienststelle zu protokollieren. Die Auswertung der Protokolldaten ist nach dem Stand der Technik zu gewährleisten. Die protokollierten Daten dürfen nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage verwendet werden, es sei denn, es liegen Anhaltspunkte dafür vor, dass ohne ihre Verwendung die Verhinderung oder Verfolgung einer schwerwiegenden Straftat gegen Leib, Leben oder Freiheit einer Person aussichtslos oder wesentlich erschwert wäre. Die Protokolldaten sind nach zwölf Monaten zu löschen. Das Bundeskriminalamt trifft die technischen und organisatorischen Maßnahmen nach § 9 des Bundesdatenschutzgesetzes.

– Zollfahndungsdienstgesetz

§ 11 Zollfahndungsinformationssystem

(4) Werden beim Zollkriminalamt Daten abgerufen, hat es bei durchschnittlich jedem zehnten Abruf für Zwecke der Datenschutzkontrolle den Zeitpunkt, die Angaben, die die Feststellung der aufgerufenen Datensätze ermöglichen, sowie die für den Abruf verantwortliche Dienststelle zu protokollieren. Die protokollierten Daten dürfen nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage verwendet werden, es sei denn, es liegen Anhaltspunkte dafür vor, dass ohne ihre Verwendung die Verhinderung oder Verfolgung einer schwerwiegenden Straftat gegen Leib, Leben oder Freiheit einer Person aussichtslos oder wesentlich erschwert wäre. Die Protokolldaten sind nach zwölf Monaten zu löschen. Das Zollkriminalamt trifft die technischen und organisatorischen Maßnahmen nach § 9 des Bundesdatenschutzgesetzes.

– Bundesdatenschutzgesetz

Anlage zu § 9 Satz 1 BDSG

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind, …

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle), …

§ 10 Einrichtung automatisierter Abrufverfahren

(2) Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen:

1. Anlass und Zweck des Abrufverfahrens,
2. Dritte, an die übermittelt wird,
3. Art der zu übermittelnden Daten,
4. nach § 9 erforderliche technische und organisatorische Maßnahmen.

Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden getroffen werden.

4.3.2.2 Speicherung Strafunmündiger in INPOL

In einigen Verbunddateien des polizeilichen Informationssystems INPOL sollen künftig auch personenbezogene Daten von Strafunmündigen gespeichert werden. Dies begegnet datenschutzrechtlichen Bedenken.

In den Verbunddateien „Kriminalaktennachweis – KAN“ und „Analyse-System zur Verknüpfung von Gewaltverbrechen – ViCLAS“ des polizeilichen Informationssystems INPOL sollen künftig auch personenbezogene Daten von Strafunmündigen, d. h. von Kindern unter 14 Jahren, als sog. sonstige Personen gemäß § 8 Absatz 5 BKA-Gesetz gespeichert werden (s. Kasten zu Nr. 4.3.2.2).

Das BKA hält die Speicherung Strafunmündiger dann für erforderlich, wenn von ihnen schwere Gewalttaten verübt werden und die dabei gezeigte kriminelle Energie die Annahme rechtfertigt, dass sie auch bei Eintritt der Strafmündigkeit Straftaten von erheblicher Bedeutung begehen werden.

Im Rahmen des Anhörungsverfahrens zu den Errichtungsanordnungen habe ich Zweifel an der Zulässigkeit der Speicherung geäußert. Strafrechtlich resultiert aus der Strafunmündigkeit ein Schuldausschließungsgrund, der wiederum zu einem Prozesshindernis führt, das die Strafverfolgungsbehörden zur Verfahrenseinstellung zwingt bzw. gänzlich daran hindert, Ermittlungsmaßnahmen durchzuführen. Auf der anderen Seite führt die Strafunmündigkeit einer Person nicht zu einer Einschränkung der Gefahrenabwehrbefugnis nach dem Polizeirecht. Gefahren können in gleicher Weise von strafmündigen wie von strafunmündigen Personen verursacht werden, so dass Gefahrenabwehrmaßnahmen auch gegen Letztere zulässig sind. Die Speicherung personenbezogener Daten in INPOL gemäß § 8 BKA-Gesetz dient jedoch nicht der Abwehr unmittelbar bevorstehender Gefahren. Die Daten sollen vielmehr im Vorfeld einer Gefahr zur Straftatenverhütung und zur Vorsorge für die Verfolgung künftiger Straftaten vorgehalten werden. Vor diesem Hintergrund ist fraglich, ob hierfür Daten von Kindern, denen die Einsichtsfähigkeit für die von ihnen begangenen Handlungen fehlt und die sich noch im Anfang ihrer geistigen und seelischen Entwicklung befinden, geeignet sind. Dabei ist zu berücksichtigen, dass zum Zeitpunkt der Speicherung nicht absehbar ist, wie sich die kindliche Entwicklung fortsetzen wird.

Wegen dieser Unsicherheit in der Prognosestellung besteht die Gefahr, dass „Jugendsünden“ über einen längeren Zeitraum in Polizeidaten als „kriminelle Historie“ abgebildet werden. Diese Gefahr hat offenbar an anderer Stelle auch der Gesetzgeber gesehen. Gemäß § 11 Absatz 1 Satz 2 BVerfSchG ist es dem Bundesamt für Verfassungsschutz, welches ebenfalls im Vorfeld konkreter Gefahrenlagen tätig wird und zu diesem Zweck personenbezogene Daten erheben und verarbeiten darf, untersagt, Daten von Minderjährigen vor Vollendung des 16. Lebensjahres in Dateien zu speichern.

Schließlich stellt § 8 Absatz 5 BKA-Gesetz keine normenklare Regelung für die Speicherung personenbezogener Daten Strafunmündiger dar. Nach der Gesetzesbegründung bezieht sich die Regelung auf strafmündige Personen, bei denen bisher ein konkreter Tatverdacht nicht vorliegt, bei denen aber aufgrund tatsächlicher Erkenntnisse eine spätere Straftatenbegehung prognostiziert werden kann. Strafunmündige unter diese Norm zu subsumieren, nur weil sie wegen der strafprozessualen Beschränkung weder als „Beschuldigte“ noch als „Verdächtige“ erfasst werden können, ist vom gesetzgeberischen Willen nicht gedeckt.

Ich bedaure, dass das BMI meinen Bedenken nicht gefolgt ist. Nach Abschluss des Beteiligungsverfahrens mit den Ländern sind die geänderten Errichtungsanordnungen für die genannten Dateien vom BMI erlassen worden.

Kasten zu Nr. 4.3.2.2

§ 8 Absatz 5 BKA-Gesetz

(5) Personenbezogene Daten sonstiger Personen kann das Bundeskriminalamt in Dateien speichern, verändern und nutzen, soweit dies erforderlich ist, weil bestimmte Tatsachen die Annahme rechtfertigen, dass die betroffenen Straftaten von erheblicher Bedeutung begehen werden.

4.3.2.3 Noch immer keine Rechtsverordnung gemäß § 7 Absatz 6 BKAG

Mit der Rechtsverordnung gemäß § 7 Absatz 6 BKAG hat das BMI das Nähere über die Art der Daten, die in INPOL gespeichert werden dürfen, festzulegen.

Mit Urteil vom 16. Dezember 2008 (11 LC 228/08) hat das niedersächsische Oberverwaltungsgericht das Urteil des Verwaltungsgerichts Hannover vom 22. Mai 2008 (10 A 2412/07) bestätigt, dass die Führung der INPOL-Verbunddatei „Gewalttäter Sport“ durch das BKA nur dann rechtmäßig ist, wenn das BMI durch Rechtsverordnung gemäß § 7 Absatz 6 BKAG das Nähere über die Art der Daten bestimmt, die in dieser Datei gespeichert werden dürfen. Das Urteil ist nicht nur für die Rechtmäßigkeit der Hooligan-Datei bedeutsam, sondern kann Auswirkungen auf alle im Rahmen von INPOL geführten Verbunddateien haben.

Im Rahmen der Anhörungsverfahren zu Errichtungsanordnungen für Verbunddateien des polizeilichen Informationssystems INPOL habe ich immer wieder das Fehlen der entsprechenden Rechtsverordnung moniert. Die Auffassung des BMI, wonach die Rechtsverordnung keine Zulässigkeitsvoraussetzung für die Datenverarbeitung in den Verbunddateien sei, sondern im Hinblick auf die übrigen Regelungen des BKA-Gesetzes nur deklaratorische Bedeutung habe, wird weder durch den Wortlaut der einschlägigen Regelungen noch durch die Gesetzesmaterialien zum BKA-Gesetz gestützt.

Eine nähere Bestimmung der Art der Daten, die in Verbunddateien verarbeitet werden dürfen, erfolgt durch das

BKA-Gesetz nicht hinreichend. Eine Konkretisierung der Datenkategorien und des Datenumfangs in Verbunddateien wird zwar üblicherweise in den nach § 34 BKAG zu erlassenen Dateierrichtungsanordnungen vorgenommen. Bei diesen Errichtungsanordnungen handelt es sich jedoch nicht um Gesetze im materiellen Sinne, sondern nur um interne Verwaltungsvorschriften. Während die Rechtsverordnung gemäß § 7 Absatz 6 BKAG der Zustimmung des Bundesrates und damit eines Verfassungsorganes des Bundes bedarf, unterliegen Errichtungsanordnungen von Verbunddateien lediglich der Zustimmung der Landesinnenverwaltungen. Zudem sind sie häufig als vertraulich eingestuft und damit für die Öffentlichkeit nicht zugänglich. Schließlich bestimmt auch § 13 Absatz 1 BKAG, dass eine Datenübermittlung der Länder an die Zentralstelle BKA nach Maßgabe der Rechtsverordnung gemäß § 7 Absatz 6 BKAG zu erfolgen hat.

Sollte das BMI auch vor dem Hintergrund des Urteils des niedersächsischen OVG an seiner Position festhalten und auf den Erlass einer Rechtsverordnung verzichten, riskiert es damit, dass letztlich die Gesamtheit der in Verbunddateien stattfindenden polizeilichen Datenverarbeitung durch Gerichte für rechtswidrig erklärt wird.

4.4 Bundespolizei – Noch mehr Videoüberwachung

Nach einer Änderung des Bundespolizeigesetzes darf die Bundespolizei Daten aus Videoüberwachungsanlagen bis zu einem Monat speichern. Auch auf Flughäfen soll der Einsatz von Videotechnik zu Überwachungszwecken ausgeweitet werden.

Das Thema Videoüberwachung ist ein datenschutzrechtlicher Dauerbrenner. Seit geraumer Zeit wird die Überwachung insbesondere auch öffentlicher Räume sukzessive ausgedehnt. Bereits in früheren Tätigkeitsberichten (zuletzt 21. TB Nr. 4.2 f.) habe ich mich wiederholt mit diesem Thema beschäftigt.

Der durch das Dritte Gesetz zur Änderung des Bundespolizeigesetzes (BPolG) neu formulierte § 27 BPolG gestattet es nun, Daten aus der Videoüberwachung von Objekten, die dem Schutz der Bundespolizei unterliegen, wie z. B. Flughäfen oder Bahnhöfe, bis zu 30 Tage zu speichern. Bisher waren die Aufzeichnungen unverzüglich zu löschen. In der Praxis bedeutete dies, dass die Daten nach maximal 48 Stunden gelöscht wurden.

Damit fällt bei der anlasslos durchgeführten Videoüberwachung durch die Bundespolizei, die große Bereiche des öffentlichen Verkehrs (Bahnanlagen, Flughäfen u. a.) abdeckt, nun das datenschutzrechtliche Korrektiv einer kurz bemessenen Speicherfrist weg. Die Änderung des § 27 BPolG folgte nach Vorlage eines Berichtes des Unterausschusses Führung, Einsatz, Kriminalitätsbekämpfung (UA FEK) des Arbeitskreises II „Innere Sicherheit“ der Ständigen Konferenz der Innenminister und -senatoren der Länder (IMK), der sich – auch vor dem Hintergrund der strafverfolgungs- und polizeiermittlungsmäßigen Erfahrungen mit den Kölner „Kofferbombern“ – mit „Videoaufzeichnungen öffentlicher und nicht-öffentlicher Stellen“ beschäftigte und im Ergebnis eine Ausdehnung der zulässigen Speicherdauer auf „mindestens zehn Tage“ empfohlen hatte. Ich habe daher weiterhin erhebliche Vorbehalte gegenüber der nun pauschal festgelegten Speicherungshöchstdauer von einem Monat.

Bereits vor der Gesetzesänderung hatte ich stets für ein differenziertes Vorgehen plädiert, orientiert insbesondere am Gefährdungsgrad der überwachten Örtlichkeiten. Leider wurde diese Anregung bei der in aller Eile, ohne angemessene parlamentarische Beratung, beschlossenen Gesetzesänderung nicht aufgegriffen.

Allerdings begrüße ich es, dass die Bundespolizei meine Anregungen insoweit aufgegriffen hat, als nach den Mustererrichtungsanordnungen für die dateimäßige Verarbeitung von Daten aus der Videoüberwachung von Bahnanlagen oder Flughäfen grundsätzlich eine nur zehntägige Speicherfrist erfolgen soll, die nur bei besonderen Anlässen auf 30 Tage ausgedehnt werden darf.

Der Einsatz von Videokameras durch die Bundespolizei soll auch auf Flughäfen erweitert werden. Dabei soll die Bundespolizei – ähnlich wie bei Anlagen der Deutschen Bahn AG (vgl. 21. TB Nr. 4.2.2) – auf die Überwachungskameras der privaten Betreibergesellschaft zurückgreifen, wofür eine besondere Nutzungsvereinbarung nötig ist.

Ich begrüße auch die Zusicherung des BMI, dass neu zu beschaffende Videokameras die Anforderungen des von meiner Dienststelle und dem Bundesamt für Sicherheit in der Informationstechnik entwickelten datenschutzrechtlichen Profils „Common Criteria Protection Profile Software zur Verarbeitung von personenbezogenen Bilddaten“ erfüllen sollen (s. auch Nr. 8.1).

4.5 Ermittlungsverfahren der Generalbundesanwaltschaft

Bei Ermittlungsverfahren der Generalbundesanwaltschaft stellte sich die Frage der Rechtmäßigkeit des Vollzugs von Postbeschlagnahmen sowie der Durchführung der Telekommunikationsüberwachung.

Im Zusammenhang mit einer Postbeschlagnahme war zu klären, inwieweit Polizisten als Hilfsbeamte der Staatsanwaltschaft mit dem Vollzug des Beschlagnahmebeschlusses beauftragt werden dürfen. Dabei hatte das Postunternehmen die der Postbeschlagnahmeanordnung unterliegenden Postsendungen in seinen Räumen ausgesondert und Polizeibeamten zur weiteren äußerlichen Inaugenscheinnahme vorgelegt. Ein dabei beschlagnahmter Brief wurde in Anwesenheit eines Staatsanwaltes von den Polizeibeamten geöffnet.

Nach Prüfung der Sach- und Rechtslage habe ich in der Angelegenheit keinen datenschutzrechtlichen Verstoß festgestellt und mich der Auffassung der Generalbundesanwaltschaft angeschlossen, dass diese Maßnahme in Einklang mit den §§ 99, 100 StPO stand. Die Beschlagnahmeanordnung betraf ausschließlich solche Postsen-

dungen, die nach ihrem äußeren Erscheinungsbild durch das Fehlen eines Absenders gekennzeichnet waren. Dieses Aussonderungskriterium schloss aus, dass bei der Inaugenscheinnahme durch Polizeibeamte der briefliche Kommunikationsvorgang zwischen identifizierbaren Personen bewusst zur Kenntnis genommen wurde. Das kurzzeitige Betrachten eines Briefumschlags zur Feststellung des Vorhandenseins einer Absenderangabe stellt keine staatliche Kenntnisnahme oder Erfassung eines Kommunikationsvorganges und damit keinen Eingriff in das durch Artikel 10 GG geschützte Brief- und Postgeheimnis dar. Auch die Art und Weise der Öffnung des beschlagnahmten Briefes entsprach dem Regelungsgehalt des § 100 Absatz 3 StPO.

Im Zusammenhang mit der Durchführung einer Telekommunikationsüberwachung von Anschlüssen einer Anwaltskanzlei habe ich kontrolliert, inwieweit das damit beauftragte BKA die einschlägigen gesetzlichen Regelungen sowie den zugrunde liegenden Beschluss des Ermittlungsrichters beim Bundesgerichtshof beachtet hatte. Von Interesse war vor allem, wie den schützenswerten Belangen von Mandanten des Anwaltsbüros bei erkennbar nicht verfahrensrelevanten Gesprächsinhalten vor dem Hintergrund der Vorgaben des richterlichen Beschlusses Rechnung getragen wurde.

Zwar habe ich mich davon überzeugen können, dass bei der Durchführung der Überwachung und Aufzeichnung der Telekommunikation durch das BKA der Grundsatz der Erforderlichkeit und Verhältnismäßigkeit beachtet wurde. Die vom BKA zum Schutz von nicht verfahrensrelevanten Mandantengesprächen veranlassten Maßnahmen entsprachen hingegen nicht den Vorgaben des Ermittlungsrichters in der Begründung des Überwachungsbeschlusses. Während dort ausgeführt war, dass auch Uhrzeit und Dauer der Verbindung nicht einsehbar sein sollen, waren diese Angaben beim BKA für die Sachbearbeiter jederzeit abrufbar. Lediglich Telefon- bzw. Faxnummern der Verbindungspartner waren unkenntlich gemacht.

Die Generalbundesanwaltschaft vertrat hierzu die Auffassung, dass damit dem Schutz von nicht verfahrensrelevanten Mandantengesprächen Genüge getan sei. Der maßgebliche Rahmen für die Durchführung richterlich angeordneter Ermittlungshandlungen ergebe sich allein aus dem Tenor des richterlichen Beschlusses, nicht jedoch aus seinen Gründen. Soweit dort erwähnt sei, dass Uhrzeit und Dauer eines mit einem Beweisverwertungsverbot belegten Telefongesprächs nicht einsehbar sein sollen, handele es sich lediglich um eine nicht verbindliche Durchführungsanweisung.

Ich vertrete hingegen die Auffassung, dass die richterliche Anordnung der Überwachung und Aufzeichnung der Telekommunikation im Rahmen eines Ermittlungsverfahrens, die gemäß § 100b Absatz 2 Satz 2 Nummer 3 StPO u. a. Art, Umfang und Dauer der Maßnahme anzugeben hat, für die beantragende Strafverfolgungsbehörde auch hinsichtlich ihrer Begründung bindend ist. Zwar schien in dem konkreten Fall der Schutz nicht verfahrensrelevanter Mandantengespräche dadurch erreicht zu sein, dass die Telefon- bzw. Faxnummer der Verbindungspartner nicht einsehbar war. Gleichwohl hatte die Generalbundesanwaltschaft bzw. das BKA die richterliche Anordnung nicht beachtet, auch Uhrzeit und Dauer dieser Gespräche unkenntlich zu machen.

Auf meinen Hinweis hin wurden im BKA auf Anordnung der Staatsanwaltschaft schließlich die Verbindungsdaten und Gesprächsinhalte sämtlicher mit einem Beweisverwertungsverbot belegten Verbindungen gelöscht.

4.6 Bundeszentralregister beim Bundesamt für Justiz

Durch Novellierung des Bundeszentralregistergesetzes (BZRG) soll die Erteilung eines „erweiterten Führungszeugnisses“ für Personen ermöglicht werden, die aufgrund beruflicher oder ehrenamtlicher Tätigkeit in einem besonderen Näheverhältnis zu Kindern und Jugendlichen stehen.

Das BMJ hat Ende 2008 den Referentenentwurf eines Fünften Gesetzes zur Änderung des BZRG vorgelegt, welcher das Ziel verfolgt, den Schutz von Kindern und Jugendlichen vor Straftaten zu verbessern, insbesondere dann, wenn diese Straftaten in der Ausübung beruflicher oder ehrenamtlicher Tätigkeiten mit Minderjährigen geschehen. Diese Zielsetzung unterstütze ich, ebenso wie den Ansatz des Gesetzentwurfes, das Ziel durch Einführung eines sog. erweiterten Führungszeugnisses nur für bestimmte Personengruppen, die aufgrund ihrer beruflichen oder ehrenamtlichen Tätigkeit in einem spezifischen Näheverhältnis zu Kindern und Jugendlichen stehen, zu erreichen. Mit dieser Problematik hatte sich bereits zu Beginn des Jahres 2008 der Bundesrat befasst. Auch die 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich im Frühjahr 2008 mit dieser Thematik beschäftigt. In meiner Stellungnahme zu dem Referentenentwurf habe ich allerdings Bedenken hinsichtlich des Umfangs der in ein erweitertes Führungszeugnis aufzunehmenden Verurteilungen und bezüglich der Normenklarheit der Regelung geäußert. Die Ressortberatungen waren bei Redaktionsschluss noch nicht abgeschlossen.

Das Bundeszentralregister, das seit dem 1. Januar 2007 nicht mehr beim Generalbundesanwalt, sondern bei dem neu gegründeten Bundesamt für Justiz geführt wird, enthält nicht nur Eintragungen zu strafrechtlichen Verurteilungen, sondern auch zu behördlichen und gerichtlichen Entscheidungen, z. B. sog. „Schuldunfähigkeitsvermerke“ infolge gerichtlicher Freisprüche wegen Schuldunfähigkeit. Somit umfasst das Bundeszentralregister personenbezogene Daten von äußerst sensiblem Charakter, die nur einem eng begrenzten Empfängerkreis bekannt gemacht werden dürfen. Um dies sicherzustellen, enthalten das BZRG und die einschlägigen Verwaltungsvorschriften eine Vielzahl verfahrenssichernder Regelungen.

Das BMJ hat die aus dem Jahre 1985 stammenden Verwaltungsvorschriften zum BZRG neu gefasst und aktualisiert. So ist nun im Regelfall die Anlieferung von Informationen auf elektronischem Wege in einem automatisierten Mitteilungs- und Auskunftsverfahren (AuMiAu) vorgesehen. Gegenüber dem BMJ hatte ich Vorbehalte hinsichtlich der im Entwurf der neuen Verwaltungsvorschrift enthaltenen Übermittlungsvariante geäußert, dringende Anfragen auch telefonisch oder per Telefax an das Bundesamt für Justiz richten zu können. Bei dieser Verfahrensweise kann das BMJ die Identität und Berechtigung der Antrag stellenden Person nicht angemessen prüfen, so dass sensible Daten aus dem Bundeszentralregister in falsche Hände gelangen könnten. Daher begrüße ich es, dass die am 1. Januar 2009 in Kraft getretene Verwaltungsvorschrift zum BZRG meine Bedenken berücksichtigt.

4.7 Nachrichtendienste

4.7.1 Bundesamt für Verfassungsschutz

Bei der Erteilung von Auskünften an die Betroffenen legt das Bundesamt für Verfassungsschutz (BfV) einen zu strengen Maßstab an und missachtet damit einen bereits im Jahre 1993 gefassten Beschluss des Deutschen Bundestages.

Im Berichtszeitraum haben mich mehrere Eingaben betroffener Bürger erreicht, die sich darüber beklagten, dass das BfV nur unzureichend Auskunft über dort gespeicherte Daten erteilt hat. Nach § 15 Absatz 1 BVerfSchG erteilt das BfV dem Betroffenen über die zu seiner Person gespeicherten Daten auf Antrag unentgeltlich Auskunft, soweit er hierzu auf einen konkreten Sachverhalt hinweist und ein besonderes Interesse an einer Auskunft darlegt. Die Auskunft des BfV beschränkte sich in vielen Fällen auf den vorgetragenen Sachverhalt. In den meisten dieser Fälle lagen zu den vorgetragenen Sachverhalten keine Datenspeicherungen vor. Eine weitergehende Auskunft zu sonstigen, von dem Betroffenen nicht angesprochenen Sachverhalten kommt aus Sicht des BfV auch nicht im Wege des Ermessens in Betracht, da ihr die Ausforschungsgefahr entgegenstehe.

Angesichts der herausragenden Bedeutung des Auskunftsrechts für die Wahrung des Grundrechts auf informationelle Selbstbestimmung halte ich diese Praxis für nicht hinnehmbar. Sie beruht aus meiner Sicht auf einer Fehlinterpretation des § 15 BVerfSchG und steht auch im Widerspruch zu dem Beschluss des Deutschen Bundestages vom 5. Februar 1993 (vgl. Bundestagsdrucksache 12/4094), in dem der Bundesregierung empfohlen wird, den Umfang der Auskunft nicht zwingend auf Speicherungen zu dem vorgetragenen Sachverhalt zu beschränken. Jedenfalls rechtfertigt die vom BfV herangezogene pauschale Begründung einer latent vorhandenen abstrakten Ausforschungsgefahr sein Auskunftsverhalten nicht.

Ich habe daher das BfV aufgefordert, seine Auskunftspraxis verfassungskonform auszugestalten. Eine Antwort hierzu lag bei Redaktionsschluss nicht vor.

4.7.2 Militärischer Abschirmdienst

Im Rahmen meiner Anhörung zu einer Dateianordnung hat das BMVg sich geweigert, mir eine zwischen dem MAD und dem BND getroffene Vereinbarung über die Zusammenarbeit bei besonderen Auslandsverwendungen der Bundeswehr zu überlassen. Dies habe ich als schwerwiegenden Verstoß gegen die in § 24 Absatz 4 BDSG normierte Mitwirkungspflicht förmlich beanstandet. Eine andere Regelung in dieser Dateianordnung ist mit dem Grundrecht auf informationelle Selbstbestimmung nicht vereinbar.

Nach § 8 MADG hat der MAD für jede automatisierte Datei mit personenbezogenen Daten eine Dateianordnung nach § 14 BVerfSchG zu erstellen, die der Zustimmung des BMVg bedarf und vor deren Erlass ich anzuhören bin. So hat mir das BMVg den Entwurf einer Anordnung für eine Datei zur Anhörung zugeleitet, die als Auswerte- und Organisationsmittel zur Aufgabenerfüllung des MAD während einer besonderen Auslandsverwendung der Bundeswehr gemäß § 14 Absatz 1 MADG genutzt wird. Bei den Auslandsverwendungen der Bundeswehr arbeiten MAD und BND eng zusammen. Die Einzelheiten dieser Zusammenarbeit sind für jeden Einsatz in einer Vereinbarung zwischen dem MAD und dem BND zu regeln, die der Zustimmung des Chefs des Bundeskanzleramtes und des BMVg bedarf und über die das Parlamentarische Kontrollgremium zu unterrichten ist (§ 14 Absatz 6 Satz 4 MADG). Im Rahmen des Anhörungsverfahrens habe ich das BMVg um Übersendung der für diesen Auslandseinsatz geschlossenen Vereinbarung gebeten. Dies hat das BMVg mit der Begründung abgelehnt, ein Zusammenhang mit meiner „informatorischen Beteiligung“ am ministeriellen Genehmigungsverfahren der Dateianordnung und der für die Auslandseinsätze der Bundeswehr mit dem BND abgeschlossenen Vereinbarung sei nicht erkennbar. Im Übrigen enthalte die Vereinbarung keine Regelung zum Umgang mit personenbezogenen Daten.

Kasten zu Nr. 4.7.2

§ 6 Absatz 2 MADG

(2) In Dateien oder zu ihrer Person geführten Akten gespeicherte Daten über Minderjährige sind nach zwei Jahren auf die Erforderlichkeit der Speicherung zu überprüfen und spätestens nach fünf Jahren zu löschen, es sei denn, dass nach Eintritt der Volljährigkeit weitere Erkenntnisse nach § 1 Absatz 1 oder § 2 angefallen sind. Dies gilt nicht, wenn der Betroffene nach § 1 Absatz 3 überprüft wird. Die Speicherung personenbezogener Daten über Minderjährige vor Vollendung des 16. Le-bensjahres in zu ihrer Person geführten Akten und Dateien ist unzulässig.

Abgesehen davon, dass es sich bei meiner Anhörung nicht um eine informatorische Beteiligung, sondern um eine nach § 8 MADG i. V. m. § 14 Absatz 1 Satz 2 BVerfSchG institutionalisierte formale Anhörung handelt, verstößt die Weigerung des BMVg gegen § 24 Absatz 4 BDSG. Nach dieser Vorschrift haben die öffentlichen Stellen des Bundes mich bei meiner Aufgabenerfüllung zu unterstützen und mir dabei Auskunft zu meinen Fragen sowie Einsicht in alle Unterlagen zu gewähren. Zu diesen Unterlagen gehört auch die hier in Rede stehende Vereinbarung zwischen dem MAD und dem BND. Da mir das BMVg auch nach wiederholter Bitte die Vereinbarung nicht zugänglich gemacht hat, habe ich dies als schwerwiegenden Verstoß gegen die Mitwirkungspflicht gemäß § 25 Absatz 1 BDSG förmlich beanstandet.

In seiner Erwiderung vertritt das BMVg die Auffassung, ein Verstoß gegen die Mitwirkungspflicht liege nicht vor. Gleichwohl hat es mir ohne Anerkennung einer rechtlichen Verpflichtung eine Mustervereinbarung nach § 14 Absatz 6 MADG zur Zusammenarbeit von MAD und BND bei besonderen Auslandsverwendungen der Bundeswehr übersandt. Dies ist jedoch nicht ausreichend, da die datenschutzrechtlichen Regelungen von mir nur in Bezug auf die konkret für den jeweiligen Auslandseinsatz getroffene Vereinbarung bewertet werden können. Im Übrigen hat sich gezeigt, dass bereits die übersandte Mustervereinbarung entgegen der Behauptung des BMVg Regelungen zum Umgang mit personenbezogenen Daten enthält bzw. darauf ausgerichtet ist. Das BMVg beharrt dennoch auf seiner Weigerung.

Bei einem anderen Punkt dieser Dateianordnung habe ich mit Blick auf das MADG verfassungsrechtliche Zweifel. Die Dateianordnung sieht vor, dass eine Berichtigung, Löschung oder Sperrung der in der Datei gespeicherten Daten nur dann erfolgt, wenn die Daten im Inland erhoben worden sind oder sich auf deutsche Staatsangehörige beziehen. Dies würde im Umkehrschluss bedeuten, dass für im Ausland über Ausländer erhobene Daten keine sich aus § 7 MADG (Berichtigung, Löschung und Sperrung von Daten) ergebenden datenschutzrechtlichen Pflichten ergeben. Da aber unzweifelhaft ist, dass auch die Erhebung, Verarbeitung und Nutzung solcher Daten – unbeschadet des Wortlauts des § 14 Absatz 4 Satz 1 MADG – einen Eingriff in das Persönlichkeitsrecht darstellt, ist ein differenzierter Grundrechtsschutz je nach dem Ort der Datenerhebung oder der fremden Staatsangehörigkeit nicht vertretbar. Die Regelung des § 14 Absatz 4 Satz 1 MADG würde bei dieser Auslegung einen grundrechts- und kontrollfreien Raum schaffen. Das BMVg wendet dagegen ein, dass aus Gründen schutzeffektiver Einsatzabschirmung eine weitergehende Möglichkeit zur Erhebung und Verarbeitung von Daten – z. B. auch zu Minderjährigen – bestehen müsse und nicht durch eine über den Wortlaut des § 14 Absatz 4 Satz 1 MADG hinausgehende Anwendung des § 6 Absatz 2 MADG (Verbot der Speicherung von Daten Minderjähriger – vgl. Kasten zu Nr. 4.7.2) ausgeschlossen werden dürfe. Diese Argumentation, die zwar mit Blick auf die Gefährdungslage bei Auslandseinsätzen der Bundeswehr verständlich sein mag, lässt jedoch die verfassungsrechtlichen Schranken außer Betracht. Ich habe daher eine klarstellende Änderung des § 14 Absatz 4 Satz 1 MADG angeregt und das BMVg darüber hinaus gebeten, die vorliegende Dateianordnung anzupassen.

4.7.3 Bundesnachrichtendienst

4.7.3.1 Überwachung von Journalisten

Eine über mehrere Jahre andauernde Überwachung eines Journalisten durch den BND war rechtswidrig.

Im 21. TB (Nr. 5.7.2) hatte ich über die Eingabe eines Journalisten berichtet, der sich über eine mehrere Jahre andauernde Beobachtung durch den BND beklagt hatte. Inzwischen kann ich über das Ergebnis meiner diesbezüglichen Prüfungen berichten. Die Überwachung dieses Journalisten war rechtswidrig – anders als in den beiden anderen Fällen, über die ich ebenfalls berichtet hatte. Der Journalist war über mehrere Jahre aus Gründen, auf die ich aus Geheimhaltungserwägungen nicht näher eingehen kann, gezielt vom BND unter Einsatz nachrichtendienstlicher Mittel beobachtet worden. Eine solche verdeckte, also heimliche Informationsbeschaffung ist dem BND nach § 3 BNDG nur erlaubt, wenn Tatsachen die Annahme rechtfertigen, dass dies zur Erfüllung seiner Aufgaben erforderlich ist. Diese vom Gesetzgeber geforderte hohe Eingriffsschwelle, nämlich das Vorliegen von Tatsachen, war nach meinen Feststellungen im vorliegenden Falle nicht erreicht. Der BND hat nach meiner Kontrolle die zu Unrecht erhobenen und in Akten erfassten Daten des Petenten gesperrt und zugesagt, künftig die Vorgaben des § 3 BNDG einzuhalten und hierbei den in Artikel 5 GG gewährten Schutzbereich der Pressefreiheit uneingeschränkt zu gewährleisten.

4.7.3.2 Auskunftsverpflichtung des BND auch bezüglich Akten

Trotz des nicht eindeutigen Gesetzeswortlauts ist der BND auch zur Auskunftserteilung aus Akten verpflichtet. Das Bundesverwaltungsgericht hat meine Auffassung mit der Entscheidung vom 28. November 2007 bestätigt.

Ein Petent hatte sich im Jahre 2006 an mich gewandt, weil der BND ihm auf sein Auskunftsersuchen hin lediglich Auskunft zur Speicherung personenbezogener Daten in Dateien, nicht jedoch zu solchen in Akten erteilt hatte. Ich hatte hierüber im 21. TB (Nr. 5.7.7) berichtet. Der BND hatte seine Entscheidung auf den Wortlaut des § 7 BNDG gestützt, wonach Auskunft nur über die nach § 4 BNDG – also in Dateien – gespeicherten Daten zu erteilen sei. Da diese Auslegung des BND, die vom Bundeskanzleramt gestützt wird, nicht im Einklang mit der verfassungsgerichtlichen Rechtsprechung steht, hatte ich den BND gebeten, die Vorschrift des § 7 BNDG verfassungskonform auszulegen und – ebenso wie beim BfV und beim MAD – Auskunft auch aus Akten zu erteilen.

Diesem Petitum ist der BND nicht gefolgt. In dem Verfahren beim Bundesverwaltungsgericht hat der Petent schließlich Recht bekommen. In der Entscheidung vom 28. November 2007 – 6 A 2.07 – hat das Gericht meine Rechtsauffassung bestätigt und den BND verpflichtet, dem Kläger grundsätzlich auch die von ihm begehrte Auskunft aus Akten zu erteilen.

Im Lichte dieser Entscheidung sollte § 7 BNDG bei der demnächst zu erwartenden Novellierung eindeutig geändert werden.

4.8 Sicherheitsüberprüfung

4.8.1 Notwendigkeit zur Änderung des SÜG

Mit dem Ausscheiden eines Betroffenen aus einer sicherheitsempfindlichen Tätigkeit muss die Nachberichtspflicht enden. § 18 Absatz 5 SÜG, wonach die mitwirkende Behörde erst fünf Jahre nach dem Ausscheiden aus der sicherheitsempfindlichen Tätigkeit zu unterrichten ist, verhindert dies jedoch.

Nach § 16 Absatz 1 SÜG haben sich die zuständige Stelle und die mitwirkende Behörde nach Abschluss der Sicherheitsüberprüfung über bekannt gewordene Erkenntnisse zu unterrichten. Die Nachberichtspflicht soll gewährleisten, dass nachträglich entstehende Sicherheitsrisiken bereits im Ansatz erkannt werden. Mit dem Ausscheiden aus der sicherheitsempfindlichen Tätigkeit muss diese Nachberichtspflicht jedoch auslaufen. Erkenntnisse, die nach dem Ausscheiden eines Betroffenen aus der sicherheitsempfindlichen Tätigkeit bekannt werden, dürfen nicht mehr zwischen der zuständigen Stelle und der mitwirkenden Behörde ausgetauscht werden. Die Unterrichtung ist für die Gewährleistung des Verschlusssachenschutzes nicht mehr erforderlich, da der Betroffene nach seinem Ausscheiden aus der sicherheitsempfindlichen Tätigkeit kein Geheimnisträger mehr ist.

Allerdings verhindert das SÜG, dass die Berichtspflicht mit dem Ausscheiden aus der sicherheitsempfindlichen Tätigkeit endet. Die zuständige Stelle ist nach § 18 Absatz 5 Satz 2 SÜG verpflichtet, die mitwirkende Behörde erst nach Ablauf von fünf Jahren nach dem Ausscheiden aus der sicherheitsempfindlichen Tätigkeit hierüber zu unterrichten. Die mitwirkende Behörde wird daher, weil ihr das Ausscheiden des Betroffenen nicht bekannt ist, während dieses Fünfjahreszeitraums ihrer Nachberichtspflicht weiterhin nachkommen. Dies halte ich aus Gründen des Persönlichkeitsschutzes des Betroffenen für unzulässig. Ich habe daher das BMI gebeten, das Verfahren gemäß § 18 Absatz 5 SÜG dahingehend zu ändern, dass das Ausscheiden aus der sicherheitsempfindlichen Tätigkeit der mitwirkenden Behörde unverzüglich anzuzeigen ist. Bis zu einer gesetzlichen Änderung – so habe ich weiter angeregt – sollte die geänderte Verfahrensweise im Wege eines Rundschreibens bekannt gegeben werden.

Ich bedauere es, dass das BMI meine Anregung nicht aufgegriffen hat. Die Nachberichtspflicht sei zwingend erforderlich, um im Verjährungszeitraum bei der mitwirkenden Behörde nachträglich anfallende sicherheitserhebliche Erkenntnisse durch die zuständige Stelle daraufhin prüfen zu können, ob auf Grund dieser Erkenntnisse ein Geheimnisverrat begangen worden sein könnte und daher strafrechtliche Ermittlungen veranlasst werden müssten. Der Grund für die fünfjährige Frist liege in der Verjährungsfrist für den Tatbestand des Geheimnisverrats nach § 353b StGB.

Demgegenüber halte ich an meiner Auffassung fest. Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Rahmen der Sicherheitsüberprüfung unterliegen einer strikten Zweckbindung, nämlich der Gewährleistung des Verschlusssachenschutzes bzw. des vorbeugenden personellen Sabotageschutzes. Dieser Zweck endet mit dem Ausscheiden des Betroffenen aus der Tätigkeit, für die eine Sicherheitsüberprüfung durchgeführt wurde. Die vom BMI angeführte Begründung, die Nachberichtspflicht müsse zum Zwecke der Prüfung auf eine mögliche strafrechtliche Relevanz bestehen bleiben, verstößt gegen den in § 21 Absatz 1 SÜG verankerten Zweckbindungsgrundsatz. Danach dürfen personenbezogene Daten nur für die mit der Sicherheitsüberprüfung verfolgten Zwecke zum Zwecke der Verfolgung von Straftaten von erheblicher Bedeutung sowie für Zwecke parlamentarischer Untersuchungsausschüsse genutzt und übermittelt werden.

Ich werde daher weiterhin auf eine Änderung des § 18 Absatz 5 SÜG drängen.

4.8.2 Kontrollen

Bei meinen Kontrollen von Sicherheitsüberprüfungen gemäß SÜG habe ich wie bereits in der Vergangenheit Fehler festgestellt.

Im Berichtszeitraum habe ich Kontrollen der Sicherheitsüberprüfungsverfahren im öffentlichen und im nicht-öffentlichen Bereich durchgeführt. Dabei habe ich erstmals auch Sicherheitsüberprüfungen im Rahmen des durch das Terrorismusbekämpfungsgesetz 2002 eingeführten vorbeugenden personellen Sabotageschutzes nach § 1 Absatz 4 SÜG kontrolliert (vgl. 19. TB Nr. 20.1).

Erfreulich war, dass das kontrollierte Unternehmen bei der Festlegung von sicherheitsempfindlichen Stellen behutsam vorgegangen ist und so der Kreis der Betroffenen klein blieb. Bei der Kontrolle von Sicherheitsakten musste ich dagegen feststellen, dass meine Appelle zur Änderung der Praxis offensichtlich wenig gefruchtet haben.

So habe ich mehrfach festgestellt, dass Löschungs- bzw. Vernichtungsfristen nicht eingehalten wurden, weil der Geheimschutzbeauftragte oder der Sicherheitsbevollmächtigte das Ausscheiden eines Mitarbeiters aus der si-

cherheitsempfindlichen Tätigkeit nicht rechtzeitig erfahren hatte oder das tatsächliche Datum des Ausscheidens nicht eindeutig festgestellt worden war (vgl. 21. TB Nr. 5.8.3.2). Ich begrüße es, dass das BMI nunmehr alle obersten Bundesbehörden darauf hingewiesen hat, dass beim Ausscheiden von Mitarbeitern aus der sicherheitsempfindlichen Tätigkeit der Geheimschutzbeauftragte unverzüglich zu informieren ist.

Ein weiteres Problem hat sich erneut beim Zugriff des Geheimschutzbeauftragten auf das jeweilige elektronische Personalverwaltungssystem gezeigt (vgl. 21. TB Nr. 5.8.3.2). Bei dem von mir kontrollierten Bundespolizeipräsidium hatte der Geheimschutzbeauftragte Zugriff auch auf bestimmte Daten zu Personen, die nicht der Geheimschutzbetreuung unterlagen. Nach meiner Intervention wurde der lesende Zugriff des Geheimschutzbeauftragten auf das System wieder unterbunden.

Da ich befürchte, dass eine derartige Praxis auch bei anderen Behörden und Unternehmen besteht, bedarf es einer eindeutigen generellen Regelung, ob und in welchem Umfang dem Geheimschutzbeauftragten bzw. dem Sicherheitsbevollmächtigten Zugriff auf das Personalverwaltungssystem zu gestatten ist.

Bei meiner Kontrolle eines Bundespolizeipräsidiums im Jahre 2005 hatte ich bemängelt, dass dort Personalmitteilungen, Veränderungsanzeigen und dergleichen durch die Personalverwaltung sowohl dem Geheimschutzbeauftragten als auch anderen Stellen (z. B. Personalrat, Vertrauensperson der Schwerbehinderten) oft in Form von Sammelverfügungen zur Kenntnis gebracht wurden (vgl. 21. TB Nr. 5.8.3.1). Leider musste ich bei der Kontrolle eines anderen Präsidiums im Jahre 2007 den gleichen Mangel feststellen. Von einer Beanstandung nach § 25 BDSG habe ich abgesehen, nachdem das BMI alle Dienststellen der Bundespolizei verpflichtet hatte, den Geheimschutzbeauftragten ausnahmslos nur solche Informationen zugänglich zu machen, die im Einzelfall eine sicherheitsüberprüfte Person betreffen und die für Belange des Geheimschutzes relevant sind. Des Weiteren hat das BMI die Dienststellen verpflichtet, bei Sammelverfügungen die Namen Dritter vor Weitergabe an den Geheimschutzbeauftragten unkenntlich zu machen.

Bei zwei von mir kontrollierten Unternehmen teilten sich die Sicherheitsbevollmächtigten das Büro – wenn auch zum Teil nur zeitweilig – mit anderen Mitarbeitern, die nicht mit Aufgaben der Sicherheitsüberprüfung betraut sind. Dies halte ich im Hinblick auf die strengen Auflagen zur Aufbewahrung von Sicherheitsunterlagen (§ 30 i. V. m. § 19 Absatz 1 SÜG) für bedenklich. Bei der Mitbenutzung des Büros des Sicherheitsbevollmächtigten durch eine weitere Person ist – auch bei aller Sorgfalt – nicht auszuschließen, dass diese Person Einblick in die Sicherheitsakten und den vom Sicherheitsbevollmächtigten benutzten PC nehmen kann. Zudem kann diese Person durch das Mithören von im Einzelfall unvermeidbaren Telefonaten und Gesprächen Kenntnis von vertraulichen Inhalten erlangen. Ich habe daher das BMWi gebeten, bei den kontrollierten Unternehmen für entsprechende organisatorische Änderungen zu sorgen.

Ein grundsätzliches Problem hat sich bei der Kontrolle eines Unternehmens gezeigt, das selbst keine Verschlusssachen (VS) verwaltet. Dennoch waren alle Geschäftsführer einer Sicherheitsüberprüfung unterzogen worden. Das BMWi rechtfertigt dies damit, dass die Überprüfung der Geschäftsleitung nach Nr. 4.1.3 Absatz 1 des Geheimschutzhandbuches als Teil der Zuverlässigkeitsüberprüfung eines Unternehmens ausdrücklich vorgesehen sei. Nach dieser Vorschrift richtet sich die Überprüfung der Geschäftsleitung nach der höchsten VS-Einstufung der VS-Aufträge des Unternehmens. Da das kontrollierte Unternehmen keine VS verwaltet, halte ich es für fragwürdig, wenn Geschäftsführer von Unternehmen ohne materiellen Geheimschutz einer Sicherheitsüberprüfung unterzogen werden. Da sie keinen Zugang zu VS haben und auch der vorbeugende personelle Sabotageschutz ausscheidet, sehe ich hierzu keine Notwendigkeit. Auch der – höchst theoretische – Fall, dass ein Mitglied der Geschäftsleitung im Einzelfall Zugang zu einem betreuten Unternehmen mit materiellem Geheimschutz bekommt, rechtfertigt nicht die Durchführung einer Sicherheitsüberprüfung, die mit erheblichen Eingriffen in das Persönlichkeitsrecht verbunden ist. Sollte die Sicherheitsüberprüfung der Geschäftsführer mehr den Charakter einer Zuverlässigkeitsüberprüfung haben, sähe ich hierfür keine gesetzliche Grundlage (vgl. hierzu Nr. 4.8.3.2).

Ich habe das BMWi zu einer weiteren Stellungnahme aufgefordert, die aber bei Redaktionsschluss noch nicht vorlag.

4.8.3 Sicherheitsüberprüfungen außerhalb des SÜG

Bei Sicherheits- bzw. Zuverlässigkeitsüberprüfungen gibt es einen zunehmenden Wildwuchs. Teilweise stehen Zuverlässigkeitsüberprüfungen aber auch mit dem geltenden Recht nicht in Einklang.

Zahlreiche Gesetze und Verordnungen enthalten Regelungen zur Überprüfung der Zuverlässigkeit von Personen. Die wichtigsten Regelungen mit detaillierten Verfahrensvorschriften sind das Sicherheitsüberprüfungsgesetz, das Luftsicherheitsgesetz (LuftSiG) und das Atomgesetz (AtG). Obwohl die Zielsetzungen dieser Vorschriften in weiten Teilen übereinstimmen, weichen die materiellrechtlichen Regelungen und die Verfahrensvorschriften zum Teil erheblich voneinander ab. Nachdem im Jahre 2002 durch das Terrorismusbekämpfungsgesetz der vorbeugende personelle Sabotageschutz in das SÜG aufgenommen wurde (vgl. 19. TB Nr. 20.1), stellt sich die Frage, ob weiterhin eigenständige Regelungen zur Zuverlässigkeitsüberprüfung von Personen außerhalb des SÜG sinnvoll und erforderlich sind, da es sich bei den Überprüfungen nach dem

LuftSiG und dem AtG um Varianten des vorbeugenden personellen Sabotageschutzes handelt.

Neben diesen gesetzlich geregelten Überprüfungen werden Personenüberprüfungen auch bei Großveranstaltungen, z. B. anlässlich der Fußball-Weltmeisterschaft, und vielfach von Arbeitgebern durchgeführt, ohne dass es hierfür – trotz erheblicher Eingriffe in das Persönlichkeitsrecht – eine gesetzliche Grundlage gibt. Es ist daher an der Zeit, die Vorschriften über Zuverlässigkeitsüberprüfungen zusammenzuführen und eine für alle Überprüfungsarten geltende einheitliche gesetzliche Grundlage zu schaffen, in die auch die bisher ohne Rechtsgrundlage durchgeführten Überprüfungen einzubeziehen sind.

4.8.3.1 Atomgesetz

Die vorgesehenen Gesetzesänderungen für atomrechtliche Zuverlässigkeitsüberprüfungen sind datenschutzrechtlich unbefriedigend.

Im Berichtszeitraum hat mich das BMU bei dem Entwurf zur Änderung des § 12b AtG und der atomrechtlichen Zuverlässigkeitsüberprüfungsverordnung beteiligt. Mit der Gesetzesinitiative reagiert das BMU auf die veränderte Beurteilung der Sicherheitslage hinsichtlich der Gefährdung von kerntechnischen Anlagen und Nukleartransporten durch terroristische Anschläge. Der Entwurf sieht insbesondere eine Erweiterung des Katalogs der bei Zuverlässigkeitsüberprüfungen zulässigen Anfragen bei anderen Stellen und die Einführung von Nachberichtspflichten vor. Während einige der erweiterten Befugnisse aus meiner Sicht nachvollziehbar und im Hinblick auf die Sicherheitsgefährdung angemessen erscheinen, hatte ich bereits in meinen ersten Stellungnahmen andere Regelungen in den Arbeitsentwürfen kritisiert. So war z. B. vorgesehen, den gegenwärtigen Arbeitgeber der zu überprüfenden Person zu befragen. Im Falle einer Bewerbung hätte somit der bisherige Arbeitgeber zwangsläufig Kenntnis von der Bewerbung erlangt, mit möglicherweise weit reichenden Folgen für den Betroffenen. Erfreulicherweise wurden im Verlaufe der weiteren Beratungen einige meiner Anregungen aufgegriffen und problematische Regelungen fallen gelassen bzw. entschärft. Der schließlich beschlossene Gesetzentwurf (Bundesratsdrucksache 880/08) enthält aber noch einige datenschutzrechtlich unbefriedigende Regelungen.

– Das Gesetz selbst verlagert wichtige Regelungen in die untergesetzliche Zuverlässigkeitsüberprüfungsverordnung. Nach der Wesentlichkeitstheorie (vgl. Volkszählungsurteil des BVerfG vom 15. Dezember 1983 – 1 BvR 209), müssen die wesentlichen Regelungen, die zu Eingriffen in das Persönlichkeitsrecht führen, jedoch vom Gesetzgeber selbst getroffen werden.

– Die zuständigen Behörden dürfen die zur Überprüfung erhobenen personenbezogenen Daten speichern und nutzen, soweit dies für die Überprüfung erforderlich ist. Im Gegensatz zu den Regelungen im SÜG, in denen im Einzelnen enumerativ aufgeführt ist, wer welche Daten speichern darf (vgl. § 20 SÜG), wird hier die Befugnis zur Speicherung von personenbezogenen Daten erheblich ausgeweitet. Auch dies steht im Widerspruch zum vorgenannten Volkszählungsurteil, wonach es mit dem informationellen Selbstbestimmungsrecht nicht vereinbar ist, wenn der Bürger nicht mehr wissen kann, wer, was, wann und bei welcher Gelegenheit über ihn weiß. Insbesondere habe ich Bedenken, wenn die von angefragten Stellen mitgeteilten Erkenntnisse, die vielfach äußerst sensibel sind und zum Teil auch aus dem nachrichtendienstlichen Vorfeld stammen, automatisiert und damit voll recherchierbar gespeichert werden. Der Gesetzgeber hat beim SÜG die Gefahren, die von einer automatisierten Informationsverarbeitung für das informationelle Selbstbestimmungsrecht ausgehen, gesehen und deshalb die automatisierte Speicherung von personenbezogenen Daten durch die zuständige Stelle auf die Personengrunddaten beschränkt. Entsprechendes sollte auch hier vorgesehen werden.

4.8.3.2 Zuverlässigkeitsüberprüfungen ohne gesetzliche Grundlage

Einwilligungen der Betroffenen können Zuverlässigkeitsüberprüfungen bei Großveranstaltungen oder durch Arbeitgeber nicht legitimieren. In einem Fall habe ich eine förmliche Beanstandung ausgesprochen.

Im 21. TB (Nr. 5.2.5) hatte ich über die Zuverlässigkeitsüberprüfungen anlässlich der Fußball-Weltmeisterschaft 2006 berichtet und Zweifel geäußert, ob die Einwilligung der zu akkreditierenden Personen eine ausreichende Rechtsgrundlage für diese Überprüfungen – insbesondere im Hinblick auf die Beteiligung des Verfassungsschutzes und des BND – darstellte. Wegen der Einmaligkeit dieses Ereignisses hatte ich diese Eingriffsmaßnahmen aber noch als hinnehmbar angesehen, zumal die Betroffenen umfassend informiert worden waren.

Im Zusammenwirken der Datenschutzbeauftragten des Bundes und der Länder wurde festgestellt, dass vergleichbare Zuverlässigkeitsüberprüfungen inzwischen in zahlreichen weiteren Fällen durch öffentliche Stellen des Bundes oder der Länder und durch nicht-öffentliche Stellen durchgeführt werden. Die Prämisse, dass es sich bei den einwilligungsbasierten Zuverlässigkeitsüberprüfungen um singuläre Ereignisse gehandelt habe, ist daher nicht mehr haltbar. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher am 25./26. Oktober 2007 in einer Entschließung festgestellt, dass Einwilligungen solche Maßnahmen nicht legitimieren können (s. Kasten a zu Nr. 4.8.3.2).

Kasten a zu Nr. 4.8.3.2

Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2007

Zuverlässigkeitsüberprüfungen bei Großveranstaltungen

Anlässlich der Fußball-WM 2006 wurden im Rahmen der Akkreditierung umfassende Zuverlässigkeitsüberprüfungen nach einem auf Verwaltungsebene festgelegten Verfahren durchgeführt. Dabei wurde auf die Datenbestände der Polizei- und Verfassungsschutzbehörden des Bundes und der Länder zurückgegriffen. Dieses gesetzlich nicht vorgesehene Verfahren soll nunmehr beliebigen weiteren Veranstaltungen als Vorbild dienen.

Solche Zuverlässigkeitsüberprüfungen greifen in das Grundrecht auf informationelle Selbstbestimmung ein. Grundrechtseingriffe dürfen nicht unter Umgehung gesetzlicher Vorschriften durchgeführt werden, die Voraussetzungen und Begrenzungen solcher Verfahren regeln. Die Sicherheitsüberprüfungsgesetze des Bundes und der Länder sind für die Durchführung von allgemeinen Zuverlässigkeitsprüfungen, z. B. anlässlich von Veranstaltungen, nicht einschlägig. Eine generelle rechtliche Grundlage für Zuverlässigkeitsüberprüfungen besteht außerhalb der spezialgesetzlichen Bestimmungen nicht.

Einwilligungen können – auch wenn die Betroffenen über die Umstände informiert wurden – diese Maßnahme alleine nicht legitimieren. Dies nicht nur deshalb, weil Betroffene oft Nachteile befürchten müssen, wenn sie die Einwilligung verweigern und insoweit eine echte Freiwilligkeit fehlt. Viele Regelungen zu Überprüfungsverfahren verlangen – zusätzlich – zu den materiellen und verfahrensrechtlichen Regelungen die Mitwirkung der betroffenen Personen in Form einer schriftlichen Erklärung bei der Einleitung einer solchen Überprüfung. Außerdem sollen die Vorschriften ein transparentes Verfahren gewährleisten, in dem u. a. die Rechte Betroffener geregelt sind, so etwa das Recht auf Auskunft oder Anhörung vor negativer Entscheidung. Diese flankierenden Schutzmechanismen sind bei Überprüfungsverfahren unerlässlich.

Des weiteren wurde mir bekannt, dass die Deutsche Bundesbank in Kooperation mit den Landeskriminalämtern auf der Grundlage von Einwilligungen Zuverlässigkeitsüberprüfungen von Fremdpersonal durchführt. Einige Landeskriminalämter haben diese Kooperation jedoch unter Hinweis auf entgegenstehende landesrechtliche Vorschriften oder wegen Fehlens einer gesetzlichen Grundlage abgelehnt. Die Datenschutzkonferenz hat in einer Entschließung vom 3./4. April 2008 (s. Kasten b zu Nr. 4.8.3.2) festgestellt, dass Zuverlässigkeitsüberprüfungen durch Arbeitgeber auf die von den Betroffenen abzugebenden Einwilligungserklärungen allein nicht gestützt werden können, da es wegen der von den Betroffenen zu befürchtenden Nachteile, insbesondere im Hinblick auf den Erhalt oder die Sicherung ihres Arbeitsplatzes an der für die Wirksamkeit einer Einwilligung konstitutiven Freiwilligkeit mangelt. Nach dem Vorbehalt des Gesetzes ist es Aufgabe des Gesetzgebers, Grundrechtseingriffe gesetzlich hinreichend normenklar und insbesondere dem Verhältnismäßigkeitsgebot entsprechend zu regeln. Diesem Gebot folgend, hat der Gesetzgeber für bestimmte Bereiche entsprechende Zuverlässigkeitsüberprüfungen abschließend gesetzlich geregelt (z. B. SÜG, LuftSiG, AtG). Die von der Deutschen Bundesbank durchgeführten Verfahren sind unter keine dieser Vorschriften zu subsumieren. Da es somit an einer Rechtsgrundlage fehlt, verstoßen diese Überprüfungen gegen § 4 BDSG (Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur auf Grund eines Gesetzes oder einer wirksamen Einwilligungserklärung).

Ich habe die Deutsche Bundesbank daher aufgefordert, das Verfahren zur Zuverlässigkeitsüberprüfung unverzüglich einzustellen und die insoweit rechtswidrig erhobenen personenbezogenen Daten der Betroffenen zu löschen und zu vernichten. Die Deutsche Bundesbank ist in Übereinstimmung mit dem BMI der Auffassung, dass die Zuverlässigkeitsüberprüfungen in rechtmäßiger Weise erfolgen und die Schaffung einer besonderen Rechtsgrundlage nicht erforderlich sei. Da die Deutsche Bundesbank an dem Verfahren weiter festhält, habe ich dies nach § 25 BDSG förmlich beanstandet.

Kasten b zu Nr. 4.8.3.2

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008

Keine Daten der Sicherheitsbehörden an Arbeitgeber zur Überprüfung von Arbeitnehmerinnen und Arbeitnehmern

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Übermittlung polizeilicher und nachrichtendienstlicher Erkenntnisse an Arbeitgeber zur Überprüfung von Bewerberinnen und Bewerbern, Beschäftigten und Fremdpersonal (z. B. Reinigungskräfte) außerhalb gesetzlicher Grundlagen. In zunehmendem Maß bitten Arbeitgeber die Betroffenen, in eine Anfrage des Arbeitgebers bei der Polizei oder dem Verfassungsschutz zu etwaigen dort vorliegenden Erkenntnissen zu ihrer Person einzuwilligen. In anderen Fällen sollen die Betroffenen eine solche Auskunft („fremdbestimmte Selbstauskunft“) selbst einholen und ihrem Arbeitgeber vorlegen. Eine solche „Einwilligung des Betroffenen“ ist regelmäßig keine wirksame Einwilligung. Die Betroffenen sehen sich oftmals dem faktischen Druck des Wohlverhaltens zum Zwecke des Erhalts und der Sicherung des Arbeitsplatzes ausgesetzt.

Die gesetzliche Grundentscheidung, in einem „Führungszeugnis“ dem Arbeitgeber nur ganz bestimmte justizielle Informationen zu einer Person verfügbar zu machen, wird dadurch unterlaufen. Es stellt einen Dammbruch dar, wenn jeder Arbeitgeber durch weitere Informationen direkt oder indirekt an dem Wissen der Sicherheitsbehörden und Nachrichtendienste teilhaben kann. Die Übermittlung dieser Informationen an Arbeitgeber kann auch den vom Bundesarbeitsgericht zum „Fragerecht des Arbeitgebers“ getroffenen Wertentscheidungen widersprechen. Danach darf der Arbeitgeber die Arbeitnehmerinnen und Arbeitnehmer bei der Einstellung nach Vorstrafen und laufenden Ermittlungsverfahren fragen, wenn und soweit die Art des zu besetzenden Arbeitsplatzes dies erfordert.

Polizei und Nachrichtendienste speichern – neben den in ein „Führungszeugnis“ aufzunehmenden Daten – auch personenbezogene Daten, die in das Bundeszentralregister gar nicht erst eingetragen werden oder Arbeitgebern in einem „Führungszeugnis“ nicht übermittelt werden dürfen. Es stellt eine grundsätzlich unzulässige Durchbrechung des Zweckbindungsgrundsatzes dar, wenn ein Arbeitgeber diese Daten – über den Umweg über die Polizei oder einen Nachrichtendienst – für Zwecke der Personalverwaltung erhält. Dabei ist besonders zu beachten, dass polizeiliche oder nachrichtendienstliche Daten nicht zwingend gesicherte Erkenntnisse sein müssen, sondern oftmals lediglich Verdachtsmomente sind. Die Folgen von Missdeutungen liegen auf der Hand.

5 Rechtswesen und Innere Verwaltung

5.1 Telekommunikationsüberwachung und andere heimliche Ermittlungsmaßnahmen nach der StPO

Die Neuregelung der strafprozessualen Telekommunikationsüberwachung und anderer heimlicher Ermittlungsmaßnahmen enthält zwar einige zusätzliche grundrechtliche Sicherungen, weist aber auch erhebliche datenschutzrechtliche Defizite auf. Eine Studie des Max-Planck-Instituts belegt Nachbesserungsbedarf bei der Abfrage von Verkehrsdaten der Telekommunikation.

Im 21. TB (Nr. 6.1) hatte ich über den vom BMJ vorgelegten Referentenentwurf zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen in der StPO (sowie zur Umsetzung der Richtlinie zur Vorratsdatenspeicherung, vgl. dazu Nr. 3.2.1) berichtet. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die datenschutzrechtlichen Bedenken, die insbesondere den nicht ausreichenden Schutz des Kernbereichs privater Lebensgestaltung und der Berufsgeheimnisträger sowie zu niedrige Eingriffsschwellen für verdeckte Ermittlungsmaßnahmen betrafen, in einer Entschließung vom 8./9. März 2007 bekräftigt (vgl. Kasten a zu Nr. 5.1).

Das BMJ hat diese Einwände – mit Ausnahme der Forderung, für Erkenntnisse aus dem Kernbereich privater Lebensgestaltung nicht ein auf Strafverfahren begrenztes, sondern ein absolutes Verwertungsverbot vorzusehen – leider nicht berücksichtigt. Der von der Bundesregierung im April 2007 beschlossene Gesetzentwurf enthielt – verglichen mit dem Referentenentwurf – sogar noch datenschutzrechtliche Verschlechterungen. So wurde insbesondere der Anwendungsbereich des sog. IMSI-Catchers zur Ortung von Mobiltelefonen (§ 100i StPO) erheblich ausgeweitet, obwohl dieses Instrument unter Umständen eine Vielzahl unbeteiligter Personen betrifft und das BVerfG den Gesetzgeber ausdrücklich zur Prüfung aufgerufen hatte, ob und in welchem Umfang von einer neuerlichen Ausdehnung heimlicher Ermittlungsmethoden im Hinblick auf Grundrechtspositionen unbeteiligter Dritter Abstand zu nehmen ist (Beschluss vom 22. August 2006, 2 BvR 1345/03, vgl. hierzu auch 21. TB Nr. 6.1). Ich bedauere sehr, dass auch im Rahmen der parlamentarischen Beratungen keine substantiellen Verbesserungen erreicht wurden. Im Gegenteil hat der Bundestag sogar noch Änderungen beschlossen – etwa wurde die maximale Anordnungsdauer von Telekommunikationsüberwachungen nun doch nicht von drei auf zwei Monate reduziert –, welche die verfahrensrechtlichen Schutzvorkehrungen des Regierungsentwurfs wieder verwässern.

Gegen die am 1. Januar 2008 in Kraft getretenen (BGBl. I 2007 S. 3198) Neuregelungen der StPO sind mehrere Verfassungsbeschwerden anhängig. Eilanträge auf Aussetzung bestimmter dieser Vorschriften hat das BVerfG zwar abgelehnt, jedoch betont, dass die aufgeworfenen Fragen einer umfassenden Prüfung im Hauptsacheverfahren bedürfen und insoweit als offen angesehen werden können (Beschluss vom 15. Oktober 2008, 2 BvR 236/08, 2 BvR 237/08). Ich sehe den Entscheidungen des BVerfG mit großem Interesse entgegen.

Im Februar 2008, also erst nach Abschluss des Gesetzgebungsverfahrens zur Neuregelung der heimlichen Ermittlungsmaßnahmen, hat das BMJ eine Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht in Freiburg zur „Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO“ veröffentlicht (Bundestagsdrucksache 16/8434). Das Gutachten bestätigt die datenschutzrechtliche Kritik an der Ausgestaltung der Verkehrsdatenabfrage zu Strafverfolgungszwecken. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die maßgeblichen Ergebnisse der Studie und die hieraus von Gesetzgeber und Praxis zu ziehenden Konsequenzen in einer Entschließung vom 6./7. November 2008 im Einzelnen dargestellt (vgl. Kasten b zu Nr. 5.1). Ich appelliere an die Bundesregierung, die Regelung des § 100g StPO unter diesen Aspekten zügig nachzubessern.

Kasten a zu Nr. 5.1

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007

Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen

Die gesetzlichen Regelungen der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sollen nach der Ankündigung der Bundesregierung unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts einer umfassenden Neuregelung unterzogen werden. Die Bundesregierung will in diesem Zusammenhang auch die europäische Richtlinie zur Vorratsspeicherung von Telekommunikationsverkehrsdaten umsetzen. Das Bundesministerium der Justiz hat zwischenzeitlich einen Referentenentwurf vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont erneut, dass die Vorratsdatenspeicherung deutschem Verfassungsrecht widersprechen würde. Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken verfassungswidrig. Zudem würde die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich beeinträchtigt. Die Konferenz fordert die Bundesregierung auf, die Umsetzung der Europäischen Richtlinie zur Vorratsdatenspeicherung zumindest solange zurückzustellen, bis der bereits angerufene Europäische Gerichtshof über deren Rechtmäßigkeit entschieden hat.

Die geplante Ausweitung der Vorratsdatenspeicherung geht weit über die europarechtliche Umsetzungsverpflichtung hinaus und wäre ein zusätzlicher unverhältnismäßiger Eingriff in die Kommunikationsfreiheit der Bürgerinnen und Bürger. So sollen die Daten auch zur Verfolgung von Straftaten von erheblicher Bedeutung sowie mittels Telekommunikation begangener Straftaten genutzt werden. Zudem soll die Möglichkeit zur anonymen E-Mail-Kommunikation abgeschafft und die Nutzenden öffentlich zugänglicher E-Mail-Dienste sollen zur Angabe ihres Namens und ihrer Adresse verpflichtet werden. Diese Angaben sollen außerdem einer Vielzahl von Behörden zum Online-Abruf zur Verfügung gestellt werden, darunter der Polizei, den Staatsanwaltschaften, den Nachrichtendiensten, dem Zoll und der Bundesanstalt für Finanzdienstleistungsaufsicht. Auch dies begegnet erheblichen datenschutzrechtlichen Bedenken.

Zwar stärken einige der vorgesehenen Änderungen der Strafprozessordnung die rechtsstaatlichen und grundrechtlichen Sicherungen bei verdeckten strafprozessualen Ermittlungsmaßnahmen. Es besteht jedoch noch erheblicher Verbesserungsbedarf, insbesondere im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung, den Schutz von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern und die Voraussetzungen der Telekommunikationsüberwachung:

- Mit einer erneuten Ausweitung des Straftatenkatalogs für die Telekommunikationsüberwachung würde die Tendenz zunehmender Überwachungsmaßnahmen in verstärktem Maße fortgesetzt. Der Katalog sollte deshalb mit dem Ziel einer deutlichen Reduzierung kritisch überprüft werden. Es sollten nur Straftaten auf genommen werden, deren Aufklärung in besonderem Maße auf die Telekommunikationsüberwachung angewiesen ist, die mit einer bestimmten gesetzlichen Mindeststrafe (z. B. ein Jahr) bedroht sind und die auch im Einzelfall schwer wiegen.
- Die vorgesehene Kernbereichsregelung ist ungenügend. Sie nimmt in Kauf, dass regelmäßig auch kernbereichsrelevante Informationen erfasst werden. Für solche Informationen muss stattdessen grundsätzlich ein Erhebungsverbot gelten. Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung, die dennoch erlangt werden, müssen zudem einem absoluten Verwertungsverbot unterliegen, nicht nur für Strafverfahren.
- Der Schutz des Kernbereichs privater Lebensgestaltung ist nicht nur in den Bereichen der Wohnraum- und Telekommunikationsüberwachung zu gewährleisten. Auch für alle anderen verdeckten Ermittlungsmaßnahmen ist eine Regelung zum Schutz des Kernbereichs zu treffen.
- Für die Kommunikation mit Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern sollte ein absolutes Erhebungs- und Verwertungsverbot geschaffen werden, das dem jeweiligen Zeugnisverweigerungsrecht entspricht. Dieses sollte unterschiedslos für alle Berufsgeheimnisträgerinnen und Berufsgeheimnisträger und deren Berufshelferinnen und Berufshelfer gelten. Die im Entwurf enthaltene Differenzierung zwischen bestimmten Gruppen von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern ist sachlich nicht gerechtfertigt.
- Für Angehörige i.S.v. § 52 StPO sollte ein Erhebungs- und Verwertungsverbot für die Fälle vorgesehen werden, in denen das öffentliche Interesse an der Strafverfolgung nicht überwiegt. Die besonderen verwandtschaftlichen Vertrauensverhältnisse dürfen nicht ungeschützt bleiben.
- Für teilnehmende Personen von Kernbereichsgesprächen, die weder Berufsgeheimnisträgerinnen und Berufsgeheimnisträger noch Angehörige i. S. v. § 52 StPO sind, sollte insoweit ein Aussageverweigerungsrecht aufgenommen werden. Andernfalls bleibt der Kernbereich teilweise ungeschützt.

- Für die sog. Funkzellenabfrage, die alle Telefonverbindungen im Bereich einer oder mehrerer Funkzellen erfasst, sollten klare und detaillierte Regelungen mit engeren Voraussetzungen normiert werden. Diese sollten vorsehen, dass im Rahmen einer besonderen Verhältnismäßigkeitsprüfung die Anzahl der durch die Maßnahmen betroffenen unbeteiligten Dritten berücksichtigt und die Maßnahme auf den räumlich und zeitlich unbedingt erforderlichen Umfang begrenzt wird. Die Unzulässigkeit der Maßnahme zur Ermittlung von Tatzeuginnen und Tatzeugen sollte ins Gesetz aufgenommen werden.
- Die aufgrund einer Anordnung der Staatsanwaltschaft bei Gefahr in Verzug erlangten Daten dürfen nicht verwertet werden, wenn die Anordnung nicht richterlich bestätigt wird. Dieses Verwertungsverbot darf nicht – wie im Entwurf vorgesehen – auf Beweiszwecke begrenzt werden.
- Art und Umfang der Begründungspflicht für den richterlichen Beschluss der Anordnung der Telekommunikationsüberwachung sollte wie bei der Wohnraumüberwachung im Gesetz festgeschrieben werden. Im Sinne einer harmonischen Gesamtregelung sollten darüber hinaus qualifizierte Begründungspflichten für sämtliche verdeckte Ermittlungsmaßnahmen geschaffen werden.
- Zur Gewährleistung eines effektiven Rechtsschutzes ist sicherzustellen, dass sämtliche Personen, die von heimlichen Ermittlungsmaßnahmen betroffen sind, nachträglich von der Maßnahme benachrichtigt werden, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Darüber hinaus sollte bei Massendatenerhebungen über eine ergänzende Benachrichtigung durch eine öffentliche Bekanntmachung der Maßnahme nachgedacht werden.
- Die für die Telekommunikationsüberwachung vorgesehenen Berichts- und Statistikpflichten sollten um Angaben zur Dauer der Überwachung, zur Anzahl der Gespräche und zur Benachrichtigung Betroffener ergänzt werden.
- Die im Entwurf enthaltenen erweiterten Eingriffsgrundlagen sollten befristet und einer unabhängigen, gründlichen und wissenschaftlich unterstützten Evaluation unterzogen werden.

Kasten b zu Nr. 5.1

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008

Abfrage von Telekommunikationsverkehrsdaten einschränken: Gesetzgeber und Praxis müssen aus wissenschaftlichen Erkenntnissen Konsequenzen ziehen

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Auftrag des Bundesministeriums der Justiz die Nutzung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung (§§ 100g, 100h StPO alte Fassung) evaluiert. Die Studie geht zu Recht davon aus, dass Verkehrsdaten ein hohes Überwachungspotential in sich tragen und besser als andere Daten dazu geeignet sind, soziale Netzwerke nachzuweisen, Beziehungen zu identifizieren und Informationen über Individuen zu generieren. Der Studie zufolge ist die Zahl der Verkehrsdatenabfragen erheblich und kontinuierlich von 10 200 (2002) auf 40 000 Abfragen (2005) angestiegen. Zudem erfasst die Maßnahme regelmäßig auch eine Vielzahl unbescholtener Bürgerinnen und Bürger.

Das Bundesministerium der Justiz hat die Studie erst im Februar dieses Jahres und somit nach der Neuregelung der Telekommunikationsüberwachung und Einführung der Vorratsdatenspeicherung veröffentlicht. Das Gutachten liefert Erkenntnisse, deren Berücksichtigung im Gesetz vom 21. Dezember 2007 erforderlich gewesen wäre. Die Datenschutzbeauftragten des Bundes und der Länder sehen sich durch die Studie in ihrer schon früher geäußerten Kritik (vgl. ihre Entschließung vom 8./9. März 2007) bestätigt. Sie fordern den Gesetzgeber auf, die gesetzliche Regelung unter folgenden Aspekten nun zügig nachzubessern:

- Die Straftatenschwelle für Verkehrsdatenabfragen sollte insbesondere im Hinblick auf die inzwischen eingeführte Vorratsdatenspeicherung auf schwere Straftaten angehoben werden. Ein bedeutsamer Anteil der überprüften Verfahren war allenfalls der mittleren Kriminalität zuzuordnen.
- Die gesetzliche Höchstdauer der Maßnahme sollte von drei auf zwei Monate reduziert werden. Das Gutachten hat gezeigt, dass die praktischen Bedürfnisse, wie sie sich in den Aktendaten und Befragungsergebnissen äußern, dadurch vollständig abgedeckt würden.

– Für die Verkehrsdatenabfrage sollten (nach dem Vorbild der Regelungen für die akustische Wohnraumüberwachung) qualifizierte Begründungspflichten in der StPO vorgesehen werden. Dabei sollten auch die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen gesetzlich geregelt werden (z. B. Beweisverwertungsverbote). Wesentliche Kritikpunkte der Studie waren insbesondere die lediglich formelhafte Wiedergabe des Gesetzestextes sowie die häufig wörtliche Übernahme der staatsanwaltschaftlichen Anträge in den Begründungen.

– Zur Vermeidung von Rechtsunsicherheit und zur Stärkung des Richtervorbehalts sollte in den Fällen staatsanwaltschaftlicher Eilanordnung die Verwertbarkeit der erlangten Daten davon abhängig gemacht werden, dass ein Gericht rückwirkend die formelle und materielle Rechtmäßigkeit der Maßnahme feststellt. Dem Gutachten zufolge besteht insbesondere bei den Telekommunikationsunternehmen Unsicherheit, inwieweit sie zur Herausgabe der Verkehrsdaten verpflichtet sind, wenn eine staatsanwaltschaftliche Eilanordnung nicht innerhalb der gesetzlichen Frist richterlich bestätigt wird.

– Der tatsächliche Nutzen der Vorratsdatenspeicherung für die Strafverfolgung und damit die Erforderlichkeit der Maßnahme müssen in Frage gestellt werden. Bereits bei der früheren Höchstspeicherdauer von 3 Monaten waren nach der Studie 98 Prozent der Abfragen erfolgreich.

Auch in der praktischen Anwendung der Regelungen zur Verkehrsdatenabfrage hat die Studie Defizite deutlich gemacht. Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher auch an die Strafverfolgungsbehörden und Gerichte, aus dem Gutachten Konsequenzen zu ziehen. Besonderes Augenmerk ist vor allem auf die Prüfung der Angemessenheit der Maßnahme zu richten. Dies muss auch in substantiierten Begründungen zum Ausdruck kommen. Die gesetzlich festgeschriebenen, dem Grundrechtsschutz dienenden Benachrichtigungs-, Löschungs- und Dokumentationspflichten müssen – trotz hoher Belastungen in der Praxis – unbedingt eingehalten werden. Der Richtervorbehalt muss seine grundrechtssichernde Funktion effizient erfüllen können. Die Justizverwaltungen sind in der Verantwortung, hierfür ausreichende personelle Ressourcen zur Verfügung zu stellen.

Eine Fortführung der wissenschaftlichen Evaluation der Verkehrsdatenabfrage ist – unter den neuen rechtlichen Rahmenbedingungen und aufgrund der Weiterentwicklung der Technik – unerlässlich. Insbesondere sollten dabei Notwendigkeit und Nutzen der Verkehrsdatenabfrage – auch im Vergleich zu anderen möglichen Maßnahmen – mit Blick auf den Verhältnismäßigkeitsgrundsatz auf den Prüfstand gestellt werden.

5.2 Bundesmeldegesetz – Zentralregister als zentrales Problem

Das BMI hat einen Referentenentwurf zum Bundesmeldegesetz (BMG) mit einem zentralen Bundesmelderegister (BMR) vorgelegt. Der Bedarf für ein zusätzliches umfangreiches zentrales Melderegister auf Bundesebene ist jedoch nicht belegt. Unabhängig davon muss die datenschutzrechtliche Position der Meldepflichtigen insgesamt verbessert werden.

Das Meldewesen ist einer der wenigen Bereiche der öffentlichen Verwaltung, der – von geringen Ausnahmen abgesehen – Daten über alle Bewohner des Bundesgebietes sammelt und für administrative Zwecke zur Verfügung stellt. Schon aus diesem Grunde hatte bereits der erste Bundesbeauftragte für den Datenschutz, Professor Dr. Hans-Peter Bull, in seiner gutachterlichen Stellungnahme vom 15. Oktober 1978 (abrufbar unter www.bfdi.bund.de) die hohe datenschutzrechtliche Bedeutung des Meldewesens herausgestellt und datenschutzrechtliche Forderungen geltend gemacht, die größtenteils in das Melderechtsrahmengesetz vom 16. August 1980 (BGBl. I 1980 S. 1429) Eingang fanden (vgl. 1. TB Nr. 3.2.2; 2. TB Nr. 2.1.4). Die seinerzeitigen Kernforderungen haben angesichts der heutigen informationstechnischen Möglichkeiten ein Vielfaches an Bedeutung gewonnen:

– Beschränkung der Aufgaben der Meldebehörden auf den Identitätsnachweis,

– schlanker, gesetzlich festgelegter Merkmalskatalog,

– strenge Zweckbindung der über die Grunddaten hinausgehenden Angaben,

– gesetzlich festgelegte Betroffenenrechte (gebührenfreie Auskunft, Berichtigung, Löschung, Unterrichtung über die Erteilung sog. erweiterter Auskünfte, Übermittlungs- und Auskunftssperren).

Die Begleitung der Erarbeitung des Referentenentwurfs eines BMG mit Schaffung eines BMR durch das BMI stellte daher einen Schwerpunkt meiner Arbeit im Berichtszeitraum dar. Hierbei verfolge ich das Ziel, den erreichten Datenschutzstandard bei der Neuordnung des Meldewesens nicht nur zu erhalten, sondern unter Nutzung moderner Technologien noch deutlich zu verbessern.

Mit der Föderalismusreform des Jahres 2006 war dem Bund die ausschließliche Gesetzgebungskompetenz für das Meldewesen übertragen worden. Das BMI hatte daraufhin einen Entwurf eines BMG angekündigt (vgl. 21. TB Nr. 7.3). Gemeinsam mit den Datenschutzbeauftragten der Länder habe ich in einem Eckpunktepapier datenschutzrechtliche Anforderungen an ein solches Gesetz formuliert (vgl. Kasten zu Nr. 5.2). Der vom BMI im April 2008 vorgelegte Referentenentwurf sieht eine umfassende Neuregelung des Meldewesens und die Einrichtung eines BMR vor. Die datenschutzrechtlichen Forderungen blieben dabei bisher leider weitgehend unberücksichtigt.

Kasten zu Nr. 5.2

Gemeinsames Eckpunktepapier der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2007 – Auszug –

Datenschutzrechtliche Forderungen für ein Bundesmeldegesetz

[…]

1. Ein zentrales Bundesmelderegister und die damit verbundene mehrfache Datenhaltung sind nicht erforderlich. […]
2. Ein Bundesmeldegesetz hätte das verfassungsrechtliche Verbot eines einheitlichen und verwaltungsübergreifenden Identifikationsmerkmals zu beachten. Identifikationsmerkmale dürfen nur bereichsspezifisch gebildet, verwendet und gespeichert werden, jedoch nicht zur Zusammenführung von Daten aus unterschiedlichen Verwendungswecken. Dies schließt auch die Speicherung fremder bereichsspezifischer Identifikationsmerkmale (z. B. SteuerID) in den Melderegistern aus. Es muss untersucht werden, wie ein datenschutzgerechtes Identitätsmanagement unter Beachtung der verfassungsrechtlichen Vorgaben zu konzipieren ist.
3. Aus Datenschutzsicht muss der vollständige Meldedatenbestand bei den jeweiligen kommunalen Meldeämtern und unter ihrer Verantwortung verbleiben.
4. Eine Reform des Melderechts muss den Umfang der im Meldewesen gespeicherten Daten einer kritischen Prüfung unter den Gesichtspunkten der Erforderlichkeit und der Zweckbindung unterziehen. So steht die Anreicherung der Melderegister mit zusätzlichen, über ihre Kernaufgabe hinausgehenden Informationen (Waffenerlaubnis, Sprengstofferlaubnis, steuerliche Identifikationsnummer) im Widerspruch zu ihrem originären Zweck, Identität und Wohnsitz der Einwohner festzustellen und zu registrieren.
5. Es muss sichergestellt werden, dass jede Behörde nur die Daten erhält, die sie für ihre Aufgaben benötigt. […]
6. Eine Melderechtsreform muss auch Anlass sein, die Rechte der Meldepflichtigen deutlich zu stärken. Daher sollten bestehende Widerspruchsregelungen (bspw. Gruppenauskünfte an Parteien zur Wahlwerbung) zum Schutz der Betroffenen durch Einwilligungslösungen ersetzt werden. […]
7. Gerade weil das Melderegister in den zurückliegenden Jahren immer mehr zu einem multifunktionalen Informationspool für Wirtschaft und Verwaltung geworden ist, ist es notwendig, die Mechanismen der Fachaufsicht und der Datenschutzkontrolle sowie das Auskunftsrecht der Betroffenen im Melderecht zu stärken. Die Betroffenen können heute kaum noch erkennen, an welche Stellen Meldedaten fließen. Sie sollten deshalb grundsätzlich auch die Möglichkeit haben, Kenntnis über sie betreffende Datenabrufe, -übermittlungen und -auskünfte zu erhalten.

Die Zweifel an der Notwendigkeit der Einrichtung eines inhaltlich umfänglichen zentralen BMR konnten bislang nicht entkräftet werden. Die Einführung eines derartig gestalteten BMR wäre mit erheblichen verfassungsrechtlichen Risiken behaftet. Nach ständiger Rechtsprechung des BVerfG darf es keine Datenspeicherung auf Vorrat für unbestimmte Zwecke geben. Deshalb müssen gerade bei einem Register, das von einer Vielzahl öffentlicher und nicht-öffentlicher Stellen für unterschiedliche Verwendungszwecke zugänglich sein soll, hohe Anforderungen hinsichtlich des Umfangs der erfassten personenbezogenen Daten, der Verwendungszwecke und der Definition von Zugriffsrechten, der Form der Speicherung und der Maßnahmen zur Gewährleistung des Datenschutzes gestellt werden. Der Gesetzgeber hat dabei auch organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

Ein BMR, das die Daten sämtlicher Einwohner enthält, würde erheblich tiefer in den Datenschutz eingreifen als die bestehenden dezentralen Register, insbesondere weil die Auswirkungen eines eventuellen Datenmissbrauchs erheblich größer wären. Zudem würde ein BMR die Möglichkeit eines direkten Zugriffs auf sämtliche Melderegisterdaten und ihre Verknüpfung mit anderen Dateien ermöglichen. Da das BMR die kommunalen Register nicht ersetzen, sondern nur ergänzen soll, muss für jedes in das BMR aufzunehmende Merkmal der Nachweis geführt werden, dass seine Speicherung in einer bundesweiten Datei erforderlich ist.

Ein BMR darf auch nicht den Weg zu einem allgemeinen Personenkennzeichen bereiten, mit dessen Hilfe sich eine Vielzahl von Dateien verknüpfen ließe. Ein solches wäre, wie das BVerfG bereits 1969 in seiner Mikrozensusentscheidung dargelegt hat, nicht mit dem Grundgesetz vereinbar (1 BvL 19/63). Da sich eine umfassende Datei aller gemeldeten Personen in besonderer Weise eignen könnte, die verfassungsrechtlich gebotene „informationelle Gewaltenteilung“ zu unterlaufen, müssen bei der Konzeption des BMR zusätzliche Vorkehrungen getroffen werden, die eine zweckübergreifende Zusammenführung und Nutzung personenbezogener Daten verhindern. Hierbei käme einem datenschutzrechtlich wirkungsvollen Identitätsmanagement entscheidende Bedeutung zu (zu den technischen Rahmenbedingungen s. u. Nr. 6.5).

Ich halte den Referentenentwurf auch unter weiteren Aspekten für verbesserungsbedürftig:

– Bereits im letzten Tätigkeitsbericht (21. TB Nr. 7.3) hatte ich eine kritische Prüfung des Umfangs der in den lokalen Melderegistern gespeicherten Daten gefordert. Der Entwurf bleibt jedoch in keinem Punkt hinter den gegenwärtigen gesetzlichen Datenkatalogen (§ 2 MRRG) zurück, sondern erweitert diese (z. B. um die Tatsache des dauernden Getrenntlebens bei Verheirateten). Dies halte ich nicht für akzeptabel.

– Die datenschutzrechtliche Position der Meldepflichtigen muss gestärkt werden, indem bestehende bloße Widerspruchsrechte (z. B. gegen Melderegisteraus-

künfte an Parteien zur Wahlwerbung oder an Adressbuchverlage) durch das Erfordernis einer vorherigen Einwilligung in die entsprechende Datenübermittlung ersetzt werden.

– Unbefriedigend ist auch die sog. einfache Melderegisterauskunft, die praktisch keinerlei Einschränkungen unterliegt. Der Meldepflichtige kann zur Zeit – von wenigen gesetzlichen Ausnahmeregelungen abgesehen – nicht verhindern, dass seine Grunddaten an jedermann herausgegeben werden. Ich halte daher an meiner Forderung fest, als Korrektiv zumindest ein generelles Widerspruchsrecht des Betroffenen gegen einfache Melderegisterauskünfte einzuführen, weil es sich hier um Daten handelt, die zwangsweise beim Bürger und primär zur Erfüllung hoheitlicher Aufgaben erhoben werden (vgl. 18. TB Nr. 5.7).

– Die Auskunftsrechte der Betroffenen gegenüber den Meldebehörden sollten gestärkt werden. Die Betroffenen können nicht erkennen, an welche Stellen Meldedaten fließen. Sie sollten daher die Möglichkeit erhalten zu erfahren, welche Datenübermittlungen im Einzelfall stattgefunden haben und welche öffentlichen und privaten Stellen Melderegisterauskünfte über sie eingeholt haben. Das bestehende Auskunftsrecht über regelmäßige Datenübermittlungen an andere Stellen sollte entsprechend ergänzt werden.

– Die seit langem erhobene Forderung nach der Abschaffung der allgemeinen Hotelmeldepflicht bleibt aktuell (vgl. etwa 8. TB Nr. 2.2 und 19. TB Nr. 7.3). Die mit der Hotelmeldepflicht verbundene millionenfache Datenerhebung ist unverhältnismäßig. Hotelgäste können nicht schlechthin als Gefahrenquellen oder potentielle Straftäter angesehen werden.

Ob es in der laufenden Legislaturperiode noch zu der vom BMI angestrebten Reform des Melderechts kommt, war zu Redaktionsschluss offen.

5.3 Neue Ansätze in der amtlichen Statistik

Die statistische Datenerhebung und -aufbereitung befinden sich im Wandel und erfordern Flexibilität auf Seiten des Datenschutzes.

In der amtlichen Statistik vollzieht sich seit einiger Zeit ein tief greifender Wandel, der sowohl die Datenerhebungsprozesse als auch die Aufbereitung der statistischen Daten und deren Nutzungsmöglichkeiten betrifft.

So gibt es eine deutliche Tendenz zu einer immer stärkeren Nutzung der in Verwaltungsregistern vorgehaltenen Datenbestände an Stelle von Befragungen der Betroffenen, also weg von der Primärerhebung hin zur Sekundärerhebung. Etwa sollen bei dem Zensus 2011 die Erhebungsdaten zu einem großen Teil aus verschiedenen Verwaltungsregistern gewonnen werden (vgl. hierzu Nr. 5.5). Die Hinwendung zu dieser „sekundären" Datenerhebung wird vor allem mit der Entlastung der von statistischen Erhebungen betroffenen Bürger und der Notwendigkeit von Kosteneinsparungen begründet.

Dabei kann man nicht von vorneherein sagen, dass eine der beiden Methoden datenschutzfreundlicher sei. Bisweilen wird gegen statistische Primärerhebungen angeführt, dass der hiermit verbundene Eingriff größer sei als bei einer Sekundärerhebung, da ja bei letzterer keine „neuen" Daten erhoben würden. Dies ist nur bedingt richtig. Bei einer Sekundärerhebung werden Daten genutzt und zusammengeführt, die im Regelfall für andere Zwecke erhoben wurden. Sekundärerhebungen gehen deshalb ganz überwiegend mit Zweckänderungen einher. Die Betroffenen „merken" zudem nichts davon, dass ihre zunächst für ganz andere Zwecke angegebenen Daten in einem neuen Zusammenhang verwendet werden. Sie können also auch die Rechtmäßigkeit der Erhebung nicht selbst prüfen oder den Vorgang der Erhebung beeinflussen. Damit wird von dem datenschutzrechtlichen Grundsatz abgewichen, dass personenbezogene Daten beim Betroffenen mit seiner Kenntnis zu erheben sind. Einen gewissen Ausgleich bietet die auch bei Sekundärstatistiken notwendige bundesgesetzliche Grundlage, in der schutzwürdige Belange der Bürger unter Wahrung des Grundsatzes der Verhältnismäßigkeit berücksichtigt werden müssen. Schließlich setzen umfangreichere Sekundärstatistiken – zum Beispiel die für 2011 geplante Volkszählung – voraus, dass die Daten aus unterschiedlichen Quellen zusammengeführt werden können, wofür eine entsprechende Infrastruktur benötigt wird. Es besteht immer die Gefahr, dass diese, für die Durchführung der statistischen Erhebung eingerichtete Infrastruktur entgegen der ursprünglichen Intention auch für die Zusammenführung von Datenbeständen außerhalb der Statistik verwendet werden kann, mit möglicherweise erheblichen Folgen für die Betroffenen.

In Politik, Wirtschaft und Wissenschaft wächst das Interesse an tiefer gegliederten, detaillierteren Informationen. Einzelangaben sollen deshalb gegebenenfalls in ihrer Veränderung im Zeitablauf betrachtet werden. Dies bedeutet aber, dass sie auch längerfristig auf den Betroffenen rückführbar sind. Während es in der traditionellen statistischen Auswertung regelmäßig um Datenaggregate geht, die grundsätzlich nicht personenbeziehbar sind, handelt es sich bei diesem Ansatz um eine Ergänzung statistischer Aggregate um die Dokumentation des Verhaltens der einzelnen Erhebungseinheiten (Haushalte, Unternehmen) auf der so genannten „Mikroebene".

Dieser Methodenwechsel ist aus datenschutzrechtlicher Sicht mit einem erheblichen Risiko behaftet, da hier eine wirksame Anonymisierung, die einen Rückschluss auf eine identifizierbare statistische Erhebungseinheit zumindest faktisch ausschließt, kaum möglich erscheint. Darüber hinaus steht eine längerfristige Speicherung personenbezogener Einzelangaben im Konflikt mit dem vom Bundesverfassungsgericht in seinem Volkszählungsurteil von 1983 herausgearbeiteten Gebot der möglichst frühzeitigen Anonymisierung im Bereich der amtlichen Statistik. Eine umfassende, auf Dauer bestehende, aus den unterschiedlichsten Quellen gespeiste und fortgeschriebene Mikro-Datensammlung dürfte daher unzulässig sein. Unterhalb dieses umfassenden Ansatzes kann aller-

dings die Verwendung von Mikrodaten durchaus mit den verfassungsrechtlichen Anforderungen vereinbar sein (s. u. Nr. 5.4).

5.4 KombiFiD

Ein Beispiel für den beschriebenen Methodenwandel bei Erhebung und Auswertung statistischer Daten ist das Projekt „KombiFiD – Kombinierte Firmendaten für Deutschland“.

Von den Statistischen Ämtern des Bundes und der Länder und dem Institut für Arbeitsmarkt- und Berufsforschung der Bundesagentur für Arbeit (IAB) wurde in Zusammenarbeit mit der Deutschen Bundesbank, der Universität Lüneburg und der Fachhochschule Mainz das Projekt „KombiFiD“ ins Leben gerufen. Hierbei sollen in verschiedenen Verwaltungsbereichen (Statistische Ämter, IAB, Deutsche Bundesbank) vorhandene Unternehmensdaten aus den Jahren 1995 bis 2006 von stichprobenartig ausgewählten Unternehmen auf freiwilliger Basis für Forschungszwecke zusammengeführt und verknüpft werden. Die Initiatoren der Studie gehen davon aus, dass das so gewonnene Datenmaterial auf Mikroebene besser für die wissenschaftliche Analyse insbesondere dynamischer Prozesse geeignet sei.

Bei KombiFiD ist als Rechtsgrundlage der geplanten Datenverarbeitungsprozesse die schriftliche Einwilligung der betroffenen Unternehmen nach einer umfassenden Aufklärung über das Projekt vorgesehen. Dagegen habe ich keine grundsätzlichen Bedenken. Die Studie befindet sich derzeit noch in der Anfangsphase. Im weiteren Verlauf wird darauf zu achten sein, dass bei der Zusammenführung der Daten die für die jeweiligen Verwaltungsbereiche geltenden Geheimhaltungsbestimmungen beachtet werden. Eine Speicherung wird nur in einem jeweils abgeschotteten Forschungsbereich bei den Statistischen Ämtern, beim IAB und der Deutschen Bundesbank erfolgen.

5.5 Volkszählung 2011

Die Volkszählung 2011 wirft ihre Schatten voraus. Das hierfür vorgesehene neue Verfahren besteht aus einer Kombination von Registerzusammenführungen und Befragungen, so dass der überwiegende Teil der Bevölkerung durch die Erhebungen nicht direkt in Anspruch genommen wird.

Die letzte Volkszählung in der Bundesrepublik Deutschland, die damals nur die alten Bundesländer umfasste, fand im Jahre 1987 statt. Sie war ursprünglich für 1983 angesetzt, konnte aber auf Grund einer Anordnung des Bundesverfassungsgerichts zunächst nicht durchgeführt werden. Einzelne Vorschriften des zu Grunde liegenden Volkszählungsgesetzes 1983 wurden schließlich im so genannten Volkszählungsurteil des Gerichts vom 15. Dezember 1983 für verfassungswidrig erklärt (1 BvR 209, vgl. auch Nr. 15.3 Veranstaltung „25 Jahre Volkszählungsurteil“). Vorangegangen war eine breite und zum Teil stark emotional aufgeladene öffentliche Diskussion, in der die Sorge weiter Teile der Bevölkerung vor dem Vordringen einer kaum noch durchschaubaren modernen Informationstechnologie und deren scheinbar unabsehbaren Anwendungsmöglichkeiten in der öffentlichen Verwaltung zum Ausdruck kam. In seiner Entscheidung zu den zahlreichen Verfassungsbeschwerden befasste sich das BVerfG erstmals grundlegend mit den Gefahren der modernen Datenverarbeitung und entwickelte, ausgehend von dem allgemeinen Persönlichkeitsgrundrecht (Artikel 2 Absatz 1 GG) und der Menschenwürde (Artikel 1 Absatz 1) das Grundrecht auf informationelle Selbstbestimmung. Es garantiert die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Das BVerfG stellte damit klar, dass jede Verarbeitung personenbezogener Daten einen Grundrechtsbezug hat und am Maßstab des Grundrechtschutzes gemessen werden muss, was für das damals noch junge Datenschutzrecht einen wahren Meilenstein der Entwicklung bedeutete. Die Positionen des Volkszählungsurteils haben in der Folgezeit die Gesetzgebung, wie etwa das Volkszählungsgesetz 1987, grundlegend geprägt. Sie sind auch der datenschutzrechtliche Maßstab für die rechtliche Regelung des kommenden Zensus.

Deutschland wird sich an der nächsten EU-weiten Volkszählungsrunde mit dem Zensus 2011 in einem neuartigen registergestützten Verfahren beteiligen. Dabei sollen im Wesentlichen Daten aus bestehenden Verwaltungsregistern zu einem bestimmten Stichtag im Jahre 2011 bei den Statistischen Ämtern des Bundes und der Länder zusammengeführt werden, ergänzt durch eine postalische Befragung der Eigentümer und Verwalter von Gebäuden und Wohnungen, durch Stichprobenerhebungen sowie Erhebungen in Gemeinschaftsunterkünften. Gegen dieses neue Verfahren habe ich keine grundlegenden datenschutzrechtlichen Bedenken. Gesetzliche Grundlagen sind zum einen das Zensusvorbereitungsgesetz 2011 und zum anderen das vom Bundeskabinett beschlossene Zensusgesetz 2011.

5.5.1 Gesetzliche Vorgaben

Über den Inhalt des „Gesetzes zu Vorbereitung eines registergestützten Zensus einschließlich einer Gebäude- und Wohnungszählung 2011 (Zensusvorbereitungsgesetz – ZensVorbG 2011)“ habe ich bereits berichtet (21. TB Nr. 7.5). Es dient der Schaffung eines Anschriften- und Gebäuderegisters beim Statistischen Bundesamt als zentralem Hilfsmittel des registergestützten Zensusverfahrens und ist am 13. Dezember 2007 in Kraft getreten (BGBl. I 2007 S. 2808). Nach dem Zensusvorbereitungsgesetz werden erstmals auch die genauen geografischen Koordinaten der Gebäude gespeichert, um die gemäß damaliger Planung angestrebte Georeferenzierung der Zensusergebnisse zu ermöglichen. Auf damit verbundene datenschutzrechtliche Gefahren hatte ich hingewiesen.

In dem vom Bundeskabinett am 3. Dezember 2008 beschlossenen „Entwurf eines Gesetzes zur Anordnung des Zensus 2011 (ZensG 2011 – zum Inhalt s. Kasten a zu 5.5.1 –) sowie zur Änderung von Statistikgesetzen“ ist überraschend auch eine Änderung des ZensVorbG vorge-

sehen. Danach sollen Daten des Anschriften- und Gebäuderegisters, darunter auch die Namen der Auskunftspflichtigen für die Gebäude- und Wohnungszählung mit gebäudebezogenen Angaben aus der postalischen Zensuserhebung verknüpft und für zensusunabhängige „umwelt- und wohnungsstatistische Stichprobenerhebungen“ genutzt werden können. Da das Anschriften- und Gebäuderegister nach der bisherigen Fassung des ZensVorbG nur zur Vorbereitung des Zensus 2011 dienen sollte, handelt es sich um einen eindeutigen Fall der nachträglichen Zweckänderung für eine umfassende Datensammlung. Ich hatte bereits auf die grundsätzliche Gefahr hingewiesen, dass die für die Durchführung von Sekundärerhebungen notwendige Infrastruktur entgegen der ursprünglichen Intention auch für andere Zwecke genutzt werden könnte (s. u. Nr. 5.3). Das Anschriften- und Gebäuderegister sollte ein zentrales Infrastrukturelement für den registergestützten Zensus bleiben und nur für diesen. Die Bundesregierung wollte aber aus politischen Gründen den bestehenden Datenbedarf des BMVBS im Bereich der Klima- und Energiepolitik bei der Zensuserhebung nicht berücksichtigen, um mit dem Merkmalskatalog nicht über die EU-Zensusverordnung hinauszugehen. Deshalb verfiel sie auf den Ausweg, diesen Bedarf unter Nutzung des Anschriften- und Gebäuderegisters unabhängig vom Zensus 2011 durch Stichprobenerhebungen zu decken.

Leider war ich bei der Erarbeitung dieser Änderung nicht beteiligt worden. Ich werde meine Bedenken im parlamentarischen Verfahren geltend machen.

Kasten a zu Nr. 5.5.1

Die **Zensuserhebungen nach dem geplanten ZensG 2011** bestehen aus folgenden Komponenten:

- Auf den Stichtag 9. Mai 2011 bezogene Zusammenführung und Auswertung der Daten der Meldebehörden, der Bundesagentur für Arbeit und von Dateien zum Personalbestand der öffentlichen Hand
- Postalische Befragung der rund 17,5 Mio. Gebäude- und Wohnungseigentümer zur Gewinnung von Wohnungs- und Gebäudedaten
- Stichprobenerhebungen bei ca. 8 Prozent der Bevölkerung zur Gewinnung aus den Registern nicht entnehmbarer erwerbs- und bildungsstatistischer Daten
- Befragung der Verwalter oder Bewohner von Gemeinschaftsunterkünften wie Anstalten, Wohnheimen und ähnlichen Einrichtungen (sog. Sonderbereiche)

Hinsichtlich der Merkmale hält sich der Entwurf strikt an die Vorgaben der EU-Zensusverordnung. Die Erhebung von über die Anforderungen der EU-Zensusverordnung hinausgehenden Merkmalen, wie der oben erwähnten klima- und energiepolitischen Merkmale oder auch der Religionszugehörigkeit, ist nach dem Entwurf des ZensG 2011 nicht vorgesehen (näheres s. Kasten b zu Nr. 5.5.1).

Kasten b zu Nr. 5.5.1

Um den **Anforderungen der EU-Zensusverordnung** zu entsprechen, sollen zur Bevölkerung Daten über deren Größe und Zusammensetzung erhoben werden wie Geschlecht, Alter, Familienstand, Staatsangehörigkeiten, üblicher Aufenthaltsort und Geburtsland. Des Weiteren geht es um erwerbsstatistische Daten wie Erwerbsbeteiligung, ausgeübter Beruf, Stellung im Beruf, und bildungsstatistische Daten wie höchster allgemeiner Schulabschluss, höchster beruflicher Bildungsabschluss, aktueller Schulbesuch. Bezüglich des Gebäude- und Wohnungsbestandes sollen Daten zu Art, Lage, Eigentumsverhältnissen, Baujahr der Gebäude, zur Ausstattung der Wohnungen und zu deren Belegung erhoben werden.

Der Gesetzentwurf verzichtet auf die im ZensVorbG angelegte und nach dessen Begründung auch geplante Georeferenzierung der Zensusdaten mit Hilfe der geografischen Koordinaten. Unter Georeferenzierung ist in diesem Zusammenhang vor allem die Vorhaltung der Zensuserhebungsdaten im Bereich der amtlichen Statistik in geografisch festgelegter kleinräumiger Zuordnung zu verstehen. Hierbei könnte ein Konflikt mit dem vom BVerfG im Volkszählungsurteil von 1983 betonten Gebot der frühzeitigen und vollständigen Anonymisierung der statistischen Erhebungsdaten auftreten. Deshalb bestand zwischen den beteiligten Ressorts und mir Einigkeit darüber, dass die Art der georeferenzierten Vorhaltung (zum Beispiel im Rahmen eines geografischen Quadrats von bestimmter Größe) im Zensusgesetz festgelegt werden müsste. Im Hinblick auf die Schwierigkeiten, eine den Anforderungen des BVerfG genügende Regelung zeitgerecht zu erarbeiten, hat sich die Bundesregierung beim Zensus 2011 jedoch für den Verzicht auf diese Art der Datenvorhaltung entschieden.

Außerdem hat das BVerfG im Volkzählungsurteil von 1983 festgestellt, dass Statistik und Verwaltung strikt zu trennen sind. Die Weitergabe personenbezogener Daten, die zu statistischen Zwecken erhoben wurden, für Zwecke des Verwaltungsvollzugs ist ein unzulässiger Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Damals ging es vor allem um den im Volkszählungsgesetz 1983 vorgesehenen Abgleich der Volkszählungsdaten mit den Melderegisterdaten. Da der Hauptteil der Erhebungen zum Zensus 2011 aus einer Zusammenführung von vorhandenen Verwaltungsregisterdaten besteht, liegt die Gefahr nahe, dass durch die Zusammenführung korrigierte Daten in nicht anonymisierter Form in die Ursprungsregister, insbesondere in die Melderegister, zurückfließen. Ich habe besonders darauf geachtet, dass sowohl das Zensusvorbereitungsgesetz als auch das Zensusgesetz zu diesem Punkt die erforderlichen Schranken enthalten. Der Bürger kann also sicher sein, dass die Zensuserhebungen 2011 nicht zu einer Korrektur von Verwaltungsdaten und damit unter Umständen zu Verwaltungsmaßnahmen gegen ihn genutzt werden.

Datenschutzrechtlich problematisch ist die in dem Gesetzentwurf enthaltene Regelung der Erhebung in sensiblen Sonderbereichen. Damit sind Gemeinschaftsunterkünfte gemeint, bei denen allein die Information über die Zugehörigkeit für die Betroffenen die Gefahr einer sozialen Benachteiligung hervorrufen könnte, wie etwa bei Justizvollzugsanstalten. Die Zensuserhebungen in Sonderbereichen gehören im Verfahren des registergestützten Zensus 2011 zu den ergänzenden Primärerhebungen. Auskunftspflichtig sind für Personen in sensiblen Sonderbereichen die Anstaltsleitungen, soweit ihnen die Daten bekannt sind. Die Betroffenen werden über Art und Inhalt der Auskunftserteilung informiert. Anders als bei der Volkszählung von 1987 sollen nach dem ZensG 2011 die Daten auch in sensiblen Sonderbereichen in personenbezogener Form erhoben werden. Zwar sollen hier nur wenige Merkmale erhoben und die identifizierenden Merkmale nach einem Abgleich mit den bereits bei den statistischen Ämtern vorhandenen Meldedaten sofort gelöscht werden. Dennoch bleibt die personenbezogene Erhebung in diesen Bereichen bedenklich. Das BVerfG hatte im Volkszählungsurteil ausgeführt, dass in den Bereichen, in denen für den Betroffenen die Gefahr der sozialen Abstempelung bestehe, vorzugsweise eine anonymisierte Erhebung stattfinden sollte, um eine unverhältnismäßige Beeinträchtigung des Rechts auf informationelle Selbstbestimmung zu vermeiden. Deshalb war die Zählung in Gemeinschafts- und Anstaltsunterkünften bei der Volkszählung 1987 anonym durchgeführt worden. Die neue Regelung für den Zensus 2011 wird damit begründet, dass das anonymisierte Verfahren zu unzureichenden Ergebnissen geführt habe. Für den registergestützten Zensus sei diese Methode vollends ungeeignet, da das Verfahren auf verschiedenen personengenauen Datenabgleichen im Bereich der amtlichen Statistik beruhe. Es würden sowohl Datenabgleiche zwischen den Daten aus den verschiedenen für den Zensus genutzten Verwaltungsregistern als auch zwischen Meldedaten und Daten der primärstatistischen Erhebungen vorgenommen. Um die notwendige Qualität der Abgleichsergebnisse sicher zu stellen, müssten die Daten auch in den sensiblen Sonderbereichen personenbezogen erhoben werden. Dem ist jedoch entgegenzuhalten, dass anerkanntermaßen der registergestützte Zensus ebenso wie die herkömmliche Volkszählung ohnedies keine „perfekten“ Einwohnerzahlen liefern kann. Jedenfalls sollte im weiteren Gesetzgebungsverfahren sorgfältig geprüft werden, ob die statistikfachlichen Bedürfnisse eine personenbezogene Erhebung in sensiblen Sonderbereichen wirklich rechtfertigen.

Als zentrales Instrument für die Durchführung des registergestützten Zensus wird seit Frühjahr 2008 beim Statistischen Bundesamt nach den Vorschriften des Zensusvorbereitungsgesetzes das Anschriften- und Gebäuderegister (AGR) aufgebaut, in dem alle Gebäude mit Wohnraum in Deutschland einschließlich aller bewohnbaren Unterkünfte erfasst werden sollen. Mit seiner Hilfe sollen im Zensus 2011 vor allem die vorgesehenen primärstatistischen Erhebungen (Gebäude- und Wohnungszählung, Stichprobenerhebung, Erhebung in Sonderbereichen) gesteuert werden. Darüber hinaus soll das Register aber auch zur Zusammenführung der verschiedenen Datenquellen und zur Vollständigkeitsprüfung genutzt werden.

Die Daten für das AGR werden von den Landesvermessungsbehörden über das Bundesamt für Kartografie und Geodäsie, von den Landesmeldebehörden über die statistischen Landesämter und von der Bundesagentur für Arbeit an das Statistische Bundesamt übermittelt. Die erstmalige Übermittlung dieser Daten ist bereits im April 2008 erfolgt. Sie werden in den Jahren bis zur Durchführung des Zensus jeweils zu bestimmten Stichtagen durch weitere Datenübermittlungen aktualisiert.

5.5.2 Stand der Vorbereitungen

Ich habe mich im November 2008 beim Statistischen Bundesamt über den Stand der Zensusvorbereitung und insbesondere über den Aufbau des AGR informiert. Mein Besuch fiel in die Phase der Aufbereitung der Melderegisterdaten durch die Statistischen Landesämter, die in deren alleiniger Verantwortung vorgenommen wird. Das Statistische Bundesamt hatte daher noch keinen Zugriff auf Originaldatensätze. Der Zugriff soll erst nach der Freigabe durch die Landesämter freigeschaltet werden, voraussichtlich im Frühjahr 2009. Danach werden die Melderegisterdaten vom Statistischen Bundesamt mit den Daten der Vermessungsbehörden und der Bundesagentur für Arbeit zusammengeführt und zu anschriftenbezogenen Gruppen zusammengefasst.

Die für den Aufbau des AGR benötigten personenbezogenen Daten dürfen nur vorgehalten werden, solange und soweit sie für die Aufgabenerfüllung der Behörde erforderlich sind. Hierzu sieht das Zensusvorbereitungsgesetz vor, dass die anschriftenbezogenen Familiennamen und die von der Bundesagentur für Arbeit übermittelten Daten bereits nach der Registerzusammenführung und Plausibilisierung gelöscht werden. Das gesamte AGR soll dann zum frühest möglichen Zeitpunkt nach Abschluss der Zensusauswertung, spätestens sechs Jahre nach dem Zensusstichtag gelöscht werden.

Bei meinem Besuch im Statistischen Bundesamt habe ich mich auch über die für den Zensus geplante IT-Architektur informiert. Die gesamte Datenverarbeitung zum Zensus 2011 soll in einem besonders abgeschotteten Bereich stattfinden, zu dem nur die mit dem Zensus befassten Mitarbeiter Zugang haben, und dass alle Teilsysteme des Zensus nur über ein Zugangsportal genutzt werden können. Ich werde die Vorbereitung des Zensus weiterhin aufmerksam beobachten und auf die Einhaltung der vom BVerfG im Volkzählungsurteil von 1983 aufgezeigten Grundsätze hinwirken.

5.6 Novellierung des Bundesarchivgesetzes

Die Übernahme laufend aktualisierter digitaler Daten in staatliche Archive wirft schwierige datenschutzrechtliche Fragen auf.

Archive verkörpern – mehr als alle anderen Institutionen – das gesellschaftliche Langzeitgedächtnis. Öffentliche Stellen des Bundes haben ihre nicht mehr benötigten Ak-

ten, Urkunden und andere Schriftstücke nach dem Bundesarchivgesetz dem Bundesarchiv anzubieten. Das Bundesarchiv entscheidet auf Grund fachlicher Kriterien über die Archivwürdigkeit. Schon aus Platzgründen wird nur ein geringer Teil der Unterlagen in das Bundesarchiv übernommen; der Rest wird zur Vernichtung freigegeben. Soweit die archivierten Materialien personenbezogen sind – etwa Personalakten – sorgen Datenschutz- und Löschungsregelungen für die Wahrung des Rechts auf informationelle Selbstbestimmung der Betroffenen.

Der Übergang zu digitalen Verarbeitungsverfahren in der öffentlichen Verwaltung stellt die Archive vor erhebliche Herausforderungen. So muss entschieden werden, wie zukünftig mit elektronischen Registern (etwa dem Ausländerzentralregister oder dem Bundeszentralregister) umgegangen werden soll.

Ein Referentenentwurf des BKM, der sich zur Zeit noch in der Ressortabstimmung befindet, sieht für die laufend aktualisierten digitalen Aufzeichnungen vor, dass das Bundesarchiv zu bestimmten mit der zuständigen Behörde festzulegenden Stichtagen Kopien aller Registerinhalte übernimmt. Dies wäre datenschutzrechtlich nicht akzeptabel.

Schon nach der bisherigen Fassung des Bundesarchivgesetzes (BArchG) war die Übernahme von digitalen Datenträgern („maschinell lesbare Datenträger“ nach § 2 Absatz 5 Satz 2 BArchG) ausdrücklich vorgesehen. Dies ist etwa bei elektronischen Akten auch kein Problem, wenn dafür die bei traditionellen Akten verwendeten Verfahren angewandt werden. Die archivrechtliche Besonderheit der fortlaufend aktualisierten Register und sonstigen digitalen Dateien besteht nun darin, dass der archivrechtlich traditionell vorgegebene Archivierungszeitpunkt, der Zeitpunkt also, an dem die Unterlagen zur Erfüllung der behördlichen Aufgaben nicht mehr benötigt werden (§ 2 Absatz 1 Satz 1 BArchG), niemals eintritt. Diese Dateien werden laufend aktualisiert, also neue Bestände hinzugefügt und alte gelöscht. Sie werden zur Aufgabenerfüllung ständig benötigt. Die Vertreter der Archive halten es für fachlich geboten, diese Aufzeichnungen in Querschnittsproben der Nachwelt, insbesondere für wissenschaftliche Untersuchungen, zu erhalten.

Hiergegen habe ich massive Bedenken. Die Register und Dateien enthalten sehr sensible persönliche Daten. Die Eintragungen unterliegen deshalb strikten Löschungsregelungen. Auch wenn ich den Wert von Kopien als „Momentaufnahmen“ bestimmter Register für die historischen Sozialwissenschaften durchaus nachvollziehen kann, halte ich es verfassungsrechtlich für unabdingbar, auch die schutzwürdigen Belange der Betroffenen zu berücksichtigen. Die Abwägung erübrigt sich auch nicht dadurch, dass die in das Bundesarchiv überführten Kopien erst jeweils 30 Jahre nach dem Tode der Betroffenen genutzt werden sollen. Denn die Kopien betreffen ja zunächst lebende Personen. Ihr Grundrecht auf informationelle Selbstbestimmung ist durch die (zusätzliche) Speicherung der sensiblen Registereintragungen im Bundesarchiv beeinträchtigt, selbst wenn diese dort so gespeichert werden, dass sie nicht ohne weiteres miteinander verknüpft werden können.

Jede Vervielfältigung und Übermittlung personenbezogener Daten stellt für sich genommen bereits einen Eingriff in das Grundrecht dar, der aus meiner Sicht auch durch das wissenschaftliche Interesse nicht zu rechtfertigen ist. Im Übrigen würde durch diese Form der Archivierung die auch in dem Referentenentwurf des BKM enthaltene datenschutzrechtliche Grundregel unterlaufen, dass Rechtsvorschriften über die Verpflichtung zur Vernichtung von Unterlagen der Archivierung vorgehen.

Es müssen also Lösungen gefunden werden, die sowohl archiv- als auch datenschutzrechtlichen Positionen gerecht werden. Eine vollständige, ungeprüfte Übernahme der Daten aus fortlaufend aktualisierten Registern lehne ich ab.

5.7 Zentrale Einlader- und Warndatei

Die Errichtung einer zentralen Datei zur Speicherung von Einlader- und Warndaten zur Bekämpfung von Visumsmissbrauch begegnet starken datenschutzrechtlichen Bedenken.

Der Koalitionsvertrag zwischen CDU/CSU und SPD von 2005 spricht sich dafür aus, das europäische Visa-Informationssystem (VIS, vgl. dazu Nr. 16.2) als so genannte „Warndatei“ auszugestalten. Es solle eine nationale Warndatei geschaffen werden, falls diese Bemühungen nicht erfolgreich sein sollten. Nachdem sich die Bundesregierung im Hinblick auf den Umfang der Warndaten – das VIS sieht keine vom Visum-Antrag losgelösten Speicheranlässe vor – nicht durchsetzen konnte, wird seit geraumer Zeit an der Ausgestaltung einer nationalen „Einlader- und Warndatei“ gearbeitet.

Ein entsprechender Gesetzentwurf des BMI sah vor, neben Daten von Personen, die bestimmte Straftaten begangen haben, auch die Daten zu sämtlichen Einladern, Verpflichtungsgebern und sonstigen Bestätigenden (natürliche Personen und Organisationen) im Ausländerzentralregister zu speichern. Ganz überwiegend würden nach diesem Modell Daten über Menschen gespeichert, über die keine tatsächlichen Anhaltspunkte für ein rechtswidriges Handeln vorliegen. Zu den zu speichernden Daten zählen u. a. Name, Geburtsdatum, Staatsangehörigkeit und – soweit vorhanden – Lichtbild sowie Angaben zur Beziehung zum Visum-Antragsteller. Zugriffsrechte auf die Einlader- und Warndaten sollen neben den Ausländerbehörden und den Auslandsvertretungen einer großen Anzahl von Stellen, insbesondere der Polizei und Nachrichtendiensten eingeräumt werden.

Diese Planungen sehe ich insgesamt sehr kritisch. Insbesondere die vorgesehene umfassende Speicherung der Einladerdaten wäre bedenklich. Denn mit der Erfassung von Einladern, Verpflichtungsgebern und sonstigen Bestätigenden geht die Erhebung und Speicherung personenbezogener Daten zumeist völlig unverdächtiger Personen einher. Diese weit in das Vorfeld der Gefahrenabwehr hinein vorverlagerte Datenspeicherung würde einen gravierenden Eingriff in das Recht auf informationelle

Selbstbestimmung darstellen, an dessen Verhältnismäßigkeit Zweifel erlaubt sind. Verstärkt werden meine Zweifel durch den geplanten Aufbau des europäischen VIS, das den Sicherheitsbehörden ebenfalls weit reichende Zugriffsrechte auf Daten von Visum-Antragstellern und zugehörigen Referenzpersonen einräumt (vgl. Nr. 13.3.5). Auch den zunächst im Entwurf vorgesehenen, die Speicherung der Warndaten veranlassenden Straftatenkatalog habe ich als zu umfassend kritisiert, da er auch Straftaten mit geringerem Unrechtsgehalt enthielt. Zudem ließen sich nicht sämtliche der aufgeführten Delikte den einschlägigen Kriminalitätsbereichen, deren Verhinderung das Gesetz zum Ziel hat, zuordnen. Ein umfangreicher Straftatenkatalog würde zu einer „Quasi-Spiegelung" großer Teile des Bundeszentralregisters führen, ohne dass die dort geltenden Beschränkungen und Sicherungen des sensiblen Datenbestandes auf die Warndatei übertragen würden.

Es bleibt abzuwarten, ob das Vorhaben noch in dieser Legislaturperiode auf den Weg gebracht werden kann. Bei Redaktionsschluss war das Gesetzgebungsverfahren jedenfalls noch nicht abgeschlossen.

5.8 Die Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU)

Neben den Anträgen auf Akteneinsicht stellt die Verwendung der Unterlagen für die politische und historische Aufarbeitung der Tätigkeit des Staatssicherheitsdienstes oder der Herrschaftsmechanismen der ehemaligen DDR einen meiner Kontrollschwerpunkte dar.

Als Ergebnis zweier Beratungs- und Kontrollbesuche bei Außenstellen der BStU kann ich erneut festhalten, dass die Mitarbeiter der BStU sich durch Sensibilität und Gewissenhaftigkeit im Umgang mit den personenbezogenen Daten auszeichnen.

Neben dem einwandfreien Arbeitsablauf für einen Antrag auf Akteneinsicht habe ich den Sachbereich „Verwendung von Unterlagen für die politische und historische Aufarbeitung" nach § 32 Stasi-Unterlagen-Gesetz (StUG) geprüft. Auf der Grundlage von Eingaben habe ich insbesondere erörtert, inwieweit die Antragsteller von Forschungsvorhaben eine Belehrung erfahren, dass die zur Verfügung gestellten Unterlagen ausschließlich für den beantragten Zweck der politischen und historischen Aufarbeitung verwendet werden dürfen und dass Veröffentlichungen der Forschungsergebnisse den strengen Anforderungen des StUG entsprechen müssen. Ich begrüße es, dass die BStU zu einer Vielzahl von Vorschriften des StUG Auslegungsvorschriften und Anwendungshinweise erlassen hat, so auch zu diesem Fragenkomplex, um zum einen der Sensibilität der Materie gerecht zu werden und zum anderen eine einheitliche und juristisch belastbare Anwendung der einschlägigen Rechtsgrundlagen in der Zentrale und in allen Außenstellen sicherzustellen. Die Vorschriften zu § 32 StUG sowie die zu § 34 StUG (Verwendung von Unterlagen durch Presse, Rundfunk und Film) werde ich wegen ihrer datenschutzrechtlichen Bedeutung im Detail prüfen.

In organisatorischer Hinsicht gilt mein besonderes Augenmerk den technischen Fortschritten der Bearbeitungsverfahren durch Einsatz moderner IT-Bürokommunikation und anderer IT-Anwendungen. Auch insoweit war ein hohes Niveau an Datenschutz und Datensicherheit festzustellen. Jedoch sind im Bereich des Dokumentenmanagements zur Bescheiderteilung Verbesserungen bei Datenspeicherung und Löschung erforderlich, die ich im Einzelnen mit der BStU erörtere.

5.9 Dopingbekämpfung

Auch bei der Dopingbekämpfung darf der Datenschutz nicht vergessen werden.

Zahlreiche Dopingfälle im Leistungssport haben dazu geführt, dass die Bekämpfung des Dopings zunehmend an Bedeutung gewinnt. Im Rahmen von Dopingkontrollen und zur Dopingprävention werden zunehmend persönliche Daten über Sportlerinnen und Sportler erhoben, gespeichert, übermittelt und ausgewertet. Diese Entwicklung hat mich veranlasst, mich verstärkt der Problematik des Datenschutzes bei der Dopingprävention und -verfolgung zu widmen.

Die Bekämpfung des Dopings im Sport ist zweifellos ein wichtiges Ziel. Schon jetzt besteht in diesem Bereich eine hohe Kontrolldichte, die mit erheblichen Belastungen des Persönlichkeitsrechts des jeweiligen Sportlers verbunden ist. Für Dopingkontrollen werden Daten erhoben, die sehr sensibel sind und weit reichende Rückschlüsse auf die Gesundheit und Persönlichkeit der Sportler erlauben: einerseits das zu untersuchende biologische Material selbst, andererseits aber auch Angaben, die von den Sportlern im Vorfeld der Kontrollen verlangt werden, wie etwa Aufenthaltsdaten zur Ermöglichung von Spontankontrollen oder Krankheits- und Behandlungsdaten für medizinische Ausnahmegenehmigungen. Durch die Errichtung neuer Datenbanken – insbesondere des von der Welt-Anti-Doping-Agentur (WADA) in Kanada verwalteten, webbasierten und somit weltweit zugänglichen Informationssystems ADAMS („Anti-Doping Administration and Management System", vgl. Kasten zu Nr. 5.9) – und die Vielzahl beteiligter Kontrollorganisationen entsteht hier eine große Datenmenge, die vor unberechtigtem Zugriff, Missbrauch und Manipulation zu schützen ist.

Angemessene Datenschutzregelungen sind daher auch hier unerlässlich. Die WADA hat inzwischen einen internationalen Datenschutzstandard zum Welt-Anti-Doping-Code beschlossen, der am 1. Januar 2009 in Kraft getreten ist. Die Artikel-29-Gruppe hatte in einer Stellungnahme (WP 156 vom 1. August 2008) ein solches Regelwerk grundsätzlich begrüßt, allerdings festgestellt, dass die konkrete Ausgestaltung in mehreren Punkten europäischen Datenschutzstandards nicht entspricht. Außerdem fehlt es dort an detaillierten Regelungen für die Datenbank ADAMS. Eine Überarbeitung des WADA-Datenschutzstandards erscheint daher dringend erforderlich. Ich stehe mit dem BMI und der Nationalen Anti-Doping-Agentur (NADA) im Kontakt, um die entsprechenden Belange des Datenschutzes auch in weiteren europäischen Gremien zu unterstützen und verstärkt in die nationale Anti-Doping-Diskussion einzubringen.

Kasten zu Nr. 5.9

Zur Datenbank ADAMS

ADAMS („Anti-Doping Administration and Management System“) ist ein Internet-basiertes, weltweit abrufbares Datenmanagementsystem, das von der Welt-Anti-Doping-Agentur (WADA) in Kanada betrieben wird. Es dient als zentrale Informationsplattform für Anti-Doping-Maßnahmen und kann von nationalen Anti-Doping-Organisationen, internationalen und nationalen Sportverbänden, Veranstaltern großer Wettkämpfe, der WADA und durch sie akkreditierte Labore genutzt werden. ADAMS enthält personenbezogene Informationen der beteiligten Athleten, u. a. die Ergebnisse von Dopingkontrollen und etwaige Sanktionen, Angaben zu medizinischen Ausnahmegenehmigungen sowie Daten zu Aufenthaltsort und Erreichbarkeit. Die Aufenthaltsdaten (sog. whereabouts) werden von den Athleten selbst in ADAMS eingegeben.

Nach dem Welt-Anti-Doping-Code sind die Athleten verpflichtet, vierteljährlich genaue und vollständige Angaben darüber zu machen, wo sie im kommenden Quartal wohnen, trainieren und an Wettkämpfen teilnehmen werden, sowie Änderungen unverzüglich anzuzeigen, damit sie jederzeit für Dopingkontrollen erreichbar sind. Spitzensportler müssen seit 1. Januar 2009 darüber hinaus für jeden Tag eine Stunde benennen, zu der sie sich an einem vorher angegebenen Ort für Dopingkontrollen bereit halten.

6 Elektronische Identität

Wissen Sie, wie viele elektronische Identitäten Sie haben? Ob im Internet, am Arbeitsplatz oder in der Freizeit, überall werden wir von elektronischen Systemen aufgrund von Nutzerkennungen oder anderen Authentisierungsmechanismen erkannt und wieder erkannt. Eine Unterstützung beim Management dieser (unterschiedlichen) Identitäten ist daher dringend geboten.

Bereits in früheren TB habe ich Vorschläge zum Identitätsmanagement (IDM – s. Kasten a zu Nr. 6) veröffentlicht, z. B. im 21. TB Nr. 4.4, 4.13 oder 20. TB Nr. 4.1.1.

Durch die Verwendung von Chipkarten und durch die Nutzung des Internets hat die Frage von bewusster Anonymität bzw. bewusstem Umgang mit Kennungen, die die eigene Person identifizieren, z. B. mit E-Mail-Adressen, eine neue und zuvor nie gekannte Komplexität erreicht.

Besonders im Internet werden häufig viele unterschiedliche und kurzlebige Kennungen verwendet. Die Anwendungsbreite reicht von der Einrichtung verschiedener E-Mail-Adressen für unterschiedliche Zwecke bis zu einer eher spielerischen Verschleierung der eigenen Identität in Foren oder Chats. Daneben spielen Prozesse und Fragen der Anonymität und der Identifizierbarkeit im Internet aber auch bei Anwendungen im elektronischen Geschäftsverkehr oder im E-Government eine wichtige Rolle.

Kasten a zu Nr. 6

Das **Identitätsmanagement (IDM)** bezeichnet den geordneten und optimierten Umgang mit (unterschiedlichen) Identitätsdaten sowie mit Anonymität und Pseudonymen. Es umfasst die Verwaltung der Information über diese Identitäten, die Verwaltung der Authentifikationsnachweise, die Verwaltung der Berechtigungsstrukturen, die mit einer Identität verknüpft sind und die Protokollierung dieser Aktivitäten.

Gemäß ISO/IEC JTC 1/SC 27/WG 5 Document N5517 – A Framework for Identity Management – umfasst IDM:

- die sichere Verwaltung von Identitäten,
- den Identifikationsprozess einer Einheit (inkl. optionaler Authentisierung) und
- die Information, die mit der Identifikation einer Einheit innerhalb eines bestimmten Kontexts verbunden ist.

In vielerlei Hinsicht können Identitätsmanagementsysteme problematisch sein. Mit Hilfe dieser Systeme müssen Nutzerinnen und Nutzer die vollständige Kontrolle über ihre Daten erhalten. Dort wo Anonymität oder pseudonyme Nutzungsarten angeboten werden, darf die Zusammenführung dieser Daten nicht ungewollt zu weiter gehender Identifizierung führen.

Nicht zu den IDM-Systemen im engeren Sinne gehören geschlossene Systeme. In vielen Organisationen und Unternehmen werden IT-Systeme, die nur eine Anmeldung für unterschiedliche Anwendungen erfordern (so genannte Single Sign On-Systeme), als IDM bezeichnet. Hier steht der Komfort für die Anwender – man soll sich nur einmal an einem System anmelden – und der Komfort für die Administration dieser Anmeldedaten – man möchte alle Zugangsberechtigungen usw. an einer Stelle verwalten – im Vordergrund. Wichtig ist die ausreichende Granulierung von Rechten. Es muss z. B. möglich sein, Leserechte auf die Personaldaten nur der dafür zuständigen Organisation zu geben. Auch muss eine Datenschutzkontrolle über die jeweils zugewiesenen Rechte möglich sein. D. h., diese IDM-Systeme müssen eine ausreichende und sichere Protokollierung unterstützen.

In den vergangenen Jahren hat die missbräuchliche Nutzung der Identitätsdaten einer natürlichen Person durch Dritte (Identitätsdiebstahl) deutlich zugenommen. Die am häufigsten auftretenden Formen von Identitätsdiebstahl sind Kreditkartenbetrug, Kontenraub und Bankbetrug; dabei wird für diese Diebstähle immer öfter das Internet genutzt. Dies machen auch jüngste Beispiele aus der Telekommunikationsbranche wieder deutlich.

Elektronischer Handel und elektronische Verwaltungsdienstleistungen werden von den Bürgerinnen und Bürgern jedoch nur akzeptiert, wenn ihre Daten gegen Missbrauch und unrechtmäßige Kenntnisnahme geschützt sind. Hierzu gehört auch der Schutz vor Identitätsmissbrauch, etwa bei Bestellungen über das Internet. Gleich-

zeitig ist sicherzustellen, dass bei der Nutzung möglichst wenig personenbezogene Daten preisgegeben werden. Auch ist darauf zu achten, dass die „informationelle Gewaltenteilung“ bestehen bleibt, also die Trennung der zwischen den von verschiedenen Verwaltungsbereichen für unterschiedliche Zwecke erhobenen Daten (s. Kasten b zu Nr. 6). Eindeutige Authentifizierung und Datenvermeidung stehen dabei nicht in einem unauflösbaren Widerspruch, denn intelligente Authentifizierungsmechanismen kommen ohne übergreifende Identifikationsnummern und Personenkennzeichen aus. Durch ein modernes Identitätsmanagement können sowohl der Datenschutz als auch die Informationssicherheit gewinnen.

K a s t e n b zu Nr. 6

Daten- und Verbraucherschutz halten folgende **Mindestforderungen beim Identitätsmanagement (IDM)** für notwendig:

- selbstständige Verwaltung und Kontrolle der Verwendung von Identitätsdaten durch die Nutzer,
- den jeweiligen Erfordernissen angepasste und abgestufte Nutzungsmöglichkeiten auch hinsichtlich Anonymität und Authentizität,
- sichere Authentifizierung auch auf der Anbieterseite,
- Vermeidung von zentralen Verfahren und der Möglichkeiten zur Zusammenführung von Identitätsdaten,
- Einführung von Benachrichtigungspflichten bei Datenpannen und -verlusten.

6.1 Elektronische Gesundheitskarte

Die elektronische Gesundheitskarte wird später als vorgesehen kommen. Die lange Verzögerung ruft aber Konkurrenten auf den Plan, die alternative Modelle von elektronischen Gesundheitsakten auf dem Markt anbieten.

Über die Einführung der elektronischen Gesundheitskarte habe ich in meinen letzten Tätigkeitsberichten ausführlich berichtet (zuletzt 21. TB Nr. 4.1). Bereits damals habe ich darauf hingewiesen, dass bei diesem wichtigen Projekt der Grundsatz „Gründlichkeit geht vor Schnelligkeit“ gelten muss. Nachdem der ursprünglich vorgesehene Einführungstermin seit über drei Jahren verstrichen ist, hat nun in der Region Nordrhein der sog. Basis-Rollout begonnen. Bis die ersten freiwilligen Anwendungen der elektronischen Gesundheitskarte, wie z. B. Notfalldatensatz oder Arzneimitteltherapiesicherheitsüberprüfung, genutzt werden können, wird noch einige Zeit verstreichen. Jahre dürften noch vergehen, bis die sog. Königsdisziplin der Gesundheitskarte, die elektronische Patientenakte, verfügbar ist. Dies führt dazu, dass Krankenkassen und kommerzielle Anbieter sich auf dem Gesundheitsmarkt positionieren und eigenständige Gesundheitsakten anbieten. Diese Gesundheitsakten unterliegen aber nicht den strengen datenschutzrechtlichen Anforderungen des § 291a SGB V und dürfen nicht mit der elektronischen Patientenakte verwechselt werden. Darüber hinaus ist auch die elektronische Fallakte sowohl von der Patienten- als auch der Gesundheitsakte zu unterscheiden. Kernanliegen der Fallakte ist die Verbesserung der Kommunikation zwischen Krankenhaus und ambulantem Arzt im Rahmen der Behandlung eines konkreten Falles.

Der Basis-Rollout hat begonnen

Nach Abschluss der ersten Testphase ist Ende 2008 mit der Ausgabe der Kartenlesegeräte für die neuen Gesundheitskarten bei den Leistungserbringern in der Region Nordrhein der sog. Basis-Rollout angelaufen. Daran schließt sich Anfang 2009 die Ausgabe der elektronischen Gesundheitskarten in dieser Region an. Im weiteren Verlauf des Jahres 2009 werden dann die weiteren Regionen mit den Gesundheitskarten und den entsprechenden Lesegeräten ausgerüstet (s. Kasten zu Nr. 6.1). Die Verzögerung ist u. a. darauf zurückzuführen, dass für die Leistungserbringer nur eine ungenügende Anzahl an zertifizierten Lesegeräten vorhanden ist.

K a s t e n zu Nr. 6.1

Zwiebelschalenmodell des Basis-Rollouts;
die Zahlen geben den zeitlichen Ablauf wieder.

Bild entnommen aus einem Vortrag von D. Drees/ gematik beim Euroforum am 20. Mai 2008

Zunächst wird die Gesundheitskarte im Unterschied zur bisherigen Krankenversichertenkarte ein Lichtbild enthal-

ten und nur im Offline-Betrieb eingesetzt. Sie kann zwar schon die Basisfunktionen Versichertenstammdatendienst, elektronisches Rezept und Notfalldatensatz bedienen, was teilweise nur im Online-Betrieb geht. Voraussetzung hierfür ist das Vorhandensein eines Heilberufsausweises bei den Leistungserbringern und eine funktionierende Telematikinfrastruktur. Diese schrittweise Migration ist den bisherigen Testergebnissen geschuldet, die die erheblichen Sicherheitsanforderungen und die Komplexität der Infrastruktur aufzeigten.

Durch diese Migration wird ein seit Jahren überfälliges Problem gelöst. Auf der derzeitigen Krankenversichertenkarte sind die in § 291 Absatz 2 SGB V abschließend beschriebenen Daten enthalten, darunter auch der Versichertenstatus, für Versichertengruppen nach § 267 Absatz 2 Satz 4 SGB V (Teilnehmer an Disease-Management-Programmen wie z. B. Diabetiker) in einer verschlüsselten Form. Aus technischen Gründen ist es bisher nur möglich, dieses Merkmal in codierter Form zu speichern. Dieser Code ist allerdings frei zugänglich, so dass die Kenntnisnahme des Vorliegens einer chronischen Krankheit des betroffenen Versicherten durch unbefugte Dritte ohne Weiteres möglich ist. Da der Umstieg von der Krankenversichertenkarte auf die Gesundheitskarte nur schrittweise erfolgen kann, ist vorgesehen, die Daten der Krankenversichertenkarte auch zusätzlich auf der Gesundheitskarte in einem geschützten Bereich zu speichern. Im Konzept zur Gesundheitskarte ist ein Zugriffsschutz auf diese jetzt noch offenen Daten vorgesehen und der Zugriff selbst ist an das Vorliegen eines Heilberufsausweises gebunden.

Nach dem aktuellen Konzept der gematik werden die schützenswerten Daten in einer Region dann in den geschützten Bereich der elektronischen Gesundheitskarte überführt, wenn sowohl in dieser Region als auch in den angrenzenden Regionen eine Anbindung von 95 Prozent aller Leistungserbringer am Online-Betrieb gegeben ist. Das BMG hat zugesagt, dass die Speicherung und Nutzung dieser Daten auf der Krankenversichertenkarte ab diesem Zeitpunkt nicht mehr zulässig ist. Die bis dahin noch offenen Daten auf der Gesundheitskarte sind ebenfalls zu löschen.

Wahrnehmung von Versichertenrechten

Nach § 291a Absatz 4 Satz 2 SGB V haben die Versicherten das Recht, auf ihre Daten zuzugreifen. Bei diesen Daten handelt es sich um die mittels der elektronischen Gesundheitskarte gespeicherten Daten, die nicht zur Pflichtdokumentation des Arztes gehören, sondern in der Hoheit der Versicherten stehen. Diese Daten sind somit vergleichbar mit Kopien der Behandlungsdokumentation des Arztes, die bereits heute auf Wunsch der Versicherten in der Arztpraxis anzufertigen und zu übergeben sind. Das Gesetz selbst regelt nicht die technische Umsetzung des Einsichtsrechts der Versicherten. Es ist festgelegt, dass ein Zugriff auf die Daten nur mit dem Einverständnis des Versicherten und dessen Autorisierung sowie in Verbindung mit einem elektronischen Heilberufsausweis erfolgen darf. Es wird nicht unterschieden, ob ein zugriffsberechtigter Leistungserbringer oder ein Versicherter selbst auf die Daten zugreifen will. Das so genannte Zwei-Schlüssel-Prinzip des Zugriffs gilt deshalb grundsätzlich auch, wenn Versicherte ihr Recht auf Einsicht wahrnehmen. Versicherte können danach nur zusammen mit einem elektronischen Heilberufsausweis auf alle Daten der elektronischen Gesundheitskarte zugreifen. Der notwendige Einsatz eines elektronischen Heilberufsausweises bedeutet allerdings nicht, dass der Arzt oder Apotheker physisch am Ort der Einsichtnahme anwesend sein muss. Denkbar ist auch, dass das Einsichtsrecht an Terminals, sog. elektronischen Kiosken, ausgeübt wird, die im Wartezimmer der Arztpraxis oder in der Apotheke stehen und mit einem elektronischen Heilberufsausweis „freigeschaltet“ sind. An diesen Kiosken können Versicherte künftig kontrollieren, wer auf ihre Daten zugegriffen hat, sowie Zugriffsrechte für Ärzte oder Apotheker vergeben.

Zur Zeit liegt nur ein erster Stufenplan vor, wie im Rahmen des Rollouts die Verfügbarkeit von elektronischen Kiosken sichergestellt sein soll und somit schrittweise die Wahrnehmung von Versichertenrechten ermöglicht wird. Hier werde ich sehr intensiv auf eine schnellstmögliche Umsetzung drängen, damit nicht provisorische Lösungen zur gängigen Praxis werden. Darüber hinaus werde ich auch darauf hinwirken, dass das elektronische Patientenfach gemäß § 291a Absatz 3 Satz 1 Nummer 5 SGB V zügig bereitgestellt wird. Zur Wahrnehmung ihres Einsichtsrechts können sich die Versicherten nämlich dieses Patientenfach einrichten, in das die Daten der elektronischen Gesundheitskarte kopiert werden können. Auf dieses Patientenfach kann ohne elektronischen Heilberufsausweis zugegriffen werden. Damit allerdings auch beim Zugriff auf das Patientenfach eine Zugriffsprotokollierung möglich ist, schreibt das Gesetz den Einsatz einer Signaturkarte mit qualifizierter Signatur als zweiten Zugriffsschlüssel vor. Statt einer eigenen Signaturkarte ist auch denkbar, dass die elektronische Gesundheitskarte mit integrierter Signatur genutzt wird. Insofern stellt das elektronische Patientenfach eine Alternative zu den elektronischen Kiosken dar, soweit es um die Einsichtnahme in die medizinischen Unterlagen geht.

6.1.1 Patientendaten im Internet – Welche Risiken verbergen sich hinter den elektronischen Gesundheitsakten und der elektronischen Fallakte?

6.1.1.1 Die elektronischen Gesundheitsakten

Eine große deutsche Krankenkasse bietet ihren Mitgliedern im Rahmen eines Forschungsprojektes an, ihre Gesundheitsdaten im Internet über eine so genannte elektronische Gesundheitsakte zu führen.

In dieser Akte können alle persönlichen gesundheitsrelevanten Informationen abgelegt, verwaltet und jederzeit von überall mit Hilfe eines Internet-Zugangs abgerufen und eingesehen werden. Notizen über Arztbesuche, Röntgenbilder, Arztbefunde, Diagnosen, Therapien, verordnete Medikamente: Kurzum alles, was über den Gesundheitszustand des Nutzers Aufschluss gibt, ist damit per Internet verfügbar. Dabei werden medizinische Daten ge-

speichert, die gemäß § 3 Absatz 9 BDSG besonders schützenswert sind. Dementsprechend müssen datenschutzrechtliche Forderungen wie die Datenhoheit des Versicherten, die Freiwilligkeit der Teilnahme sowie das Erforderlichkeitsprinzip als Maßstab angelegt werden. Bei der Gesundheitsakte ist im Hinblick auf die Freiwilligkeit problematisch, dass diese Akte in der Regel durch die Krankenkasse finanziert wird und mit Pflichten des Versicherten verbunden ist. Deswegen wird die Krankenkasse versucht sein zu sehen, ob sich der Versicherte auch an die Bedingungen der integrierten Versorgung und die damit verbundenen Pflichten hält, indem sie den Bestand der Akte, Nutzungsgrad und Effizienz der Behandlungen unter die Lupe nimmt. Ich werde das Forschungsprojekt der Krankenkasse kritisch begleiten und auch ähnliche Verfahren, die von Softwarefirmen entwickelt und angeboten werden, beobachten.

Daneben werben verschiedene kommerzielle Anbieter seit Monaten z. B. in den USA für Programme, die persönliche Patientendaten im Internet speichern und mit medizinischen Informationen verständlicher machen sollen. Es dürfte nur eine Frage der Zeit sein, bis diese Internet-Gesundheitsakten auch in Deutschland verfügbar sind.

Bei dieser Art der elektronischen Gesundheitsakte entscheidet jeder Nutzer zunächst einmal für sich, ob er ein solches Angebot annimmt. Er kann selbst bestimmen, wer und in welchem Umfang Zugriff auf die Gesundheitsdaten haben darf. Hierzu zählen in erster Linie behandelnde Ärzte; aber auch Freunden oder Familienangehörigen kann der Zugang gewährt werden. Die Daten, auf die nur mit Hilfe eines persönlichen Passworts zugegriffen werden kann, werden verschlüsselt übertragen. In Deutschland sind Gesundheitsdaten besonders geschützt. Ihre Verwendung ist gesetzlich strikt geregelt und jede Nutzung für andere Zwecke ist ausgeschlossen. Wer dagegen verstößt, macht sich strafbar. Selbst Strafverfolgungsbehörden dürfen Gesundheitsdaten bei Ärzten nicht beschlagnahmen. Wenn nun Unternehmen damit werben, die Internet-Gesundheitsakte sei für Ärzte jederzeit verfügbar, um z. B. bei einem Unfall immer und überall auf die erforderlichen medizinischen Daten zugreifen zu können, ist dies zwar vordergründig überzeugend. Es stellen sich aber Fragen, wie die hochsensiblen Gesundheitsdaten ganz allgemein vor unberechtigten Zugriffen sicher geschützt werden können, ob die Teilnehmer sich der Risiken einer webbasierten Gesundheitsakte bewusst sind und von den Anbietern umfassend informiert werden. Solange solche Fragen nicht zufrieden stellend beantwortet sind, sollten Patienten besser auf die Einführung der elektronischen Patientenakte warten, die durch die elektronische Gesundheitskarte ermöglicht werden soll. Diese elektronische Patientenakte ist rechtlich und technisch mit der Gesundheitskarte verbunden, weil sie zu den freiwilligen Anwendungen nach § 291a Absatz 3 SGB V gehört und den dort festgeschriebenen strengen Regelungen unterworfen ist.

6.1.1.2 Die elektronische Fallakte

Daneben ist im Bereich der medizinischen Versorgung als weitere Variante die elektronische Fallakte im Gespräch.

Bei der elektronischen Fallakte handelt es sich um ein Werkzeug für eine sektorenübergreifende Kommunikation zwischen einzelnen Leistungserbringern. Sie soll nur für konkrete Behandlungsfälle angelegt werden und für eine bessere Kommunikation zwischen dem jeweiligen Krankenhaus und dem ambulant behandelnden Arzt sorgen.

Die Anlage dieser elektronischen Fallakte führt nicht zu der aus datenschutzrechtlicher Sicht bedenklichen unbefristeten Speicherung sensibelster Gesundheitsdaten, weil die Lebensdauer einer solchen Akte auf den konkreten Fall beschränkt ist. Zur Zeit bin ich in die Planung eines Projektes involviert, das von mehreren Kliniken und Arztpraxen unter Mitwirkung des Fraunhofer Instituts Software- und Systemtechnik vorbereitet wird. In enger Abstimmung mit den Landesbeauftragten für den Datenschutz wird dort ein umfassendes Datenschutzkonzept für die elektronische Fallakte entwickelt. Entscheidend ist aus datenschutzrechtlicher Sicht, dass eine solche Akte nur mit ausdrücklicher Einwilligung des Patienten eingerichtet wird. Damit ist gewährleistet, dass die umfangreiche Datenverarbeitung nicht ohne das Wissen des Patienten erfolgt. Darüber hinaus müssen auch technische und organisatorische Rahmenbedingungen geschaffen werden, um eine missbräuchliche Datenverarbeitung auszuschließen. Hierzu sollen Erfahrungen zu Pilotprojekten über die Effektivität und den Nutzen der vorgeschlagenen Spezifikation gewonnen werden. Die Umsetzung des Datenschutzkonzeptes wird durch die jeweils zuständige Datenschutzaufsichtsbehörde begleitet.

6.1.2 Status „Sozialhilfeempfänger“ auf der Krankenversichertenkarte

Aus der Krankenversichertenkarte lässt sich durch eine Ziffer erkennen, ob der Kartenbesitzer Empfänger von Sozialhilfeleistungen ist – eine eindeutige Rechtsgrundlage fehlt.

Wie ich feststellen musste, weist die Krankenversichertenkarte in durch eine Ziffer codierter Form neben dem Versichertenstatus (Mitglied, Familienversicherter oder Rentner) auch den Status „Sozialhilfeempfänger“ aus. Hiergegen bestehen datenschutzrechtliche Bedenken: § 264 SGB V regelt die Einzelheiten für die Übernahme der Krankenbehandlung für nicht Versicherungspflichtige gegen Kostenerstattung – dies sind in erster Linie Sozialhilfeempfänger – und schreibt eindeutig fest, dass als Versichertenstatus für Sozialhilfeempfänger bis zur Vollendung des 65. Lebensjahres die Statusbezeichnung „Mitglied“, für Empfänger nach Vollendung des 65. Lebensjahres die Statusbezeichnung „Rentner“ und für Empfänger, die das 65. Lebensjahr noch nicht vollendet haben, in häuslicher Gemeinschaft leben und nicht Haushaltsvorstand sind, die Bezeichnung „Familienversicherte“ gilt. Der Status „Sozialhilfeempfänger“ soll demnach gerade nicht aus der Karte hervorgehen.

In verschiedenen Stellungnahmen haben die Kassenärztliche Bundesvereinigung (KBV) sowie der Spitzenverband der gesetzlichen Krankenversicherung (GKV), die gemeinsam die „Technischen Spezifikationen der Versicher-

tenkarte“ gemäß §§ 291 Absatz 3, 87 Absatz 1 SGB V vereinbaren und damit für die nähere Ausgestaltung der Krankenversichertenkarte verantwortlich sind, plausibel dargelegt, dass die Kenntnis des in Frage stehenden Status zu Abrechnungszwecken sowie für die Anwendung von Steuerungsinstrumenten erforderlich ist: Mit dem GKV-Modernisierungsgesetz wurde die weitgehende versicherungsrechtliche Gleichstellung von Sozialhilfeempfängern mit den übrigen Versicherten der GKV eingeführt, verbunden mit der erstmaligen Ausgabe einer Krankenversichertenkarte an diesen Personenkreis. Aufgrund dieser gesetzlichen Neuregelung muss in der Abrechnung ausgewiesen werden, ob die kostenverursachende Person Sozialhilfeempfänger ist, denn die Krankenkassen müssen die entsprechenden Kosten den Trägern der Sozialhilfe oder der öffentlichen Jugendhilfe gemäß § 264 Absatz 7 SGB V in Rechnung stellen.

Diese nachvollziehbare Begründung hat mich dazu veranlasst, meine datenschutzrechtlichen Bedenken einstweilen zurückzustellen. In der Zukunft wird sich das Problem mit der Ablösung der Krankenversichertenkarte durch die elektronische Gesundheitskarte in dieser Weise nicht mehr stellen, da die neue Karte die Angaben nach § 291 Absatz 2 SGB V – dazu gehört auch das Statusmerkmal „Sozialhilfeempfänger“ – in verschlüsselter Form enthalten wird. Das Ziel, kurzfristig eine datenschutzfreundlichere Alternative zu dem codierten Merkmal auf der Versichertenkarte zu finden, die den Erfordernissen einer ordnungsgemäßen Abrechnung ebenso genügt, verfolge ich aber gegenüber dem BMG sowie der KBV und dem GKV-Spitzenverband weiter.

6.2 Die Einführung des elektronischen Entgeltnachweises (ELENA) steht bevor

Nach jahrelangen Vorarbeiten hat die Bundesregierung einen Gesetzentwurf zum ELENA-Verfahren eingebracht. Im Rahmen der parlamentarischen Beratungen habe ich darauf aufmerksam gemacht, dass noch nicht alle datenschutzrechtlichen Bedenken vollständig ausgeräumt werden konnten.

In meinen letzten Tätigkeitsberichten (s. zuletzt 21. TB Nr. 4.6) habe ich ausführlich über das sog. ELENA-Verfahren berichtet. Die Bundesregierung hat am 25. Juni 2008 einen Gesetzentwurf über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) beschlossen (Bundestagsdrucksache 16/10492). Dieser Gesetzentwurf sieht im Unterschied zum früheren Referentenentwurf des BMWi für das ELENA-Verfahren kein eigenständiges Gesetz mehr vor, sondern fügt es in das SGB IV ein. Dem Entwurf zufolge soll zunächst die Bundesagentur für Arbeit den elektronischen Entgeltnachweis für ihre Leistungsberechnung nutzen; darüber hinaus sollen nur die Bereiche Wohn- und Elterngeld von Beginn an in das Verfahren einbezogen werden. Die verfassungs- bzw. datenschutzrechtliche Kernproblematik dieses Gesetzentwurfes liegt unverändert darin, dass der Entwurf die Schaffung einer bundesweiten Zentraldatei (Zentrale Speicherstelle) vorsieht, an die monatlich die Übermittlung von Einkommensdaten der über 30 Millionen abhängigen Beschäftigten, Beamten, Richter und Soldaten erfolgt. Es steht bereits jetzt zu vermuten, dass der überwiegende Teil der vorrätig gehaltenen Daten tatsächlich niemals benötigt wird, da ein großer Anteil der Betroffenen die dem derzeitigen Anwendungsbereich des ELENA-Verfahrens unterfallenden Sozialleistungen niemals oder erst zu einem erheblich späteren Zeitpunkt geltend machen wird. Dies hat zur Konsequenz, dass die große Mehrzahl der übermittelten Daten von der Zentralen Speicherstelle wieder zu löschen sein wird, ohne jemals für irgendein Verfahren genutzt worden zu sein. Eine solche Datei darf nur dann eingerichtet werden, wenn die verfassungsrechtlichen Voraussetzungen, die Erforderlichkeit und Verhältnismäßigkeit, sowie die technisch-organisatorischen Vorkehrungen zum Schutz der dort gespeicherten personenbezogenen Daten vorliegen. Dabei verkenne ich nicht die Schwierigkeit, den Anteil der tatsächlich benötigten an den erhobenen Daten (Nutzungsgrad) abzuschätzen. Insofern bleiben Bedenken, ob die dann zu erwartenden Ersparnisse bei den Betrieben und der Verwaltung verfassungsrechtlich geeignet sind, den Eingriff in das Recht auf informationelle Selbstbestimmung zu rechtfertigen.

Der Nationale Normenkontrollrat ist in seiner umfassenden Stellungnahme (Bundestagsdrucksache 16/10492 Anlage 2) zu dem Ergebnis gelangt, dass der Gesetzentwurf im Interesse der Reduzierung der Bürokratiekosten einen wichtigen Beitrag leiste, nämlich im Saldo zu einer jährlichen Entlastung der Wirtschaft in Höhe von 85,6 Mio. Euro führe. Gleichzeitig hat er empfohlen, alle weiteren geeigneten Bescheinigungen möglichst zeitnah in das Verfahren zu integrieren. Dieser Empfehlung schließe ich mich an.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 6./7. November 2008 auf die verfassungsrechtlichen Zweifel am ELENA-Verfahren aufmerksam gemacht und darauf hingewiesen, dass derartige umfangreiche Datensammlungen Begehrlichkeiten wecken, die Daten für andere Zwecke zu verwenden (s. Kasten zu Nr. 6.2). In Übereinstimmung mit meinen Kollegen aus den Bundesländern halte ich darüber hinaus auch unter dem Gesichtspunkt des technisch-organisatorischen Datenschutzes weitere Verbesserungen durch den Gesetz- bzw. Verordnungsgeber für erforderlich. So darf der Schlüssel zur Ver- und Entschlüsselung der bei der Zentralen Speicherstelle gespeicherten Daten nicht in der Verfügungsgewalt der Zentralen Speicherstelle liegen, sondern muss von einer unabhängigen Treuhänderstelle verantwortet werden. Die Unabhängigkeit dieser Treuhänderstelle (infrastrukturell, technisch, organisatorisch und personell) sowie ein Beschlagnahmeverbot der im Verfahren verarbeiteten Daten ist im Gesetz oder der Verordnungsermächtigung festzulegen. Für abrufende Stellen sind starke Authentisierungsverfahren vorzuschreiben, die dem Stand der Technik entsprechen und den Forderungen der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren genügen (s. hierzu 21. TB Anlage 14).

Kasten zu Nr. 6.2

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008

Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren

Die Bundesregierung hat am 25. Juni 2008 den Gesetzentwurf über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) beschlossen (Bundestagsdrucksache 16/10492). Danach haben Beschäftigte die monatliche Übermittlung ihrer Einkommensdaten an die Zentrale Speicherstelle zu dulden, obwohl zurzeit nicht verlässlich abgeschätzt werden kann, in welchem Umfang die Speicherung der Daten tatsächlich erforderlich ist. Ein großer Anteil der Betroffenen wird die dem Anwendungsbereich des ELENA-Verfahrens unterfallenden Sozialleistungen niemals oder erst zu einem erheblich späteren Zeitpunkt geltend machen. Es steht somit bereits jetzt zu vermuten, dass eine große Zahl der übermittelten Daten von der Zentralen Speicherstelle wieder zu löschen sein wird, ohne jemals für irgendein Verfahren genutzt worden zu sein.

Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb wiederholt verfassungsrechtliche Bedenken unter dem Gesichtspunkt der Verhältnismäßigkeit und speziell der Erforderlichkeit geltend gemacht und eine substantiierte Begründung gefordert. Diese ist nicht erfolgt. Bisher bestehen lediglich höchst vage Erwartungen auf langfristige Effizienzsteigerungen insbesondere der Arbeitsverwaltung. Angesichts dieser Unklarheiten verbleiben erhebliche Zweifel an der Verfassungsmäßigkeit des Gesetzes. Hinzu kommt, dass derartige umfangreiche Datensammlungen Begehrlichkeiten wecken, die Daten für andere Zwecke zu verwenden.

Für den Fall, dass diese verfassungsrechtlichen Bedenken ausgeräumt werden können, sind unter dem Gesichtspunkt des *technisch-organisatorischen Datenschutzes* noch folgende Verbesserungen durch den Gesetz- bzw. Verordnungsgeber erforderlich:

- Es muss sichergestellt werden, (z. B. durch die Einrichtung eines Verwaltungsausschusses der Zentralen Speicherstelle), dass unter Mitwirkung von Datenschutzbeauftragten gemeinsame Grundsätze zur Wahrung des Datenschutzes und der technischen Sicherheit berücksichtigt werden.
- Für die Zentrale Speicherstelle muss ein Datenschutzbeauftragter eingesetzt werden, der dazu verpflichtet ist, regelmäßig an den Verwaltungsausschuss zu berichten.
- Schlüssel zur Ver- und Entschlüsselung der bei der Zentralen Speicherstelle gespeicherten Daten dürfen nicht in der Verfügungsgewalt der Zentralen Speicherstelle liegen. Die Ver- und Entschlüsselungskomponente muss von einer unabhängigen Treuhänderstelle verantwortet werden.
- Mittelfristig ist ein Verfahren anzustreben, das die technische Verfügungsmöglichkeit über die individuellen Daten den Betroffenen überträgt.
- Das im Rahmen der ELENA-Modellvorhaben erarbeitete differenzierte Löschungskonzept muss weiterentwickelt und umgesetzt werden.
- Für abrufende Stellen sind starke Authentisierungsverfahren vorzuschreiben, die dem Stand der Technik entsprechen und den Forderungen der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren genügen.
- Für die technischen Komponenten muss eine Zertifizierung durch eine unabhängige Prüfung vorgeschrieben werden.

6.3 Biometrie und Datenschutz

Biometrische Systeme nehmen in unseren Alltag Einzug, etwa der elektronische Reisepass (E-Pass) und der geplante elektronische Personalausweis (E-Personalausweis). Darüber hinaus finden viele Feldversuche zum Einsatz von Biometrie statt. Einige von ihnen habe ich datenschutzrechtlich begleitet.

Biometrische Systeme werten automatisiert physiologische oder verhaltenstypische Merkmale von Personen aus. Neben den zur Identifikation jeweils notwendigen Informationen können die biometrischen Merkmalsdaten allerdings auch so genannte Überschussinformationen (z. B. über Krankheiten) enthalten. Zudem können biometrische Verfahren auch heimlich oder zur routinemäßigen Massenkontrolle verwendet werden, etwa durch Kombination mit der Videoüberwachung. Deshalb müssen beim Einsatz biometrischer Verfahren von vornherein datenschutzrechtliche Aspekte berücksichtigt werden.

Mittlerweile wird eine Vielzahl von biometrischen Verfahren kommerziell genutzt, etwa Fingerabdruck-, Iris-, Venen-, Sprecher- oder Unterschriftenerkennung. Mit der stärkeren Verbreitung von Biometrie wächst das Missbrauchspotential, weil die derzeit häufig eingesetzten

Systeme noch keine 100 prozentige Sicherheit liefern. So waren Überwindungsversuche bei auf dem Markt befindlichen Systemen mit Fingerabdruck- und Gesichtserkennung erfolgreich. Auch bei einem System, das auf Iriserkennung basiert, konnte sich eine Person mit unterschiedlichen Identitäten in das System einspeichern lassen oder, in einem anderen Fall, Zutritt verschaffen, obwohl die Irisdaten bereits in einer Sperrliste gespeichert waren. Wenn die Biometrie einer Person kompromittiert wurde, sind die Konsequenzen meist nicht klar. Wie ist z. B. zu beweisen, dass die eigenen biometrischen Informationen missbraucht wurden? Nicht zuletzt aus diesem Grunde stufe ich den Schutzbedarf bei Biometriedaten als sehr hoch ein.

Das bedeutsamste biometrische Verfahren im Bereich des Bundes ist die Automatisierte Biometriegestütze Grenzkontrolle (ABG). Hier muss sich der Passagier registrieren, indem seine Ausweisdaten einschließlich der Irisdaten erfasst und bei der Bundespolizei bis zum Widerruf gespeichert werden. Darüber hinaus wird er erkennungsdienstlich überprüft. Beim Grenzübertritt verifiziert er sich gegenüber einem Rechner der Bundespolizei mit seinem Pass und seiner Iris und kann nach einer erneuten erkennungsdienstlichen Überprüfung den Grenzpunkt passieren (vgl. 21. TB Nr. 4.5.2).

Die im E-Pass und im E-Personalausweis gespeicherte Biometrie wird mangels vorhandener Kontrolltechnik derzeit noch nicht im Grenzkontrollverfahren eingesetzt.

Im Berichtszeitraum habe ich mich mit folgenden weiteren Anwendungen biometrischer Systeme befasst:

– Grenzkontrollsystem zur Anwendungserprobung von Gesichtserkennungsverfahren (GAnGes)

2009 will die Bundespolizei die Möglichkeiten der Gesichtserkennung im Projekt GAnGes am Frankfurter Flughafen testen. GAnGes soll im Rahmen der Grenzkontrolle zum Einsatz kommen, wobei ein aktuell aufgenommenes Foto mit dem im Ausweis gespeicherten Bild verglichen wird (s. auch Nr. 6.4). Dieses Verfahren soll der beschleunigten Kontrolle von Passagieren dienen und gleichzeitig die Hürde für einen Passmissbrauch erhöhen. Der Feldversuch hat zum Ziel, die Tauglichkeit des Verfahrens für eine automatisierte Grenzkontrolle zu überprüfen.

Bei einem erfolgreichen Test von GAnGes soll das ABG-Verfahren – das bislang nur auf freiwilliger Basis stattfindet – als offizielles Verfahren abgelöst werden.

– Fast Identification

Ein Personenkontrollverfahren zur schnellen und mobilen Identifikation ist in verschiedenen Bundesländern erfolgreich im Einsatz. Es ist vorgesehen, die Geräte zur erkennungsdienstlichen Überprüfung von Personen mit Hilfe der Fingerabdruckerkennung bei der Bundespolizei einzuführen. Über die Technik habe ich bereits früher unter dem Begriff „Fast Identification“ (s. 21. TB Nr. 5.2.4.2) berichtet. Ein mobiler Fingerabdruckscanner erfasst den Fingerabdruck einer Person. Das Gerät baut eine gesicherte Funkdatenverbindung zur Datenbank des BKA auf. Dort werden die aktuell aufgenommenen Fingerabdrücke mit dem Datenbestand der Fahndungsdatei verglichen. Das Ergebnis wird dem Polizeibeamten auf dem Display mitgeteilt. Der Beamte kann umgehend weitere Schritte einleiten.

– Foto-Fahndung

Im Forschungsprojekt „Foto-Fahndung“ hat das BKA von Oktober 2006 bis Ende Januar 2007 die biometrische Gesichtserkennung als Fahndungshilfsmittel für die Polizei getestet (s. 21 TB Nr. 5.2.6). Im Ergebnis war es mit den getesteten Systemen nur dann möglich, gesuchte Personen in Menschenmengen automatisch wieder zu erkennen, wenn die äußeren Rahmenbedingungen, insbesondere die Beleuchtung, dies zuließen. Von der Einführung des Fahndungshilfsmittels hat das BKA vorerst abgesehen. Ich begrüße dieses bedachte Vorgehen (s. auch Nr. 8.1).

– FIREBIRD

Der Test bezüglich der Leistungsfähigkeit von Gesichtserkennungssystemen muss in der Regel immer in aufwändigen Feldversuchen erfolgen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) baut zur Vereinfachung dieser Tests eine Bilddatenbank „FIREBIRD“ auf. Hierzu wird das BSI die Gesichtsbilder von Freiwilligen erfassen und in einer Datenbank speichern. Ziel ist es, über die Gesichtsbilder eines repräsentativen Querschnitts der Bevölkerung zu verfügen. Zum einen können die Anbieter von Gesichtserkennungssystemen ihre Systeme vom BSI mit Hilfe dieser Datenbank auf ihre Leistungsfähigkeit testen lassen, zum anderen können Vergleichstests für Beschaffungsmaßnahmen zwischen unterschiedlichen Systemen durchgeführt werden. Die Datenbank unterliegt strengen Restriktionen, was die Nutzung der Bilder betrifft. So sollen die Bilder z. B. nicht an Dritte weitergegeben werden dürfen.

Sieht man einmal vom E-Pass und vom E-Personalausweis ab, wurden bei den erwähnten Verfahren die biometrischen Daten außerhalb der Kontrolle der Betroffenen in externen Datenbeständen gespeichert. Dies begegnet grundsätzlichen datenschutzrechtlichen Bedenken, weil damit stets eine erhöhte Missbrauchsgefahr einhergeht. Zudem könnten die für eine bestimmte Aufgabe angelegten Biometrie-Datenbanken auch für andere Zwecke in anderen Verfahren verwendet werden. Auch diese Gefahr sollte nicht unterschätzt werden.

6.3.1 Elektronischer Pass der II. Generation

Der sog. E-Pass der II. Generation, der neben dem digitalisierten Lichtbild auch digitalisierte Fingerabdrücke enthält, ist eingeführt worden. Die datenschutzrechtliche Skepsis bleibt.

Nachdem die Ratsverordnung 2252/2004 als gemeinschaftsrechtliche Vorgabe für die Einführung von biometrischen Merkmalen in Pässe und Reisedokumente ohne die Möglichkeit zu sorgfältiger Prüfung aller datenschutzrechtlicher Aspekte und Bedenken „im Hauruck-Verfahren“ am 13. Dezember 2004 beschlossen worden war und

der so genannte E-Pass der I. Generation ab November 2005 in Deutschland eingeführt wurde, ist zum 1. November 2007 nach einer weiteren Änderung des Passgesetzes (BGBl. I S. 1566, 2317) der so genannte E-Pass der II. Generation mit auf dem Chip gespeichertem Lichtbild und digitalisierten Abdrücken der beiden Zeigefinger eingeführt worden. Über die Ratsverordnung 2252/2004 und den E-Pass der I. Generation hatte ich im 20. TB (Nr. 6.2.1) und 21. TB (Nr. 4.5.3) berichtet.

Die Fingerabdruckdaten des E-Passes der II. Generation werden durch ein besonderes Verschlüsselungs- und Zugangsverfahren, die „Extended Access Control" (EAC), geschützt. Bei diesem Verfahren werden nicht nur die Daten selbst, sondern auch die technische Kommunikation des Chips mit dem Passlesegerät besonders gesichert. Der Chip prüft, ob es sich um ein berechtigtes, speziell autorisiertes Lesegerät handelt. Die Berechtigung (Signatur) der Lesegeräte wird durch das Bundesamt für Sicherheit in der Informationstechnik verwaltet. Zuvor ist zu prüfen und festzulegen, wer Lesegeräte einsetzen darf und welche Staaten auf die besonders gesicherten Daten deutscher E-Pässe zugreifen dürfen. Wie Staaten, die über eine Leseberechtigung verfügen, mit den biometrischen Daten (und anderen Passdaten) umgehen, entzieht sich der Kontrolle deutscher Stellen. Diese Daten könnten also in Personendatenbanken einfließen.

Meine Skepsis gegen die Entscheidung für die Aufnahme der Fingerabdrücke wird durch die Erfahrungen in den USA bestätigt. So hat der dortige Rechnungshof festgestellt, dass die Aufnahme der Zeigefingerabdrücke für einen Abgleich mit der Fingerabdruckdatenbank des FBI (AFIS) nicht den erhofften Sicherheitsgewinn erbracht hat. Bei Einreise in die USA werden deshalb von Ausländern nicht mehr zwei, sondern alle zehn Fingerabdrücke aufgenommen. Damit bleibt es Reisenden aus der EU auch bei Vorlage ihres elektronischen Reisepasses der II. Generation nicht erspart, sich alle zehn Fingerabdrücke abnehmen zu lassen, die dann für unabsehbare Zeit von US-Behörden gespeichert werden.

Die Speicherung biometrischer Merkmale für staatliche Identitätskontrollen weckt zudem Begehrlichkeiten nichtöffentlicher Stellen. Ich halte es nur für eine Frage der Zeit, dass auch die Wirtschaft Interesse an einer biometrisch abgesicherten Identifizierung entwickelt und deshalb Zugriff auf die Biometriedaten im elektronischen Pass und im elektronischen Personalausweis (s. u. Nr. 6.3.2) verlangt. Unabhängig von diesem schon jetzt absehbaren Interesse der Wirtschaft stellt sich auch heute schon die Frage nach der Sicherheit der für die Aufnahme biometrischer Daten verwendeten Technik. Was geschieht, wenn kein hinreichender Kopierschutz der Daten (mehr) gewährt wird und Kriminelle „gestohlene" Fingerabdruckdaten missbrauchen können?

Die Novellierung des Passgesetzes wird immerhin einigen zentralen Forderungen des Datenschutzes gerecht:

Dies gilt insbesondere für den Ausschluss einer verdachtsunabhängigen, unbefristeten Vorhaltung von Fingerabdruckdaten. Eine derartige bundesweite Speicherung ohne irgendeine, auch nur ansatzweise präzisierte „Schwelle" und für einen im Zeitpunkt der Erhebung noch sehr unwahrscheinlichen Zweck (künftige Prävention bzw. künftige Strafverfolgung) wäre mit den vom Bundesverfassungsgericht konkretisierten verfassungsrechtlichen Vorgaben des Grundrechtes auf informationelle Selbstbestimmung nicht zu vereinen. Selbst bei zurechenbarer, vom Straftäter ausgelöster Speicherung von Fingerabdruckdaten ist nach dem Bundeskriminalamtsgesetz die Erforderlichkeit weiterer Speicherung jeweils spätestens nach zehn Jahren zu prüfen.

In Deutschland werden seitens des Bundes keine aus den biometrischen Merkmalsdaten gewinnbaren Überschussinformationen z. B. zu Erkrankungen oder sonstigen personenbezogenen Merkmalen ausgewertet. Allerdings werden die dies ermöglichenden sog. Rohdaten („Images") und nicht – wie von Seiten des Datenschutzes gefordert – der maschinenlesbare Code der Merkmalsdaten („Templates") im Ausweis gespeichert, so dass aus den Rohdaten gewinnbare Zusatzinformationen ggf. von anderen Stellen ausgewertet werden könnten.

Der Ausleseprozess am „Chipterminal" erfolgt in der Regel mit Kenntnis und in Gegenwart des Betroffenen, so dass jedenfalls hier ein gewisses Maß an Transparenz gewährleistet ist. Allerdings ist nicht völlig auszuschließen, dass die nur mit dem schwächeren Verfahren der „Basic Access Control" (BAC) geschützten Daten des Gesichtsbildes von unberechtigten Dritten ausgelesen werden können.

Aus datenschutzrechtlicher Sicht würde ich es begrüßen, wenn ein (direkter) Online-Zugriff aller Polizei- und Ordnungsbehörden auf die bei den örtlichen Passbehörden gespeicherten Lichtbilder ausgeschlossen und eine datenschutzfreundliche Regelung für eine kontrollierbare Übermittlung gefunden werden könnte.

In der Vergangenheit hatten verschiedene Meldebehörden beim Passantragsverfahren datenschutzrechtliche Probleme. Diese wurden häufig durch organisatorische Mängel in den einzelnen Behörden hervorgerufen. Ob die Schwachstellen beim Antragsverfahren gänzlich behoben sind, werden die weiteren Kontrollen der für den Bereich zuständigen Landesbeauftragten für den Datenschutz zeigen.

6.3.2 Elektronischer Personalausweis

Nach Einführung des Elektronischen Reisepasses der II. Generation mit Wirkung ab dem 1. November 2007 hat die Bundesregierung den „Entwurf eines Gesetzes über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften" (PAuswG, Bundestagsdrucksache 16/10489) am 7. Oktober 2008 beschlossen.

Der Elektronische Personalausweis (E-Personalausweis) sollte ursprünglich wie der E-Pass der II. Generation obligatorisch mit digitalisiertem Lichtbild und digitalisierten Abdrücken der beiden Zeigefinger ausgestattet werden. Darüber hinaus soll der E-Personalausweis optional einen elektronischen Identitätsnachweis und eine elektronische

Signaturfunktion nach dem Signaturgesetz ermöglichen. Der E-Personalausweis ist damit auch als einheitliches Werkzeug für verschiedene Formen verbindlichen, identitätsrelevanten Handelns im elektronischen Rechtsverkehr sowohl für E-Commerce als auch für E-Government konzipiert. Seine Funktionalitäten, aber auch die damit möglichen Risiken wie Missbrauch der ID-Funktion bzw. Identitätsdiebstahl, gehen somit deutlich über die des E-Passes hinaus.

Die Speicherung nicht nur des Lichtbildes, sondern auch der Zeigefingerabdrücke wurde im Bundestag und in der Öffentlichkeit kontrovers diskutiert. Ich hatte die ursprünglich beabsichtigte obligatorische Speicherung (auch) der Fingerabdrücke im Verlauf des Gesetzgebungsverfahrens kritisiert, da die Erforderlichkeit nicht überzeugend dargelegt werden konnte. Bereits der bisher verwendete Personalausweis zeichnet sich durch hohe Fälschungssicherheit aus. Während die Speicherung des Lichtbildes im Hinblick auf die Vorgaben der internationalen Luftfahrtorganisation ICAO noch nachvollziehbar ist, gilt dies nicht für die obligatorische Speicherung (auch) der Fingerabdrücke. Nach intensiver Diskussion ist im Gesetz die Speicherung der Fingerabdrücke auf freiwilliger Basis, also nur mit Einwilligung des Ausweisinhabers, vorgesehen. Ich habe dies als Schritt in die richtige Richtung begrüßt und ein ausdrückliches gesetzliches Benachteiligungsverbot angeregt. Die Entscheidung für die Speicherung der Fingerabdrücke muss auf der freien Entscheidung der Betroffenen beruhen. Sie darf nicht unter dem Druck einer andernfalls drohenden Benachteiligung erfolgen. Ich begrüße es deshalb, dass der Bundestag sich meine Anregung zu eigen gemacht und den Gesetzentwurf mit einer entsprechenden Ergänzung beschlossen hat.

Aus meiner Sicht sollte den Bürgerinnen und Bürgern eine zuverlässige und einfache Möglichkeit gegeben werden, die Richtigkeit der tatsächlich gespeicherten Daten zu überprüfen. Ich hoffe, dass die für eine solche IT-gestützte Verifikation erforderliche Technik für E-Personalausweis und für E-Pässe zeitnah beschafft und bundesweit in der Fläche verfügbar sein wird.

Mit der Verbreitung biometrischer Zugangssicherungsverfahren wird das Missbrauchsrisiko steigen; Fälle des – zumindest versuchten – Identitätsdiebstahles könnten zunehmen. Eine effektive Sicherung der biometrischen Daten auf dem E-Personalausweis ist deshalb unverzichtbar. Die Bundesregierung hat diese Forderung aufgegriffen und will diese Daten mit dem bereits beim E-Pass eingesetzten Zugriffsschutz (Extended Access Control) sichern.

Wegen der Zusatzfunktionen für die Bereiche des E-Commerce und des E-Government ergibt sich beim E-Personalausweis eine deutlich größere Missbrauchsgefahr als beim E-Pass.

Deshalb sollten auch die Vorkehrungen zum Schutz dieser (optionalen) Funktionen und die Rahmenbedingungen für die bei der elektronischen Kommunikation verwendeten Berechtigungszertifikate, mit denen den Diensteanbietern der Zugriff auf die Identitätsnachweisfunktion eröffnet wird, präzise und soweit als möglich durch Gesetz festgelegt werden. Ferner halte ich Konzepte zur Schadensabwehr und -minimierung insbesondere bei drohendem Angriff auf die für E-Commerce und E-Government genutzte Informationstechnik durch Schadsoftware für unverzichtbar. Ein Auslesen des Datenflusses und der PIN muss zuverlässig ausgeschlossen werden, damit Transaktionen nur vom wahren Berechtigten vorgenommen werden können. Der Zugriff auf die Identitätsdaten sollte schließlich nur solchen privaten Stellen gestattet werden, die sich einem Datenschutzaudit unterwerfen.

Das so genannte Hinterlegungsverbot des § 1 Absatz 1 Satz 3 PAuswG und die Verpflichtung des Ausweisinhabers, durch technische und organisatorische Maßnahmen zu gewährleisten, dass die Funktion des elektronischen Identitätsnachweises nur in einer sicheren Umgebung eingesetzt werden kann (§ 26 Absatz 3 PAuswG) zeigen, dass die Bundesregierung die Missbrauchsgefahren ebenfalls erkannt hat.

Diesen Gefahren sollte allerdings mit einer technischen Optimierung der Hard- und Software begegnet werden und nicht mit einer – für den technisch nicht besonders versierten Ausweisinhaber nicht ohne weiteres realisierbaren – Verpflichtung, die ID-Funktion nur in einer sicheren, dem Stand der Technik entsprechenden Umgebung zu nutzen.

6.4 Automatisierte Grenzkontrollen/Projekt GAnGes bzw. easyPass

Die Bundespolizei will ein neues Verfahren zur Durchführung der Grenzkontrolle unter Anwendung des biometrischen Merkmals des Gesichtsbildes testen. Am Flughafen Frankfurt/Main soll hierzu ein Pilotprojekt durchgeführt werden.

Neben der automatisierten biometriegestützen Grenzkontrolle (ABG), über die ich mehrfach berichtet hatte (s. 20. TB Nr. 5.3.5 und 21. TB Nr. 4.5.2; vgl. auch o. Nr. 6.3), erprobt die Bundespolizei ein weiteres biometrisches Verfahren zur Beschleunigung und Vereinfachung des Grenzkontrollprozesses. Hierfür soll das Gesichtsbild der Person, die ein Reisedokument zur Überprüfung vorlegt, herangezogen werden.

Im Rahmen des 2009 beginnenden Pilotprojektes „GAnGes“ (Grenzkontollsystem für die Anwendungserprobung von Gesichtserkennungsverfahren) bzw. „easyPass“ am Flughafen Frankfurt/Main soll u. a. geprüft werden, ob sich der Einsatz von Gesichtserkennungsverfahren in Bezug auf Erkennungsgenauigkeit und das zugrunde liegende Sicherheitsniveau, z. B. hinsichtlich der Täuschungs- oder Überwindungsmöglichkeit, für die Grenzkontrolle eignet. Die Teilnahme am Test ist nur für EU-Bürger möglich, die über einen elektronischen Reisepass (E-Pass) verfügen, in dessen integriertem Speicherchip das Gesichtsbild der Passinhaberin bzw. des Passinhabers hinterlegt ist.

Für die Durchführung des Pilotprojektes soll ein Datenbestand von Referenzbildern der am Pilotprojekt teilneh-

menden Reisenden für die Dauer des Projektes bereitgestellt werden. Nur so könne die für die Konfiguration des Systems notwendige Möglichkeit von Vergleichen zwischen den beim Kontrollprozess aufgenommenen Bildern von Reisenden und den als Referenz abgelegten Lichtbildern anderer Reisender geschaffen und das Sicherheitsniveau des biometrischen Verfahrens bestimmt werden.

Auf meine Anregung hin haben das BMI und die Bundespolizei eine Einwilligungserklärung und ein Informationsblatt über die freiwillige Teilnahme am Pilotprojekt „easyPass“ erarbeitet. Reisende, die am GAnGes- bzw. easyPass-Verfahren nicht teilnehmen, durchlaufen das herkömmliche Verfahren am Grenzkontrollschalter der Bundespolizei.

Ich werde das Projekt weiterhin begleiten.

6.5 Bundesmeldegesetz

Die Melderechtsreform darf nicht dazu führen, dass große Datensammlungen bereichsübergreifend zusammengeführt werden können. „Sprechende“ oder einheitlich durchgängige Ordnungsmerkmale im Melderegister wären mit diesem Grundsatz nicht vereinbar. Notwendig ist ein datenschutzrechtlich wirkungsvolles Identitätsmanagement mit Einrichtung einer unabhängigen Vertrauensstelle für die Generierung und das Management bereichsspezifischer Ordnungsmerkmale.

Das BMI beabsichtigt, nach der durch die Föderalismusreform im Jahre 2006 erfolgten Übertragung der Gesetzgebungskompetenz für das Melderecht auf den Bund, das Meldewesen gesetzlich umfassend neu zu regeln und ein Bundesmelderegister (BMR) einzurichten (zu grundsätzlichen Fragen und zur Historie s. Nr. 5.2).

Um die Persönlichkeitsrechte und den Schutz der Identität des Einzelnen zu gewährleisten, sind jedoch einige Funktionsbedingungen bei der Einrichtung eines BMR unerlässlich:

Die Minimierung der Datenspeicherung ist ein wesentliches Element des Datenschutzes. Ich trete daher dafür ein, dass in einem BMR – sofern ein Bedarf dafür überhaupt in Frage kommt – nur Grundpersonalien dauerhaft gespeichert werden. Diese dienen der eindeutigen Identifikation des Einzelnen oder ausdrücklich dem Persönlichkeitsschutz, z. B. in Form der Eintragung von Übermittlungssperren. Weitere Daten dürfen aus meiner Sicht von der kommunalen Meldebehörde nur dann und insoweit dem BMR bereitgestellt werden, wie sie für einen konkreten Übermittlungsbedarf aus dem BMR benötigt werden. Diese weiteren Daten wären nach der Übermittlung unverzüglich zu löschen.

Das Ordnungsmerkmal eines BMR ist das zentrale Zugriffs- und ggf. Verknüpfungselement. Die datenverarbeitungstechnische Organisation von Ordnungsmerkmalen hat daher unter Datenschutzaspekten höchste Bedeutung. Sie ist das Kernelement für den Schutz der Identität des Einzelnen. Nach meiner konzeptionellen Auffassung, die ich dem BMI unterbreitet habe, darf das BMR ein ausschließlich internes Ordnungs- und Zugriffsinstrument als eigenes Ordnungsmerkmal enthalten. Dieses wäre abstrakt zu bilden und dürfte sich nicht aus personenbezogenen Daten herleiten und keinen Rückschluss auf eine konkrete Person ermöglichen (kein „sprechendes“ Ordnungsmerkmal, kein „sprechender Schlüssel“). Dieses Ordnungsmerkmal dürfte auch nicht übermittelt werden. Für den jeweiligen Adressaten müsste vielmehr ein spezifisches eigenes abstraktes Ordnungsmerkmal dem jeweiligen personenbezogenen Meldedatensatz beigegeben werden. Dies hätte im automatisierten Verfahren im Zuge des Versendens oder Empfangens des personenbezogenen Meldedatensatzes zu erfolgen. Dieser Prozess sollte für die am Meldevorgang beteiligten Mitarbeiter nicht sichtbar sein. Die Generierung und das Management der bereichsspezifischen Ordnungsmerkmale müssen von einer unabhängigen Vertrauensstelle bei der Registerbehörde nach mathematisch sicherem Algorithmus vorgenommen werden. Eine Speicherung der generierten Ordnungsmerkmale darf im BMR nicht stattfinden.

Das BMI hat erklärt, dass es ein Identitätsmanagement bei einer Reform des Meldewesens konzeptionell vorsehen und gesetzlich absichern wolle.

6.6 Bürgerportale: Elektronischer Königsweg zur Verwaltung?

Die E-Mail ist ein einfaches, schnelles, oft kostenloses und ortsunabhängiges Massenkommunikationsmittel. Sie wird privat ebenso selbstverständlich genutzt wie in der Kommunikation mit Behörden und Geschäftspartnern. Allerdings mangelt es häufig an der Vertraulichkeit und Verlässlichkeit dieses Kommunikationsweges.

So kann eine E-Mail abgefangen, mitgelesen oder inhaltlich verändert werden. Außerdem können Sender und Empfänger nie sicher sein, mit wem sie tatsächlich kommunizieren. Um dem abzuhelfen, soll die Infrastruktur für eine sichere E-Mail-Kommunikation und für sichere Datenspeicher geschaffen werden. Unter dem Namen Bürgerportalgesetz hat die Bundesregierung hierzu einen Gesetzentwurf vorgelegt. Bürgerportale sollen die Vertraulichkeit, Integrität und Authentizität gewährleisten (s. Kasten zu Nr. 6.6). Im Gesetzentwurf werden die Anforderungen solcher Systeme im Hinblick auf die IT-Sicherheit, den Daten- und Verbraucherschutz festgelegt. Jede natürliche oder juristische Person soll auf Wunsch eine so genannte De-Mail-Adresse erhalten können. Zusätzlich wird eine sichere Dokumentenablage (De-Safe) beschrieben.

Das Gesetz definiert neben den rechtlichen Rahmenbedingungen die technischen Grundlagen. Realisierung und Betrieb der De-Mail oder des De-Safe obliegen allein privaten Unternehmen. Die Möglichkeit steht allen Unternehmen offen. Sie müssen in einem staatlichen Akkreditierungsverfahren nachweisen, dass sie bestimmte Anforderungen an Sicherheit, Datenschutz und Verbraucherschutz erfüllen.

Grundsätzlich begrüße ich diese Bemühungen. Zwar ermöglicht bereits die elektronische Signatur nach dem Signaturgesetz ein hohes Maß an Sicherheit. Leider sind

aber seit vielen Jahren die Angebote und Nutzungszahlen bei der elektronischen Signatur nicht vorangekommen, so dass diese Infrastruktur bis heute nicht in ausreichender Breite zur Verfügung steht.

Kasten zu Nr. 6.6

Bürgerportalgesetz

Ziel des Entwurfs eines Gesetzes zur Regelung von Bürgerportalen und zur Änderung weiterer Vorschriften ist,

- einen Rechtsrahmen zur Einführung vertrauenswürdiger Bürgerportale im Internet zu schaffen, der für Diensteanbieter Rechtssicherheit schafft und es ihnen ermöglicht, die Rechtsqualität der als Bürgerportaldienste erfassten Dienste im Internet zu steigern,
- für die elektronische Kommunikation im Rechts- und Geschäftsverkehr vertrauenswürdige Lösungen zu schaffen, bei denen sich die Teilnehmer der Sicherheit der Dienste, der Vertraulichkeit der Nachrichten und der Identität ihrer Kommunikationspartner sicher sein können,
- die Rechtssicherheit im elektronischen Rechts- und Geschäftsverkehr durch verbesserte Beweismöglichkeiten zu stärken,
- die Möglichkeiten elektronischer Kommunikation fortzuentwickeln, indem eine Zustellung und eine Bestätigung des Zugangs auch für elektronische Erklärungen ermöglicht wird,
- den (freiwilligen) Eintrag einer elektronischen Bürgerportaladresse in ein Melderegister zu ermöglichen und dadurch eine Möglichkeit der elektronischen Zugangseröffnung für alle Behörden zu schaffen.

Im weiteren Gesetzgebungsverfahren sind folgende wichtige Punkte noch zu verbessern:

1. Die Feststellung der Identität der Nutzer und die Verwendung und Aufdeckung von Pseudonymen sind nicht eindeutig geregelt. Der Eintrag einer De-Mail-Adresse ins Melderegister und die Folgen müssen für Bürger und Bürgerinnen erkennbar sein. Niemand darf benachteiligt werden, wenn er den Dienst nicht in Anspruch nimmt.

2. Da der Nachweis des Absenders nur durch die Anmeldung am Bürgerportal erfolgt, kann der Absender einer De-Mail nicht sicher bestimmt werden. So wäre die Versendung von De-Mail ohne Einwirken einer Person allein durch einen Trojaner, der sich auf dem PC des Nutzers eingenistet hat, möglich. In gleicher Weise könnten auch die Daten im De-Safe gelöscht oder verändert werden. Hier müssen geeignete Gegenmaßnahmen vorgesehen werden.

3. Der Entwurf sieht keine Ende-zu-Ende-Verschlüsselung vor. Zwar werden die Diensteanbieter zertifiziert und ihre Kommunikation untereinander soll verschlüsselt erfolgen, dennoch ist ein Mitlesen der Nachrichten bei den Anbietern weiterhin möglich. Hier müssen (mindestens optional) sichere Verschlüsselungsverfahren angeboten werden, so dass eine vertrauliche Ende-zu-Ende-Kommunikation zwischen Sender und Empfänger möglich ist.

4. Die Prüfung der Anbieter setzt Regelungen zur Gewährleistung eines hohen Datenschutzniveaus bei den Anbietern voraus. Die Mindestanforderungen für das Audit müssen einheitlich für alle Anbieter vorgegeben werden. Von daher bietet sich eine Verzahnung mit dem Entwurf zum Datenschutzauditgesetz an (s. auch unter Nr. 2.4).

Die Bundesregierung verfolgt weitere E-Government-Projekte mit ähnlichen Zielen. Z. B. laufen bei der Justiz Projekte zu „Elektronischen Gerichts- und Verwaltungspostfächern“. Andere Projekte sehen die Ausgabe von Chipkarten mit Authentisierungs- und Signaturfunktionen vor. Zudem soll auch der elektronische Personalausweis (E-Personalausweis) eine sichere Identifikation bei Internet-Diensten ermöglichen (s. auch o. Nr. 6.3.2). Alle diese Maßnahmen müssen eng miteinander verzahnt werden, um Sicherheitsrisiken zu reduzieren und eine Doppelerfassung von Daten zu verhindern.

6.7 RFID (Radio Frequency Identification)

Immer noch fehlt eine wirksame Selbstverpflichtung der Wirtschaft oder eine gesetzliche Regelung zum Einsatz von Funkchips.

Im letzten Tätigkeitsbericht (21. TB Nr. 4.3) habe ich bereits ausführlich über die RFID-Technologie, ihre Gefahren für die Persönlichkeitsrechte und die rechtlichen Möglichkeiten ihrer Begrenzung berichtet.

Im Januar 2008 hat die Bundesregierung auf Aufforderung des Deutschen Bundestages einen Bericht über die Aktivitäten, Planungen und den möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie vorgelegt (Bundestagsdrucksache 16/7891). Die Bundesregierung erkennt darin an, dass der Einsatz von RFID im Verbraucherbereich Gefahren für das Recht auf informationelle Selbstbestimmung in sich birgt. Sie hält es für erforderlich, den Gefährdungen präventiv zu begegnen. Dies könne auf gesetzgeberischer Ebene durch Ergänzung des BDSG oder über eine bereichsspezifische Vorschrift zum Umgang mit der RFID-Technologie erfolgen. Die Bundesregierung würde aber einer verbindlichen Selbstverpflichtung der Wirtschaft und einer Förderung datenschutzfreundlicher Technologien den Vorzug geben. Nur für den Fall, dass eine solche Selbstverpflichtung nicht oder nicht zufrieden stellend zustande kommt, zieht sie gesetzgeberische Maßnahmen in Betracht. Das BMI hat zudem das BSI beauftragt, „Technische Richtlinien für den RFID-Einsatz“ zu erstellen.

Der Bestandsaufnahme der Bundesregierung sowie den daraus gezogenen Schlussfolgerungen für den künftigen Handlungsbedarf kann ich grundsätzlich zustimmen. Die von den Datenschutzbeauftragten in Bund und Ländern erhobenen datenschutzrechtlichen Forderungen (vgl. 21. TB, Kasten zu Nr. 4.3) könnten auf diese Weise umgesetzt werden. Eine Selbstverpflichtung der Wirtschaft halte ich dann für akzeptabel, wenn dafür bestimmte Bedingungen erfüllt sind:

So muss überhaupt eine möglichst breite Beteiligung der Unternehmen sichergestellt sein, damit sich ein hoher Standard flächendeckend am Markt durchsetzen kann. Die durch eine Selbstverpflichtung definierten Anforderungen müssen für die Unternehmen verbindlich gelten. Weiterhin müssen effektive Instrumente vorgesehen werden, um diese Anforderungen gegebenenfalls durchsetzen zu können. Schließlich halte ich es für unabdingbar, dass – vor allem im Handel – eine Pflicht zur automatischen Deaktivierung von RFID-Chips an der Kasse („point of sale“) vorgesehen wird. Die Sendefunktion der RFID-Chips würde nur dann aktiviert, wenn die Nutzer dies ausdrücklich wünschen (sog. Opt-in-Lösung).

Sollten diese Bedingungen nicht erfüllt sein, ist der Gesetzgeber gefordert, durch entsprechende Ergänzungen des Datenschutzrechts Abhilfe zu schaffen. Das Gleiche gilt erst recht, wenn eine Selbstverpflichtung nicht zustande kommt.

Auch auf europäischer Ebene wurde der Konsultationsprozess der Europäischen Kommission fortgesetzt. Der Europäische Datenschutzbeauftragte hat sich dabei ebenso wie andere Datenschutzbehörden aus Deutschland und Europa für die Schaffung gesetzlicher Regeln ausgesprochen, die ein striktes Opt-in-Prinzip sowie die Förderung datenschutzfreundlicher Technologien vorschreiben.

Angesichts des offensichtlichen Stillstands bei der Realisierung einer wirksamen Selbstverpflichtung erwarte ich von der Bundesregierung, dass sie nun die erforderlichen gesetzlichen Regelungen in Angriff nimmt. Offenbar ist dies der einzige Erfolg versprechende Weg, die Verbraucherinnen und Verbraucher gegen die mit der Einführung der RFID-Technologie verbundenen Risiken zu schützen.

7 Internet

7.1 Geoinformationen und Datenschutz

Heute ist eine präzise elektronische Lokalisierung von Personen und Gegenständen für jedermann möglich. Unternehmen haben ein erhebliches Interesse an der Verwertung und Aufbereitung von solchen Geoinformationen. Auch die öffentliche Verwaltung erzeugt und nutzt Geodaten in vielfältiger Weise.

Der Umgang mit Geodaten wirft eine Reihe neuer rechtlicher Fragen auf, darunter solche des Datenschutzes. Geoinformationen geben nicht nur Aufschluss über bestimmte Eigenschaften an einem Ort oder in einem Gebiet. Angaben über den Wohn- und Aufenthaltsort von Personen oder Gegenständen können mit weiteren Informationen verknüpft und für Zwecke der Werbung (Geomarketing) oder der Einschätzung der Kreditwürdigkeit (Geo-Scoring) genutzt werden (s. dazu auch Nr. 2.3). Der Arbeitskreis „Grundsatzfragen der Verwaltungsmodernisierung“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich deshalb eingehend mit datenschutzrechtlichen Aspekten des Umgangs mit Geodaten beschäftigt.

Zunächst ist zu klären, inwieweit die jeweiligen Geoinformationen als personenbezogene Daten zu betrachten sind. Ein Personenbezug ist nicht nur dann gegeben, wenn – z. B. bei Straßenansichten im Internet (vgl. Nr. 7.2) – identifizierbare Personen abgebildet werden. Personenbezogen sind regelmäßig auch Informationen, die etwa einem bestimmten Grundstück und damit der Person des Eigentümers oder Bewohners zugeordnet werden können. Ziel der Beratungen im Arbeitskreis ist es, Kriterien aufzustellen, bei welchen Inhalten, ab welchem Maßstab und ab welcher Auflösung die Daten als direkt oder indirekt personenbezogen anzusehen sind.

Sofern Geoinformationen personenbezogen sind, ist in einem zweiten Schritt jeweils zu prüfen, ob es sich um Daten aus allgemein zugänglichen Quellen handelt. Bei solchen Daten sieht das BDSG ebenso wie andere Datenschutzgesetze nur geringe Beschränkungen für ihre Erhebung, Verarbeitung und Nutzung vor, insbesondere ist die Zweckbindung stark gelockert. Aus der Tatsache, dass der Luftraum frei zugänglich ist, kann jedoch nicht einfach geschlossen werden, dass sämtliche aus der Luft erhebbaren Informationen allgemein zugänglich sind. Auch hier sind der Inhalt und die Beschaffenheit der Informationen entscheidend: Beispielsweise können Informationen über die topografische Beschaffenheit oder das Klima unabhängig vom Personenbezug als allgemein zugänglich betrachtet werden und sind daher nahezu unbeschränkt verwertbar.

Im Berichtszeitraum war die Umsetzung der europäischen INSPIRE-Richtlinie (Richtlinie 2007/2/EG vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft, Abl. L 108 S. 1) in nationales Recht zentrales Thema des Arbeitskreises. Der Bund hat hierzu ein Gesetz über den Zugang zu digitalen Geodaten (Geodatenzugangsgesetz – GeoZG) verabschiedet, das am 14. Februar 2009 in Kraft getreten ist (BGBl. I 2009 S. 278). Die auf dieser Grundlage angestrebte einheitliche europäische Geodateninfrastruktur soll öffentlichen und privaten Nutzern einen einheitlichen, standardisierten Zugang zu Geodaten ermöglichen, wobei die Interoperabilität der bereitgestellten Geoinformationen auf allen staatlichen Ebenen zu gewährleisten ist. Dies bedeutet z. B., dass die verwendeten Koordinatenreferenzsysteme zur eindeutigen räumlichen Bezeichnung, geografische Bezeichnungen, Verwaltungseinheiten, Flur- bzw. Grundstücke oder Verkehrsnetze technisch so standardisiert bereitgestellt werden müssen, dass sie von Bund, Ländern, Kommunen, aber auch Stellen in anderen europäischen Staaten verarbeitet und mit anderen Daten kombiniert werden können. Der Anwendungsbereich des GeoZG ist aus Kompetenzgründen auf Stellen des Bundes beschränkt; die Länder müssen die INSPIRE-Richtlinie deshalb in eigenen Gesetzen umsetzen.

Kasten zu Nr. 7.1

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008

Datenschutzgerechter Zugang zu Geoinformationen

Die Einführung einer einheitlichen Geodateninfrastruktur und die Veröffentlichung der staatlichen Daten eröffnen ein großes Potential an volkswirtschaftlichem Nutzen und ist geeignet, vielen E-Government- und E-Commerce-Anwendungen die erforderliche Infrastruktur zur Verfügung zu stellen. Als einen ersten Schritt regelt das europäische Recht mit der so genannten INSPIRE-Richtlinie, die bis Mai 2009 in nationales Recht umgesetzt werden muss, die Bereitstellung von amtlichen Geodaten nach einheitlichen Standards für europaweite behördliche, kommerzielle und private Nutzungen.

Durch diese neue Infrastruktur werden georeferenzierbare Angaben auf Grund der Erschließungsmöglichkeit über Wohnanschriften oder Eigentümer- bzw. Standortdaten als personenbezogene Daten zur Verfügung gestellt. Diesem Umstand müssen die gesetzlichen Regelungen gerecht werden und angemessene Datenschutzregelungen enthalten.

Bei der Bereitstellung amtlicher Geodaten ist sowohl nach der europäischen Richtlinie als auch nach deutschem Verfassungsrecht der Schutz personenbezogener Daten angemessen zu gewährleisten. Der Entwurf der Bundesregierung zur Umsetzung dieser Richtlinie in einem Geodatenzugangsgesetz (Bundestagsdrucksache 16/10530) sieht eine entsprechende Anwendung der Schutzvorschriften des Umweltinformationsgesetzes vor. Im Gegensatz zum einzelfallbezogenen Zugang nach den Umweltinformationsgesetzen birgt der im Entwurf eines Geodatenzugangsgesetzes vorgesehene massenhafte Abruf solcher Daten aber ein höheres datenschutzrechtliches Gefährdungspotenzial. Der Verweis auf das Umweltinformationsgesetz ist nach Ansicht der Konferenzen der Datenschutz- und der Informationsfreiheitsbeauftragten des Bundes und der Länder deshalb nicht interessengerecht. Ein Geodatenzugangsgesetz muss einen differenzierenden Ausgleich zwischen Informations- und Schutzinteressen für die spezielle Problematik der Geobasis- und der Geofachdaten vornehmen. Es ist insbesondere zu berücksichtigen, dass nach der INSPIRE-Richtlinie die Zugangsmöglichkeit eingeschränkt werden soll, wenn der Zugang nachteilige Auswirkungen auf die Vertraulichkeit personenbezogener Daten haben kann.

Beim Zugang der Öffentlichkeit zu Geodaten nach dem GeoZG wird auf Regelungen im Umweltinformationsgesetz (UIG) verwiesen. Der Zugang zu personenbezogenen Daten darf danach nur versagt werden, wenn Interessen der Betroffenen erheblich beeinträchtigt würden. Die Übernahme der Zugangsregelungen aus dem Umweltinformationsrecht verkennt, dass beim Zugang zu Geodaten nach dem GeoZG ein höheres Gefährdungspotential für das Recht auf informationelle Selbstbestimmung gegeben ist: Während der Zugang nach dem UIG grundsätzlich nur auf Antrag im Einzelfall gewährt wird, stehen die Geodaten nach dem GeoZG für einen massenhaften Abruf zur Verfügung. Der Verweis auf das UIG ist deshalb nicht angemessen und lässt die in der INSPIRE-Richtlinie vorgesehenen weiteren Möglichkeiten zum Schutz der Persönlichkeitsrechte unberücksichtigt (s. Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008, Kasten zu Nr. 7.1)

7.2 Ihr Haus im Internet?

Den Dienst „Street View" bietet der Suchmaschinenkonzern Google seinen Nutzern als Ergänzung seines Stadtplandienstes „Google Maps" an. Mit der Erweiterung können Anwender virtuell durch die Häuserzeilen von Städten wandern. Dies bleibt nicht ohne Auswirkungen auf die Persönlichkeitsrechte von Eigentümern, Bewohnern und abgebildeten Personen.

In den USA zeigt der Dienst schon jetzt aus der Bodenperspektive 360-Grad-Ansichten von Straßen in über 40 Städten und hat auch dort wegen potenzieller Verletzung der Privatsphäre für Diskussionen gesorgt. In den USA ist das Ablichten von Straßenszenen legal, nur Detailaufnahmen von öffentlichen Plätzen sind nicht erlaubt. Google plant nun diesen Service auch auf europäische Großstädte auszudehnen. In Deutschland sind die Kamerawagen von Google schon in München, Berlin und Frankfurt am Main unterwegs gewesen.

Vergleichbare Daten sind zwar schon vor Jahren angeboten worden, allerdings per CD. Bereits damals haben sich hieran datenschutzrechtliche Diskussionen entzündet (vgl. 18. TB Nr. 31.3). Neu ist an „Street View", dass diese Daten kostenlos weltweit online verfügbar gemacht werden sollen. Das hat erhebliche datenschutzrechtliche Auswirkungen.

In mit dem Diensteanbieter geführten Diskussionen habe ich deutlich gemacht, dass das Unternehmen die Persönlichkeitsrechte wahren muss. Das heißt in erster Linie, dass die Personen so verfremdet werden, dass sie nicht identifiziert werden können. Dies gilt auch für zufällig ins Bild geratene Personen, da auch in diesem Falle personenbezogene Daten erhoben werden. Ein Personenbezug ist selbst dann gegeben, wenn nur wenige Betrachter die dargestellten Personen identifizieren können. So sind in Abhängigkeit von besonderen Eigenschaften einer aufgenommenen Person (z. B. ein auffälliges äußeres Erscheinungsbild) Fälle denkbar, in denen nach sozialüblichen Maßstäben nicht ausgeschlossen werden kann, dass sogar Google einen Personenbezug herstellen kann. Auch der Bildkontext kann die Identifizierung erleichtern, etwa wenn eine Person in ihrem Wohn- oder Arbeitsumfeld aufgenommen wird.

Zudem kann eine Unkenntlichmachung technisch – zumindest derzeit – noch nicht vollständig umgesetzt werden. Google hat angekündigt, die in Aufnahmen dargestellten Personen sowie KfZ-Kennzeichen besser un-

kenntlich zu machen. Die bisher dazu eingesetzte Software funktioniert noch nicht fehlerfrei.

Schließlich ist zu berücksichtigen, dass es sich auch bei den abgebildeten Gebäude- und Grundstücksansichten um personenbezogene Daten handeln kann. Die schutzwürdigen Interessen der Eigentümer oder Bewohner müssen bei der Entscheidung über die Veröffentlichung berücksichtigt werden. Die im Düsseldorfer Kreis zusammengeschlossenen obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben deshalb gefordert, dass Eigentümer und Bewohner die Möglichkeit erhalten, einer Veröffentlichung der sie betreffenden Ansichten zu widersprechen. (s. Kasten zu Nr. 7.2).

Kasten zu Nr. 7.2

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 13./14. November 2008

Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet

Bei digital erfassten Fotos von Gebäude- und Grundstücksansichten, die über Geokoordinaten eindeutig lokalisiert und damit einer Gebäudeadresse und dem Gebäudeeigentümer sowie den Bewohnern zugeordnet werden können, handelt es sich in der Regel um personenbezogene Daten, deren Erhebung und Verarbeitung nach dem Bundesdatenschutzgesetz zu beurteilen ist. Die Erhebung, Speicherung und Bereitstellung zum Abruf ist nur zulässig, wenn nicht schutzwürdige Interessen der Betroffenen überwiegen. Bei der Beurteilung schutzwürdiger Interessen ist von Bedeutung, für welche Zwecke die Bilddaten verwendet werden können und an wen diese übermittelt bzw. wie diese veröffentlicht werden. Die obersten Aufsichtsbehörden sind sich einig, dass die Veröffentlichung von georeferenziert und systematisch bereit gestellten Bilddaten unzulässig ist, wenn hierauf Gesichter, Kraftfahrzeugkennzeichen oder Hausnummern erkennbar sind. Den betroffenen Bewohnern und Grundstückeigentümern ist zudem die Möglichkeit einzuräumen, der Veröffentlichung der sie betreffenden Bilder zu widersprechen und dadurch die Bereitstellung der Klarbilder zu unterbinden. Keine schutzwürdigen Interessen bestehen, wenn die Darstellung der Gebäude und Grundstücke so verschleiert bzw. abstrakt erfolgt, dass keine individuellen Eigenschaften mehr erkennbar sind. Um die Möglichkeit zum Widerspruch schon vor der Erhebung zu eröffnen, sollte die geplante Datenerhebung mit einem Hinweis auf die Widerspruchsmöglichkeit rechtzeitig vorher bekannt gegeben werden. Die Widerspruchsmöglichkeit muss selbstverständlich auch noch nach der Veröffentlichung bestehen.

Die datenschutzrechtliche Aufsicht wird federführend von dem für die deutsche Niederlassung von Google zuständigen Hamburgischen Datenschutzbeauftragten ausgeübt. Da verschiedene Städte betroffen sind, wird es aber ein Thema bleiben, über das alle Datenschutzaufsichtsbehörden, unabhängig von der unmittelbaren Zuständigkeit, zu beraten haben, um zu einem einheitlichen Ergebnis zu kommen.

7.3 „Super Nanny“ Datenschutz?

Soziale Netzwerke verändern unsere Art der Kommunikation mit der Außenwelt. Exhibitionismus scheint dabei eines ihrer Wesensmerkmale zu sein. Kann ich nur virtuell kommunizieren, wenn ich möglichst viel über mich preisgebe? Ist das die Zukunft des Web 2.0?

Jeder muss selbst entscheiden, wie viel er oder sie von sich preisgeben möchte. Der Datenschutz will hier kein Kindermädchen sein – auch nicht bei der Nutzung des Internets. Doch wer gar nicht die Tragweite seiner Entscheidung überblickt, weil er die „Privatsphäre“-Einstellungen seines sozialen Netzwerkes nicht versteht, kann sich auch nicht wirksam schützen. Die Anbieter dürfen sich daher nicht hinter dem Argument der Selbstbestimmung der Nutzer verstecken. Es ist an ihnen, die Selbstbestimmung durch geeignete technische Vorkehrungen zu ermöglichen. Standards zu definieren, ist hier längst keine nationale Aufgabe mehr. National wie international haben sich Datenschutzaufsichtsbehörden daher Gedanken dazu gemacht, welche Kriterien für datenschutzfreundliche Netzwerke gelten sollen. Schlagwortartig möchte ich diese „Zehn Gebote“ allen Betreibern sozialer Netzwerke ins Stammbuch schreiben (s. Kasten zu Nr. 7.3).

Kasten zu Nr. 7.3

Die Zehn Gebote für Betreiber sozialer Netzwerke

1. Beachten Sie die Vorgaben des Datenschutzrechts
2. Klären Sie Ihre Nutzer verständlich und offen über den Umgang mit ihren Daten auf
3. Geben Sie Ihren Nutzern mehr Kontrolle über die Verwendung ihrer Profil- und Verkehrsdaten
4. Bieten Sie datenschutzfreundliche Standardeinstellungen an
5. Verbessern Sie kontinuierlich die Sicherheit Ihrer Informationssysteme
6. Jedermann hat ein Recht auf Auskunft über seine personenbezogenen Daten in einem Netzwerk – egal ob er oder sie Mitglied ist oder nicht
7. Profile müssen einfach und vollständig zu löschen sein
8. Ermöglichen Sie die Nutzung Ihrer Dienste unter Pseudonym
9. Verhindern Sie, dass Profildaten Ihrer Nutzer von Dritten kopiert werden
10. Stellen Sie sicher, dass Daten Ihrer Nutzer von externen Suchmaschinen nur dann gefunden werden können, wenn die Betroffenen zuvor ausdrücklich eingewilligt haben

Wichtig ist aber auch das Bewusstsein der Online-Generation im Umgang mit ihrer Privatsphäre zu schärfen. Ermutigend ist dabei, dass im letzten Jahr der Informationsbedarf zum Datenschutz im Internet deutlich zugenommen hat. Dies belegt eine Sonderstudie von TNS Infratest im Auftrag von Microsoft (www.nonliner-atlas.de). Das erforderliche Wissen zu vermitteln wird eine kontinuierliche Aufgabe bleiben.

7.4 Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums in Kraft

Seit dem 1. September 2008 können Rechteinhaber vom Provider Auskunft über die Identität möglicher „Internet-Piraten" verlangen. Die Musik- und Filmindustrie drängt aber bereits auf weitere Zugeständnisse.

In meinem letzten TB (Nr. 6.5) hatte ich über den Gesetzentwurf der Bundesregierung zur Umsetzung der sog. IPR-Enforcement-Richtlinie (Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums) berichtet. Am 1. September 2008 ist das Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums vom 7. Juli 2008 (BGBl. I 2008, S. 1191) in Kraft getreten.

Es gewährt den Rechteinhabern, wie insbesondere der Musik- und Filmindustrie mit Blick auf „Piraterie" in Internet-Tauschbörsen, nunmehr einen zivilrechtlichen Auskunftsanspruch gegen die Internet-Zugangsprovider, um mögliche Rechteverletzer zu ermitteln, § 101 Urheberrechtsgesetz (UrhG). Damit erübrigt sich das bisherige Vorgehen der Rechteinhaber, über das Akteneinsichtsrecht im strafrechtlichen Ermittlungsverfahren, § 406e StPO, an die Daten zur Identifizierung des Nutzers zu gelangen.

Die Auskunftserteilung setzt nach § 101 Absatz 9 UrhG eine richterliche Anordnung voraus. Diese Hürde ist aus verfassungsrechtlicher Sicht unabdingbar, denn den Providern ist die Auskunftserteilung nur mittels der sog. dynamischen IP-Adressen, die jedes Mal vergeben werden, wenn sich Nutzer neu in das Internet einwählen, möglich. Hierbei handelt es sich um Verkehrsdaten im Sinne des § 3 Nummer 30 Telekommunikationsgesetz (TKG), die dem Schutz des Fernmeldegeheimnisses aus Artikel 10 GG unterliegen. Diese Daten zugunsten privatrechtlicher Interessen ohne weiteres zugänglich zu machen, wäre das falsche Signal. Damit würde einseitig dem Anliegen der Rechteinhaber nachgegeben, ohne dies mit den berechtigten, grundrechtlich geschützten Interessen der Nutzer in Einklang zu bringen. Dies wäre mit dem Grundsatz der Verhältnismäßigkeit nicht vereinbar.

Gleiches gilt für den vielfach geforderten Rückgriff auf die sog. Vorratsdaten (vgl. Nr. 3.2.1) zur Auskunftserteilung an Rechteinhaber. Der Gesetzgeber hat bei der Umsetzung der Richtlinie zur Vorratsdatenspeicherung deren Verwendung ausdrücklich auf Zwecke der Strafverfolgung und der Gefahrenabwehr, § 113b Absatz 1 Satz 1 TKG, beschränkt. Damit ist aber eine Erstreckung auf zivilrechtliche Auskunftsansprüche, wofür sich im Gesetzgebungsverfahren noch der Rechtsausschuss des Bundesrates ausgesprochen hatte (Bundesratsdrucksache 798/1/07), ausgeschlossen. Durch die höchstrichterliche Begrenzung der derzeitigen Nutzung der auf Vorrat zu speichernden Daten auf schwere Katalogstraftaten gemäß § 100a Absatz 2 StPO (Beschluss des BVerfG vom 11. März 2008, 1 BvR 256/08), dürfte einer weiteren Diskussion in diese Richtung ohnehin die Grundlage entzogen sein.

Demnach dürfen nur die von den Anbietern von Telekommunikationsdiensten unter den Voraussetzungen der §§ 96 ff. TKG für eigene Zwecke gespeicherten Daten zur Auskunftserteilung an Rechteinhaber genutzt werden. Dass dieser Anspruch nicht – wie vielfach behauptet – von vornherein ins Leere läuft, belegen erste Zivilgerichtsurteile zum Auskunftsanspruch.

Dennoch sind bereits neue Forderungen der Musik- und Filmindustrie im Raum. Nach dem Vorbild einiger EU-Staaten wie z. B. Frankreich (sog. Olivennes-Vereinbarung) stellt sie sich in Kooperation mit den Providern Modelle vor, die über ein abgestuftes Verfahren Urheberrechtsverstöße verhindern bzw. eindämmen sollen. Zunächst soll dabei der potentielle Verletzer ermittelt werden, indem die im Auftrag der Rechteinhaber erhobene IP-Adresse mit den Bestandsdaten beim Provider abgeglichen wird. Der so ermittelte potentielle Verletzer soll in einer Art Mahnverfahren einen Warnhinweis vom Provider erhalten. Begeht er trotzdem weitere Verstöße, so können Sanktionen vorgesehen werden. Diese sollen nach den Vorstellungen der Rechteinhaber von der vorübergehenden Sperrung des Anschlusses bis hin zur Kündigung des Vertrages und einer befristeten Vertragssperre reichen.

Für diese Verwendung der Verkehrdaten für Mahnungen „auf Zuruf" der Rechteinhaber gibt es keine Rechtsgrundlage. Weder das TKG noch der o. g. zivilrechtliche Auskunftsanspruch in § 101 UrhG, der neben der richterlichen Anordnung offensichtliche Rechtsverletzungen in gewerblichem Ausmaß voraussetzt, erlaubt den Providern dieses Vorgehen zur Identifikation von Internet-Nutzern.

Klärungsbedarf sehe ich auch für die Frage der Zulässigkeit der Ermittlung der IP-Adresse, die Voraussetzung für die Identifizierung der Nutzer ist. Diese erfolgt z. B. durch Spähdateien, die vorgeben, die Verknüpfung zu bestimmten vom Tauschbörsennutzer gesuchten Medien zu enthalten, in Wahrheit aber nur die IP-Adresse des Interessenten ermitteln. Ein Herunterladen z. B. von Musikstücken findet also tatsächlich nicht statt. Im anderen Fall werden Tauschbörsen anhand der Prüfsumme der urheberrechtlich geschützten Dateien abgesucht. Mit dem Rechner, der die gesuchten Dateien in seinem offenen Ordner vorhält, ist auch die jeweilige IP-Adresse ermittelt. Auch hier handelt es sich um die heimliche Erhebung der IP-Adressen von Tauschbörsenteilnehmern mit dem Ziel der anschließenden zweckfremden Verwendung dieser Daten.

Auch ich kann das legitime Interesse der Musik- und Filmindustrie, gegen Urheberrechtsverletzungen im Internet vorzugehen, durchaus nachvollziehen. Die Mittel müssen aber verhältnismäßig sein, den Interessen der Rechteinhaber und dem Schutz des Fernmeldegeheimnisses sowie sonstiger Verfassungsgüter also gleichermaßen Rechnung tragen.

7.5 Die Jobbörse als Internet-Angebot der Bundesagentur für Arbeit

Die Jobbörse stellt als Teil des „Virtuellen Arbeitsmarktes" ein Verfahren der Arbeitsverwaltung dar, das nur durch das Internet ermöglicht wird.

Bereits in meinem 20. Tätigkeitsbericht (Nr. 16.2) habe ich über das Projekt „Virtueller Arbeitsmarkt" (VAM) berichtet, in dem die Bundesagentur für Arbeit (BA) ihre Online-Vermittlungs-Angebote durch das Serviceportal „Arbeitsagentur.de" ersetzt hat. Im aktuellen Berichtszeitraum habe ich mir die Jobbörse vor Ort in einer Agentur für Arbeit angesehen.

Die sog. Jobbörse mit derzeit ca. 2,5 Millionen Nutzern steht als Selbstbedienungsplattform für Arbeitgeber und Arbeit- bzw. Ausbildungsplatzsuchende jedem zur Einsichtnahme in Stellen- und Bewerberangebote zur Verfügung. Die Nutzer müssen sich bei der BA registrieren lassen. Sie müssen neben Angaben zur Person hierzu einen Benutzernamen sowie ein selbst gewähltes Kennwort hinterlegen. Ob diese Angaben stimmen, wird jedoch in keiner Weise überprüft. Danach erhält der Nutzer per Post eine PIN übersandt, mit der er die Gültigkeit seiner Registrierung verifizieren kann. Registrierte Nutzer können beim Einstellen ihrer Angebote die Unterstützung und Betreuung der Agentur für Arbeit in Anspruch nehmen.

Ich habe die BA darauf hingewiesen, dass bei diesem Verfahren praktisch jedem möglich ist, sich als Arbeitgeber registrieren zu lassen und ein u.U. unseriöses Stellenangebot zu veröffentlichen. Dies sehe ich kritisch. Im Rahmen von Vermittlungsvorschlägen dürfen Sozialdaten nicht an unseriöse Anbieter übermittelt werden. Diese Gefahr sehe ich insbesondere mit Blick auf die durch das Gesetz zur Neuausrichtung der arbeitsmarktpolitischen Instrumente vom 21. Dezember 2008 (BGBl. I 2008 S. 2917) erfolgte Änderung. Hiernach sind auch die in der Jobbörse eingestellten Stellenangebote von Arbeitgebern, die nicht von der Agentur betreut werden, Arbeitsuchenden verbindlich, d. h. mit der Möglichkeit von Sanktionen (§ 144 Absatz 1 Satz 2 Nummer 2 SGB III), zu unterbreiten.

Eine Kontaktaufnahme zwischen Bewerbern und Arbeitgebern wird durch eine Postfachfunktion und die neue sog. Call-Me-Funktion ermöglicht. Mit der „Call-Me-Funktion" können registrierte Bewerber sich von potenziellen Arbeitgebern anrufen lassen, ohne ihre eigene Telefonnummer angeben zu müssen. Dies geschieht durch Aktivierung einer entsprechenden Funktion in ihrem Bewerberprofil. Durch das „Call-Me-Symbol" im Bewerberprofil wird angezeigt, dass der Nutzer zugestimmt hat. In der Jobbörse registrierte Arbeitgeber können nun mit einem Klick auf das „Call-Me-Symbol" eine verschlüsselte Rufnummer anfordern. Mit ihr kann ein Arbeitgeber einen Bewerber per Rufumleitung innerhalb von 48 Stunden anrufen. Datenschutzrechtlich bedenklich ist in diesem Zusammenhang, dass die Wahrung der Anonymität nicht immer gewährleistet ist. Dies gilt vor allem bei Anrufbeantwortern mit persönlichen Ansagetexten oder bei Rückruf eines Arbeitgebers durch einen interessierten Bewerber, wenn die Rufnummernübertragung seines Anschlusses aktiviert ist. Auch kann derzeit nicht ausgeschlossen werden, dass unseriöse Anbieter diese Funktion zur Kontaktaufnahme nutzen können. Solange dies nicht durch Maßnahmen der Qualitätssicherung weitgehend auszuschließen ist, sollten die Bewerber im Rahmen der Aktivierung der „Call-Me-Funktion" hierauf explizit hingewiesen werden.

Die BA hat meine Kritik aufgegriffen und eine Klarstellung zur Nutzung der „Call-Me-Funktion" in Form einer zusätzlichen Handlungsempfehlung/Geschäftsanweisung für die Agenturen erlassen. Ein entsprechender Warnhinweis, dass auch unseriöse Anbieter die Funktionalitäten der Jobbörse zur Kontaktaufnahme nutzen können, soll in die in Überarbeitung befindlichen neuen Nutzungsbedingungen aufgenommen werden. Darüber hinaus will die BA die Maßnahmen zur Qualitätssicherung ausbauen. Es soll in Stichproben geprüft werden, ob die Stellenangebote den rechtlichen Rahmenbedingungen entsprechen und inhaltlich seriös sind. Rechtswidrige, sowie nicht den Nutzungsbedingungen entsprechend eingestellte Stellenangebote sollen gelöscht und ggf. der Arbeitgeber-Account deaktiviert werden. Über eine Hotline können die Nutzer der Jobbörse telefonisch oder per E-Mail weiter beraten werden. Die BA kann daraufhin das Angebot sperren und sogar Abmahnverfahren oder Strafverfahren gegen die entsprechenden Nutzer einleiten. Ob diese Maßnahmen insgesamt ausreichend sind, werde ich aufmerksam verfolgen. Ein weiterer Beitrag zu Einzelfällen in der Jobbörse findet sich unter Nr. 10.5.1.

7.6 Persönliche Daten im Fokus von Suchmaschinen

Der Datenschutz bei Suchmaschinen bleibt ein datenschutzrechtlicher Schwerpunkt.

Ohne Suchmaschinen geht im Netz nichts. Jeder nutzt sie. Doch nicht nur die Nutzer erhalten Informationen über den gesuchten Begriff, sondern auch die Anbieter von Suchmaschinen erhalten eine Fülle personenbezogener Daten, denn mit jeder Suchanfrage gibt der Nutzer seine Interessen, Vorlieben und Gewohnheiten preis, die durch den Einsatz technischer Mittel in einem Profil gesammelt werden können. Insbesondere wenn Suchmaschinenbetreiber ihr Angebot um immer neue Dienste erweitern oder die Datenbestände anderer Firmen durch Kauf erwerben, wenden sich viele Bürgerinnen und Bürger an mich, die sich angesichts solcher Datenberge in einer Hand um ihre persönlichen Daten sorgen.

Diese berechtigten Sorgen haben dazu beigetragen, dass der Datenschutz bei Suchmaschinen zu einem der wichtigsten Themen von nationalen und internationalen Da-

tenschutzgremien geworden ist. Nach der 28. Internationalen Datenschutzkonferenz (vgl. 21. TB Nr. 10.10) hat die Artikel-29-Gruppe im April 2008 ein Positionspapier (WP 148) mit Anforderungen an Suchmaschinen veröffentlicht. Vorausgegangen war die schriftliche Befragung mehrerer Anbieter von nationalen und internationalen Suchmaschinen zu deren Datenschutzpolitik. Die Auswertung der Antworten und ihre anschließende datenschutzrechtliche Bewertung bildeten die Grundlage für das Positionspapier, das konkrete Kernaussagen enthält (s. Kasten zu Nr. 7.6).

Mein Anliegen ist ein zumindest europaweit gültiger Datenschutzstandard für Suchmaschinen, der von allen Betreibern eingehalten wird und eine koordinierte Datenschutzaufsicht nach einheitlichen Kriterien ermöglicht.

Kasten zu Nr. 7.6

Anforderungen an Suchmaschinen

- Die Europäischen Datenschutzregelungen gelten auch für Suchmaschinen, die ihren Sitz außerhalb von Europa haben, ihren Dienst aber in Europa anbieten.
- Die EU-Richtlinie zur Vorratsdatenspeicherung (2006/24/EG, vgl. Nr. 3.2.1) gilt nicht für Suchmaschinen.
- Personenbezogene Daten, die von den Suchmaschinen erhoben werden, sind spätestens nach sechs Monaten zu löschen. Soweit Vorgaben des nationalen Rechts eine frühere Löschung verlangen, sind sie zu befolgen. In Deutschland müssen die Daten gemäß Telemediengesetz nach dem Ende der Nutzung gelöscht werden.
- Die Nutzer müssen über den Zweck der Datenverarbeitung sowie ihre Rechte auf Auskunft, Änderung und Löschung informiert werden.
- Die Verwendung der Daten für Nutzerprofile bedarf der Einwilligung des Betroffenen.

7.7 Ortung durch Handys und andere Gerätschaft

Die informationelle Selbstbestimmung schützt auch davor, dass Dritte (etwa Vorgesetzte oder Lebenspartner) heimlich und gegen den Willen der Betroffenen aufspüren können, wo man sich aufhält. Auch hier ist die moderne Technik schon einen Schritt weiter.

Bereits in der Vergangenheit (zuletzt 21. TB Nr. 10.2 und 6.4) habe ich das Thema Mobilfunkortung aufgegriffen. Dass die fortgesetzte Befassung mit diesem Thema sinnvoll ist, belegt ein im Fernsehen beworbenes Handyspiel. Da diese Werbung den Eindruck vermitteln konnte, bei dem Spiel würden die Aufenthaltsorte von Handybesitzern festgestellt, wendeten sich viele besorgte Bürger mit der Frage an mich, ob dies denn zulässig sei.

Meine Forderung an Anbieter von Handyortungsdiensten, in bestimmten Zeitabständen eine Informations-SMS an geortete Handys zu versenden, führte zwar zunächst zu einigen Diskussionen. Letztendlich versicherten die Netzbetreiber aber, dass mindestens nach jeder 10. Ortung eine Informations-SMS versandt wird. Ich begrüße es, dass die Bundesregierung inzwischen einen Gesetzentwurf zur Änderung des Telekommunikationsgesetzes (TKG – Bundestagsdrucksache 16/10731) vorgelegt hat, der darüber hinausgeht. Die Betreiber sollen verpflichtet werden, nach spätestens fünf Ortungen eine Benachrichtigungs-SMS zu versenden. Außerdem wird eine schriftliche Einwilligung des Teilnehmers gefordert.

Die technische Entwicklung zeigt, dass die Ortung über das Mobilfunknetz nur einen Teilaspekt darstellt. Durch die Satellitenortung mit GPS (Global Positioning System) können Geräte ihren Aufenthaltsort selbst bestimmen. Ein Handy mit GPS-Empfänger und der passenden Software kann Ortungsinformationen speichern oder versenden. Ein großer Handyhersteller will etwa einen Dienst anbieten, der auf der Karte die Position von Freunden und Bekannten in Echtzeit zeigt. So genannte GPS-Tracker können den Urlaubsfotos eine genaue Ortsangabe hinzufügen, die Schleichwege der Katze aufzeichnen oder aber ein Bewegungsprofil des Lebenspartners erstellen. Die Problematik wird durch die zunehmende Verbreitung der GPS-Handys und die preisgünstigeren GPS-Tracker immer dringlicher.

Eine andere Anwendung der Ortungstechnik, die von einer Stiftung initiierte Notfallortung für Rettungsleitstellen, hat für mich bisher nur ein grundsätzliches Problem erkennen lassen. Es ist schwierig festzustellen, wann dieses Verfahren angewandt werden darf. Bei dem sog. Röchelanruf bei einer Notrufnummer, bei dem der Hilfsbedürftige keine vollständigen Angaben zu seinem Aufenthaltsort machen kann, habe ich keine Zweifel. Bei der Ortung einer suizidgefährdeten Person wird eine Grenzziehung schon schwieriger. Auch ein Entführungsopfer, dessen Handy noch eingeschaltet ist, könnte so geortet und damit vielleicht gerettet werden. Diese Fälle zeigen, dass eine Grenzziehung zwischen einer Notfallhilfe und einer polizeilichen Maßnahme nicht einfach möglich ist. Eine weitere Diskussion der Thematik erscheint hier dringend erforderlich.

Auch die Notrufverordnung nach § 108 TKG nimmt nun Gestalt an. Ich gehe davon aus, dass sie Anfang 2009 erlassen wird. Zur Übermittlung des Standorts des Notrufenden soll neben einer Mobilfunkortung (bis auf weiteres wohl nur auf Basis der Funkzelle) auch eine Ortung im Bereich Festnetz und Voice over IP (VoIP) erfolgen. Gerade bei VoIP wird ein weiteres Problem aufgeworfen: Der VoIP-Anbieter kennt nur die IP-Adresse, nicht aber den Aufenthaltsort des Hilfesuchenden. Den Aufenthaltsort kennt aber der Internet-Anbieter, der auch die IP-Adresse vergeben hat. Hier fordert die Notrufverordnung eine Zusammenarbeit der Anbieter, wobei allerdings ein Missbrauch verhindert werden muss. Ansonsten könnten auch zwielichtige Internet-Anbieter die Adresse eines Nutzers ermitteln. Wie dies in der technischen Richtlinie

zur Notrufverordnung gelöst werden kann, bleibt abzuwarten. Außerdem muss der Wille von Nutzern respektiert werden, in bestimmten Fällen nicht präzise geortet zu werden. Hierfür müssen die erforderlichen technischen Voraussetzungen geschaffen werden, etwa die Möglichkeit, eine Satelliten-Ortungsfunktion im Handy bei Bedarf abzuschalten.

Ich bestreite nicht, dass Ortungsdienste in vielen Bereichen durchaus sinnvoll eingesetzt werden können. Umso wichtiger ist es, dass dabei die Privatsphäre der Nutzer gewahrt und Missbräuche unterbunden werden. Während andere schwere Eingriffe in den persönlichen Lebens- und Geheimbereich bereits strafrechtlich erfasst sind, etwa die Verletzung der Vertraulichkeit des Wortes oder heimliche Bildaufnahmen (§§ 201, 201a StGB), besteht beim Missbrauch von Ortungsgeräten noch eine Lücke im Strafrecht (vgl. 21. TB Nr. 6.4).

7.8 Verwendung von Telekommunikationsverkehrsdaten für Straßenverkehrsinformationen

Telekommunikationsverkehrsdaten enthalten auch Informationen, die für ganz andere Zwecke interessant sein können.

Verkehrsdaten sind für Telekommunikationsunternehmen ein wertvolles Gut – nicht nur für Abrechnungszwecke. Anders als im Festnetz fallen beim Internet-Zugang oder im Mobilfunkbereich weitaus mehr Verkehrsdaten an, die auch von wirtschaftlichem Interesse sind. So möchten etwa einige Firmen das Surfverhalten von Internet-Nutzern auswerten, um genauere Erkenntnisse über das allgemeine Nutzerverhalten zu gewinnen oder den Nutzern gezielte Werbung zu präsentieren. Alle Modelle, die mir hierzu bisher bekannt sind, gehen jedoch weit über das hinaus, was in Deutschland zulässig ist.

Eine andere Anwendung betrifft Verkehrsdaten im doppelten Sinne. In den Mobilfunknetzen muss der aktuelle Aufenthaltsort eines Handys bekannt sein, damit eine Kommunikation zwischen Handy und Netz zustande kommt. Die dafür notwendige Signalisierung – bei der es sich um Verkehrsdaten im Sinne des TKG handelt – kann ausgewertet werden, um Rückschlüsse auf Ort und Bewegungsgeschwindigkeit der Handys zu ziehen. Bei einer ausreichend großen Zahl von solchen Datensätzen können durch statistische Auswertungen Daten zum Straßenverkehr gewonnen werden. Wenn sich etwa in einem Bereich einer Autobahn alle Handys mit höchstens 30 km/h bewegen, dürfte dies ein deutlicher Hinweis auf einen Stau sein. Da eine solche Umnutzung von Verkehrsdaten im TKG nicht vorgesehen ist, ist es erforderlich, dass die Daten bereits vor ihrer Speicherung, weiteren Verarbeitung und Verknüpfung anonymisiert werden. Das Anonymisierungsverfahren ist so zu gestalten, dass die Anonymisierung irreversibel, also faktisch nicht wieder rückgängig zu machen ist. Wenn noch eine Speicherung der anonymisierten Daten erforderlich ist, sollte der Umfang soweit als möglich begrenzt werden, damit keine Möglichkeit besteht – etwa durch eine Verknüpfung mit anderen Informationen –, dennoch Rückschlüsse auf eine Person zu ziehen. Da eine solche Verarbeitung von Verkehrsdaten für andere Zwecke besondere Risiken für die Betroffenen beinhaltet, ist hierfür eine Vorabkontrolle i. S. v. § 4d Absatz 5 BDSG durchzuführen.

Von zwei Netzbetreibern ist mir bekannt, dass sie ein derartiges Verfahren einführen werden. Nach einigen Verbesserungen halte ich das eine System für akzeptabel, bei dem anderen waren zum Redaktionsschluss die Gespräche noch nicht abgeschlossen. Es erscheint einerseits bedenklich, dass die Bewegungsdaten aller Kunden verwendet werden, andererseits werden jedoch nur Statistikdaten benötigt, da es hier keine Rolle spielt, welche Person im Stau steht.

Kasten zu Nr. 7.8

In der Telekommunikation unterscheidet man folgende Arten von Daten:

Bestandsdaten sind Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. Hierzu gehören etwa Name, Adresse, Kontonummer. Es besteht eine Pflicht, für Abfragen von Sicherheitsbehörden bestimmte Bestandsdaten zu erheben, auch wenn diese betrieblich nicht erforderlich sind (s. § 111 TKG). Ein unachtsamer Umgang mit diesen Daten (s. Nr. 3.2.4) oder eine missbräuchliche Nutzung z. B. von Kontendaten kann schwerwiegende Folgen für den Teilnehmer haben.

Verkehrsdaten sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden und unterliegen dem Fernmeldegeheimnis (Artikel 10 GG, § 88 TKG). Dies sind neben den Daten, die man vom Einzelverbindungsnachweis kennt, auch Standortdaten bei Handygesprächen oder IP-Adressen beim Abruf von E-Mails. Auch hier besteht eine Pflicht zur Vorratsdatenspeicherung (s. Nr. 3.2.1). Die Aussagekraft dieser Daten ist sehr hoch, da soziale Netzwerke oder Bewegungsprofile erkennbar werden. Den Wert dieser Daten hatte auch die Sicherheitsabteilung eines großes Telekommunikationsdiensteanbieters erkannt (s. Nr. 3.2.2). Auch die temporär anfallende Signalisierung für den Netzbetrieb zählt zu den Verkehrsdaten und kann für andere Zwecke interessant sein (s. Nr. 7.8). Bei bestimmten Interessenlagen ist die Definition von Verkehrsdaten jedoch auslegungsfähig (s. Nr. 7.11).

Der **Inhalt der Telekommunikation,** also etwa das Telefongespräch, der Text einer SMS oder E-Mail oder übertragene Daten unterliegen ebenso dem Fernmeldegeheimnis und genießen den höchsten rechtlichen Schutz. Erfreulicherweise muss sich der BfDI weniger häufig mit Datenschutzproblemen zum Inhalt der Telekommunikation beschäftigen, ein Fall findet sich im 20. TB (Nr. 13.2.1).

7.9 Von der Schwierigkeit, Gesetze anzuwenden, am Beispiel des Telemediengesetzes

Durch den Einsatz von immer mehr Technik entstehen fast zwangsläufig immer mehr Daten, die eigentlich nur für die technische Durchführung benötigt werden, sich aber auch für ganz andere Zwecke eignen. Wie weit eine Zweckentfremdung gehen darf, hat der Gesetzgeber festzulegen. Das Telemediengesetz enthält strenge Regelungen zur Verwendung der Nutzungsdaten, die aber oft im Sinne von „praxisrelevanten Erwägungen" weit ausgelegt werden.

Das Telemediengesetz setzt dem Anbieter einer Website für die Verwendbarkeit der technischen Nutzungsdaten (Protokolldaten), die der Nutzer beim Besuch eines Internet-Angebots hinterlässt, enge Grenzen. Erlaubt ist ihm danach die Verarbeitung für die technische Durchführung des Dienstes und für Abrechnungszwecke. Darüber hinaus dürfen die Nutzungsdaten im Einzelfall nur dann verwendet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte für eine Leistungserschleichung vorliegen. Eine Verarbeitungsbefugnis für Datensicherheitszwecke oder – vorsorglich – für Strafverfolgungszwecke besteht nicht. Ebenso wenig zulässig ist die von einer Vielzahl der Website-Anbieter durchgeführte statistische Auswertung der Nutzungsdaten, da hierbei die IP-Adressen der Besucher, die als personenbezogene Daten anzusehen sind, verwendet werden.

Die Praxis vieler Anbieter steht im Widerspruch zu diesen strengen gesetzlichen Vorgaben. So speichern und verwenden manche Anbieter Nutzungsdaten zu Datensicherheitszwecken und für statistische Auswertungen. Vorschläge, das Problem dadurch zu lösen, dass man IP-Adressen kurzerhand zu nicht personenbezogenen Daten erklärt, was dann für die gesamten Nutzungsdaten gelten würde, hätte fatale datenschutzrechtliche Konsequenzen. Damit wäre jede beliebige Verwendung der Nutzungsdaten unabhängig von der Zweckbestimmung für den Anbieter und letztlich sogar für jedermann möglich (vgl. Nr. 7.11). Unter Verwendung der beim Zugangsprovider vorhandenen Informationen ist jedoch immer ein Personenbezug herstellbar. Ebenso, wenn von einem Internet-Anbieter formularmäßig auch persönliche Daten, z. B. bei einer Bestellung, erhoben werden. Allein schon aus diesen Gründen sind IP-Adressen im Regelfall als personenbezogene Daten anzusehen. Dafür spricht aber vor allem, dass Strafverfolgungsbehörden gerade die IP-Adressen, die bei Internet-Anbietern anfallen, dazu verwenden, die Identität mutmaßlicher Täter zu ermitteln (s. u. Nr. 7.10).

Ich habe im Jahr 2008 eine Umfrage bei den Bundesbehörden durchgeführt, um einen Eindruck über die dortige Speicherungspraxis bezüglich der Internet-Nutzungsdaten zu gewinnen. Anlass war das Urteil des Amtsgerichts Berlin-Mitte vom 27. März 2007 (5 C 314/06) – bestätigt durch das Landgericht Berlin als Berufungsinstanz durch Urteil vom 6. September 2007 (23 S 3/07) –, das dem Bundesministerium der Justiz untersagt, Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus zu speichern. Meine Umfrage umfasste auch die Frage, ob und wie die Bundesbehörden statistische Auswertungen der Zugriffe auf ihre Websites durchführen. Das Ergebnis ist in jeder Hinsicht gemischt: Einige Behörden verzichten ganz auf die Speicherung der Nutzungsdaten, andere führen Datensicherheitsgründe für ein teils mehrmonatiges Vorhalten der Protokolldaten an. In vielen Fällen werden statistische Untersuchungen durchgeführt, um das Angebot zu optimieren. Nur in wenigen Fällen stehen Gesetz und Praxis in Einklang.

Angesichts dieser Situation halte ich einen verbindlichen Leitfaden zur rechtskonformen Verarbeitung von Nutzungsdaten für die Bundesbehörden für erforderlich.

Unabhängig davon gibt es Bestrebungen, das Telemediengesetz zu ändern und eine dem Telekommunikationsgesetz entsprechende Regelung aufzunehmen, die eine Verarbeitung der Nutzungsdaten „zum Erkennen, Eingrenzen und Beseitigen von Störungen und Fehlern" erlaubt. Ich bin von der Notwendigkeit einer zusätzlichen Speicherung nicht überzeugt. Zunächst ist zu prüfen, ob nicht bereits verwendete, erforderlichenfalls zu optimierende Mittel (Firewalls) zur Verhinderung und Abwehr von Angriffen genügen.

Was die Verarbeitung für statistische Zwecke betrifft, soll jedoch alles beim Alten bleiben. Deshalb kann ich den Website-Anbietern nur raten, die Nutzungsdaten vor der Auswertung in geeigneter Weise zu anonymisieren, wie das auch bei den Besucherdaten meiner eigenen Website geschieht. Auch wenn dadurch das Ergebnis der Auswertung ein wenig verzerrt wird, reichen die anonymen Daten zur Optimierung des Internet-Angebots aus.

7.10 Homepage-Überwachung durch das Bundeskriminalamt

Das BKA hat die Zugriffe auf veröffentlichte Fahndungsausschreibungen auf seiner Website erfasst. Die Maßnahme wurde inzwischen eingestellt, da ich das BMI und das BMJ von der Rechtswidrigkeit der Erhebung überzeugen konnte.

Im Berichtszeitraum habe ich geprüft, in welcher Weise das BKA das Internet zur Erfüllung seiner Aufgaben nutzt. Dabei habe ich u. a. festgestellt, dass es die Erfassung der Zugriffe auf Fahndungsausschreibungen, die auf seiner Website im Zusammenhang mit ungeklärten Straftaten veröffentlicht werden, als neue Fahndungsmaßnahme entwickelt hat.

Diese sog. Homepage-Überwachung zielte darauf ab, diejenigen Internet-Nutzer zu identifizieren, die die entsprechenden Fahndungsseiten häufiger aufrufen und sich damit offensichtlich intensiver als der Durchschnittsnutzer über den Fortgang der Ermittlungen informieren. Nach Darlegung des BKA habe die kriminalistische Erfahrung gelehrt, dass sich Täter bei manchen Straftaten, insbesondere bei Delikten von großem öffentlichem Interesse, regelmäßig über den Fortgang der Ermittlungen informiert haben.

Bei der Homepage-Überwachung werden Zugriffe auf Fahndungsseiten auf dem Webserver des BKA mit einem

separaten Auswertungsserver protokolliert. Außerdem werden „Cookies“ oder „Web-Bugs“ auf dem Computer des Nutzers gespeichert. Damit wird es möglich, einen Nutzer wiederzuerkennen, wenn er die Seiten mehrfach mit zeitlichem Abstand betrachtet. Die Zugriffe werden u. a. mit Angaben über die Anzahl der aufgerufenen Seiten, Zeitpunkt und IP-Adresse der ersten und der letzten Nutzung sowie Informationen zum Provider aufgelistet. Zudem können weitere Informationen, etwa die aufgerufene Seite, aufgeführt werden. Damit wird eine exakte Rekonstruierung der Nutzung jedes einzelnen Absenders möglich. Die Nutzungsdaten bleiben auf dem Auswertungsserver bis zum Abschluss des jeweiligen Falles bzw. bis zur Beendigung der Maßnahme gespeichert.

Das BKA vertrat die Auffassung, dass diese Form der Homepage-Überwachung auf die Ermittlungsgeneralklausel des § 163 StPO gestützt werden könne. Der Internet-Nutzer rechne außerdem damit, dass die Protokolldaten auf den Webservern gespeichert würden. Er gebe damit Daten beim Surfen im Internet freiwillig preis. Zudem müsse der Nutzer auch mit der Installation von „Cookies“ rechnen.

Gegenüber der Bundesregierung habe ich hingegen die Auffassung vertreten, dass es für die vom BKA betriebene Homepage-Überwachung an einer Rechtsgrundlage fehlt. Informationen darüber, wer wie oft auf eine bestimmte Website zugegriffen hat, sind Angaben zu den näheren Umständen der Telekommunikation, die durch Artikel 10 GG geschützt sind. Stellt ein Anbieter eine Website ins Netz, handelt es sich um ein Angebot im Bereich der Telemedien. Der Umgang mit den beim Anbieter eines solchen Angebots anfallenden Nutzungsdaten richtet sich abschließend nach dem Telemediengesetz, welches keine Befugnis für die vom BKA vorgesehene Verwendung der Nutzungsdaten einräumt (s. o. Nr. 7.9). Selbst wenn die Strafprozessordnung zur Anwendung käme, reichte § 163 StPO als Rechtsgrundlage für die heimliche Homepage-Überwachung im Hinblick auf den damit verbundenen Eingriff in das informationelle Selbstbestimmungsrecht überwiegend unbescholtener Personen nicht aus.

Nach ausführlichen Beratungen der Thematik hat sich die Bundesregierung nunmehr meiner Rechtsauffassung angeschlossen. Das BMJ hat mir mitgeteilt, dass der Generalbundesanwalt derartige Maßnahmen nicht mehr veranlassen werde. Das BMI hat das BKA angewiesen, mit den betreffenden Staatsanwaltschaften Einvernehmen über die Beendigung etwaiger noch laufender Maßnahmen herzustellen und zukünftig das Instrument der Homepage-Überwachung nicht mehr einzusetzen.

7.11 Kontroverse: Auskunft über Inhaber von IP-Adressen

Seit langem ist strittig, auf welcher Rechtsgrundlage ein Provider Auskunft über den Inhaber einer IP-Adresse geben muss.

Nur der Internet-Zugangsprovider weiß, welchem seiner Kunden er zu welchem Zeitpunkt eine bestimmte IP-Adresse dynamisch zugeteilt hat. Denn diese Informationen sind in seinen Protokolldateien gespeichert, die aus Datensicherheitsgründen kurzfristig zur Verfügung stehen und die er spätestens seit dem 1. Januar 2009 sechs Monate lang für Strafverfolgungszwecke vorhalten muss (vgl. Nr. 3.2.1). Die Ermittlungsbehörden müssen daher bei der Aufklärung von Straftaten, die im oder mit Hilfe des Internet begangen wurden, in zahlreichen Fällen entsprechende Anfragen beim jeweiligen Provider stellen.

Strittig ist, welche Vorschrift als Grundlage für ein Auskunftsersuchen herangezogen werden muss. Unstrittig ist, dass es sich bei den Protokolldaten um Verkehrsdaten (und nicht um Bestandsdaten) der Telekommunikation handelt (s. Kasten zu Nr. 7.8). § 113 TKG verpflichtet die Provider, den Strafverfolgungs- und Sicherheitsbehörden die Bestandsdaten eines Kunden auf Anfrage unverzüglich mitzuteilen, und stellt dabei keine besonderen Voraussetzungen an das Auskunftsersuchen. Die Anfragen seien auf Bestandsdaten gerichtet, auch wenn zur Ermittlung der Identität der Person hinter einer IP-Adresse Verkehrsdaten hinzugezogen werden müssten, argumentieren die Befürworter dieser Rechtsgrundlage. Entsprechend hat z. B. die Bundesnetzagentur die Deutsche Telekom AG verpflichtet, Auskünfte zur Identität von Internet-Nutzern auf Basis von § 113 TKG zu erteilen. Gegen diesen Bescheid hat die Deutsche Telekom AG Widerspruch eingelegt, eine Entscheidung liegt noch nicht vor.

Weil zur Ermittlung der Person, die Telekommunikationsdienste in Anspruch genommen hat, Verkehrsdaten genutzt werden müssen, vertrete ich die Auffassung, dass die entsprechenden Bestandsdaten nur auf Grundlage des § 100g StPO an Strafverfolgungsbehörden herausgegeben werden dürfen. Dies setzt – außer in Eilfällen – einen richterlichen Beschluss voraus. Das Gesetz sieht für die vom Fernmeldegeheimnis geschützten Verkehrsdaten eine höhere Eingriffsschwelle vor als für eine „einfache“ Bestandsdatenabfrage nach § 113 TKG.

Besonders deutlich wird die Unzulänglichkeit der Vorschrift des § 113 TKG im Zusammenhang mit Auskunftsersuchen, die Kunden von sog. Resellern der Provider betreffen. Ohne sie zu „kennen“, vergibt der Provider auch für diese Kunden die dynamischen IP-Adressen, da er seine Technik für die Reseller zur Verfügung stellt. Anfragen der Ermittlungsbehörden werden daher an ihn gerichtet. Da er die nach § 113 TKG geforderte Auskunft zu den Bestandsdaten nicht erteilen kann, stellt sich die Frage, ob die Auskunft, welcher Reseller die Daten liefern kann, von dieser Vorschrift gedeckt ist oder ob eine erneute Anfrage nach § 161a StPO zur Zeugenaussage erforderlich ist.

Mit Einführung der Vorratsdatenspeicherung wurden – am Ende des parlamentarischen Verfahrens und daher weitgehend unbemerkt – durch einen knappen Einschub im Gesetzestext die Vorratsdaten für Auskunftsersuchen nach § 113 TKG „geöffnet“. Damit soll nun klargestellt sein, dass IP-Adressen grundsätzlich auf dieser Rechtsgrundlage zu beauskunften sind. Diese „Klarstellung“ an unerwarteter Stelle als solche zu erkennen und zu verste-

hen, verlangt schon genaues Hintergrundwissen, vor allem hinsichtlich ihrer Entstehungsgeschichte. Das Bundesverfassungsgericht hat in seiner einstweiligen Anordnung zur Vorratsdatenspeicherung diese Nutzung leider nicht eingeschränkt.

Die Fachgerichte haben in der Frage der Rechtsgrundlage für die Auskunftserteilung unterschiedlich entschieden. Dies führt dazu, dass in den Bundesländern unterschiedlich verfahren wird. Ein Zustand, der für alle Beteiligten unbefriedigend ist und dringend einer Änderung bedarf. Ich hoffe daher, dass die Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung auch einen Weg weist, wie diese sehr wichtige Frage des Zugriffs auf Verkehrsdaten im Sinne eines effektiven Schutzes des Fernmeldegeheimnisses und des Rechts auf informationelle Selbstbestimmung zu lösen ist.

7.12 Auf dem Prüfstand: die Telekommunikations-Richtlinien

Der seit dem Jahr 2003 bestehende europäische Rechtsrahmen für elektronische Kommunikationsnetze und -dienste wird hinsichtlich der Entwicklung des Marktes und der Förderung der Bürgerinteressen überprüft. Die sich abzeichnenden Rechtsänderungen haben erhebliche Konsequenzen für den Datenschutz.

Im November 2007 veröffentlichte die Europäische Kommission einen Vorschlag zur Änderung der Richtlinien zur Regulierung des Telekommunikationssektors (KOM (2007) 697 endg., KOM (2007) 698 endg., KOM (2007) 699 endg.). Betroffen sind sowohl der Rechtsrahmen für die Anbieter von Kommunikationsdiensten als auch die nutzerorientierten Richtlinien: die Universaldienst-Richtlinie, die u. a. die allgemeinen Rechte der Nutzer regelt, und die Datenschutzrichtlinie, die die Verarbeitung von personenbezogenen Daten und den Schutz der Privatsphäre normiert.

In den darauf folgenden Monaten beschäftigten sich das Europäische Parlament und der Rat mit den Vorschlägen der Kommission. Einige datenschutzrelevante Themen wurden in den Ausschüssen des Parlaments kontrovers diskutiert und riefen Datenschützer wie Bürgerrechtler auf den Plan.

Für viel Zündstoff sorgte der Vorschlag für eine Abänderung der TK-Datenschutzrichtlinie, nach der IP-Adressen nur noch eingeschränkt als personenbezogene Daten angesehen werden sollten. Kriterium sollte sein, ob ein Personenbezug von einem Diensteanbieter direkt hergestellt werden könnte. Dies hätte bedeutet, dass bei allen Anbietern, außer den Zugangsprovidern, die Surfdaten der Nutzer beliebig verwendet worden wären und somit eine eskalierende Auswertung des Nutzerverhaltens im Internet und auch in der realen Welt legitimiert wäre. Nach meiner Auffassung sind IP-Adressen in jedem Fall personenbezogene Daten, da unter Verwendung der beim Zugangsprovider vorhandenen Informationen immer ein Personenbezug herstellbar ist. Möglich ist dies auch, wenn formularmäßig persönliche Daten von einem Internet-Anbieter erhoben werden. Der Vorschlag wurde vom Parlament nicht angenommen, ebenso wenig der Auftrag an die Kommission, innerhalb einer Frist von zwei Jahren einen Gesetzesvorschlag zur Behandlung von IP-Adressen vorzulegen.

Diskussionen gab es auch über den Vorschlag einer „Blankett-Ermächtigung“, nach der jede natürliche oder juristische Person Verkehrsdaten für Datensicherheitszwecke verarbeiten dürfte. Das hätte bedeutet, dass jeder mit einem wirtschaftlichen Verarbeitungsinteresse, insbesondere auch die Hersteller von Sicherheitssoftware, zur Speicherung von sensiblen Verkehrsdaten der Telekommunikation berechtigt wäre, die dem Telekommunikationsgeheimnis unterliegen. Ein kurzfristig eingebrachter modifizierter und schließlich vom Parlament angenommener Vorschlag engt die neue Befugnis zwar auf „die berechtigten Interessen der verarbeitenden Stelle“, d. h. der Anbieter von Telekommunikationsdiensten ein, ohne jedoch den Kreis der Ermächtigten selbst zu adressieren. Diese Version ist in den geänderten Richtlinienvorschlag der Kommission eingegangen.

Ich habe mich schon im Rahmen der Vorbereitung der politischen Einigung im Rat gegenüber dem BMWi dafür eingesetzt, dass im Richtlinientext eine Präzisierung entsprechend dem deutschen Telekommunikationsgesetz erfolgt. Hiernach ist zum Erkennen, Eingrenzen und Beseitigen von Störungen und Fehlern an Telekommunikationsanlagen die Verarbeitung von Verkehrsdaten für einen kurzen Zeitraum möglich. Entsprechende Verfahren haben sich im Einsatz bei den deutschen Zugangsprovidern bewährt. Die gemeinsame Position des Rates ist jedoch weiterhin weit formuliert, da die von mir favorisierte engere Regelung nicht durchzusetzen war. Lediglich der Erwägungsgrund enthält nun eine Zweckbegrenzung, die den Regelungen des Telekommunikationsgesetzes entspricht. Auch in den weiteren Verhandlungen werde ich auf eine entsprechende Änderung des Richtlinientextes hinwirken.

Im Rahmen der Diskussionen in den Ausschüssen des Europäischen Parlaments wurde von einigen Abgeordneten versucht, das „französische Modell“ in den Richtlinien zu verankern. Hiernach wäre in einem mehrstufigen Verfahren der „Internet-Piraterie“ Einhalt geboten (s. o. Nr. 7.4). Nach einer ersten Verwarnung und einer auf einen Monat befristeten Zugangssperre im Wiederholungsfall würde am Ende der Entzug der Zugriffsrechte der betroffenen Nutzer für bis zu einem Jahr stehen. Im Plenum wurde dieses Modell abgelehnt; die Parlamentarier wollten die Provider aber zumindest zur „Förderung rechtmäßiger Inhalte“ verpflichten. Angenommen wurden auch Vorschläge zur Kooperation zwischen Providern und Rechteinhabern, die illegale Downloads eindämmen bzw. von vornherein unterbinden sollen. In der Position des Rates finden sich ähnliche weiche Formulierungen, die die Kooperation zwischen Providern und „an rechtmäßigen Inhalten Interessierten“ begründen.

Vom Tisch ist das Thema damit jedoch keineswegs. Denn die Kommission überprüft derzeit die Richtlinien, die die Verbreitung von Inhalten betreffen, und hat mit einer „Mitteilung über kreative Online-Inhalte im Binnen-

markt“ (KOM (2007) 836 endg.) einen Prozess eingeleitet, „um die bereits ermittelten und dringlichsten Herausforderungen im Zusammenhang mit der Online-Verbreitung kreativer Inhalte zu bewältigen“.

Aus Datenschutzsicht sehr positiv ist der Vorschlag des Parlaments, Informationspflichten in die Datenschutzrichtlinie aufzunehmen. Danach müssen die Provider bei Verlust, Diebstahl oder Missbrauch personenbezogener Daten unverzüglich die hiervon betroffenen Bürgerinnen und Bürger und die zuständigen Aufsichts- oder Kontrollbehörden unterrichten. Unklar ist noch, in welcher Ausprägung diese Regelung letztendlich festgeschrieben wird. Denn sowohl die gemeinsame Position des Rates als auch der geänderte Richtlinienvorschlag der Kommission sehen einen Vorbehalt vor, der die Provider nur in schweren Fällen bzw. bei einer abzusehenden Gefährdung in die Pflicht nimmt.

Das Europäische Parlament hat seinen Bericht am 24. September 2008 mit verschiedenen Abänderungen zu den Vorschlägen der Kommission und zu den Richtlinien selbst verabschiedet. Die Kommission hat zu diesen Abänderungen Stellung genommen und am 6. November 2008 einen geänderten Vorschlag für die Richtlinien vorgelegt, der einen Teil der Vorschläge des Parlaments – teils modifiziert – übernimmt. Die Diskussion im Rat mündete am 27. November 2008 in einer politischen Einigung der Minister der Mitgliedstaaten. Die gemeinsame Position bildet die Grundlage für die weiteren Verhandlungen mit dem Parlament, um eine Einigung in der zweiten Lesung zu erreichen.

Anfang 2009 beginnt der „Trilog“ (Einigungsverfahren zwischen Parlament und Rat unter Beteiligung der Kommission) mit dem Ziel, eine gemeinsame Lösung zu erarbeiten. Gelingt dies, wird die zweite Lesung im Parlament Ende März 2009 überflüssig.

8 Technologischer Datenschutz

Immer enger sind Fragen zur Informationstechnologie oder ihres Einsatzes mit rechtlichen Fragestellungen verknüpft. Das Urteil des BVerfG zur Online-Durchsuchung vom 27. Februar 2008 setzt hier neue Maßstäbe.

„Das allgemeine Persönlichkeitsrecht (Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.“ So lautet der erste Leitsatz in dem Urteil des BVerfG zu Vorschriften des Verfassungsschutzgesetzes Nordrhein-Westfalen. Diese Entscheidung hat Konsequenzen, die weit über den eigentlichen Streitgegenstand, die Befugnisse des Landesamtes für Verfassungsschutz zu heimlichen Zugriffen auf informationstechnischen Systeme, hinausgehen. Diese Konsequenzen sind zum einen rechtlicher Natur (s. auch unter Nr. 4.1). Darüber hinaus werden zur Gewährleistung des Datenschutzes im Sinne des „neuen Grundrechts“ auch technisch-organisatorische Vorkehrungen umzusetzen sein. Deshalb müssen die Regelungen zu den technisch-organisatorischen Maßnahmen im BDSG – aber auch in einigen Landesgesetzen – fortgeschrieben werden, um den verfassungsrechtlichen Vorgaben gerecht zu werden. Zudem ist eine bessere Verzahnung der Regelungen dringend geboten.

Da das Datenschutzrecht kein reines Abwehrrecht ist, sondern auch als (IT-Systeme) gestaltendes Recht im öffentlichen und nicht-öffentlichen Bereich wirkt, sollte das Urteil in den Regelungen der Datenschutzgesetze einfließen. So könnten die Sicherheitsziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz (s. Kasten a zu Nr. 8) bei der Modernisierung der Datenschutzgesetze Einzug halten, denn moderne Technik verlangt moderne Regelungen. Diese Sicherheitsziele sind technologieunabhängig und bieten damit einen Sicherheitsrahmen, der auch bei neuen Formen der Informationstechnik Bestand haben kann. Auch die EG-Datenschutzrichtlinie und eine Reihe von Landesdatenschutzgesetzen bedienen sich dieser Begriffe.

Kasten a zu Nr. 8

Stichwort Sicherheitsziele:

Vertraulichkeit:	Nur Befugte dürfen Daten zur Kenntnis nehmen.
Integrität:	Daten müssen während der Erhebung, Verarbeitung und Nutzung unversehrt, vollständig und aktuell bleiben.
Verfügbarkeit:	Daten müssen zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet oder genutzt werden können.
Authentizität:	Daten müssen jederzeit ihrem Ursprung zugeordnet werden können.
Revisionsfähigkeit:	Es muss feststellbar sein, wer wann welche Daten in welcher Weise erhoben, verarbeitet oder genutzt hat.
Transparenz:	Die Verfahren zur Erhebung, Verarbeitung und Nutzung müssen nachvollziehbar und aktuell dokumentiert sein.

Angesichts der exponentiell zunehmenden Erhebung, Verknüpfung und Bewertung von Informationen werden Fragen des Datenschutzes und der Informationsfreiheit immer bedeutsamer. Um eine Diskussion dieser Fragen anzustoßen, habe ich aus Anlass des Dritten Nationalen IT-Gipfels am 21. November 2008 eine Charta des digitalen Datenschutzes und der Informationsfreiheit vorgeschlagen (s. Kasten b zu Nr. 8). Es ist für mich besonders wichtig, auf die Verantwortlichkeit aller Beteiligten, also sowohl staatlicher Stellen und Unternehmen, aber auch jedes Einzelnen für die Inhalte hinzuweisen, die er über sich und insbesondere andere veröffentlicht. Der Vorschlag soll einen grundsätzlichen Meinungsaustausch zu diesen Kernfragen anstoßen. Gerne werde ich den Dialog mit den Bürgerinnen und Bürgern fortsetzen, aber auch weitere Organisationen und Gruppen beteiligen.

Kasten b zu Nr. 8

Vorschlag für eine Charta des digitalen Datenschutzes und der Informationsfreiheit

In einer durch Interaktivität geprägten Welt sind die Einzelnen nicht mehr bloß Nutzer, sondern Netzbürger mit unveräußerlichen Rechten. Als solche sind sie aber auch verantwortlich für Inhalte, die sie über sich und andere veröffentlichen.

Die Gestaltung und Verwendung elektronischer Dienste sollte sich an folgenden Grundsätzen orientieren:

- Jeder hat das Recht, sich unbeobachtet und frei von Überwachung im Internet zu bewegen. Dienste müssen nach Möglichkeit auch anonym oder unter Pseudonym in Anspruch genommen werden können.
- Die Privatsphäre muss auch in der digitalen Welt beachtet werden. Sowohl staatliche Stellen als auch Unternehmen sind aufgerufen, ihr Handeln an dieser Maxime auszurichten. Datenvermeidung und Datensparsamkeit kommt dabei zentrale Bedeutung zu.
- Die Vertraulichkeit und Integrität elektronischer Datenverarbeitung ist zu gewährleisten. Einfach zu bedienende sichere Verschlüsselungsverfahren gehören zur informationstechnischen Grundversorgung.
- Jeder hat das Recht, über die Preisgabe seiner Daten selbst zu bestimmen. Dienste müssen entsprechende Einstellmöglichkeiten aufweisen. Personenbezogene Daten dürfen nur erhoben, verarbeitet oder genutzt werden, wenn die Betroffenen darin ausdrücklich einwilligen (opt in). Elektronisch erteilte Einwilligungen müssen jederzeit – auch elektronisch – widerrufen werden können.
- Transparenz beim Umgang mit persönlichen Daten ist eine Bringschuld aller verantwortlichen Stellen. Betroffene haben ein unveräußerliches Recht auf Auskunft hinsichtlich der zu ihrer Person oder zu ihrem Pseudonym gespeicherten Daten.
- Öffentliche Stellen sind gehalten, sich stärker zu öffnen. Bürgerinnen und Bürgern haben ein Recht zu erfahren, wie Entscheidungen zu Stande kommen und wie Steuergelder ausgegeben werden. Fachliche Weisungen, Dienst- und Verwaltungsvorschriften sollten über das Internet verfügbar gemacht werden.
- Zu einer offenen Verwaltung gehören einfach zu nutzende, sichere Kommunikationsmöglichkeiten mit Bürgerinnen und Bürgern. Sie erwarten zu Recht kompetente und zügige Reaktionen auf ihre Anliegen.
- Wer das Internet in Anspruch nimmt und dabei Informationen preisgibt, muss sich der Folgen bewusst sein, denn im Netz gibt es kein Vergessen. Besondere Sorgfalt ist geboten bei Bewertungen, Bildern oder sonstigen Informationen über Dritte; ihre Rechte sind zu beachten.
- Die Bildungseinrichtungen – vom Kindergarten, über die Hochschule bis zur Erwachsenenbildung – sind gehalten, allen Generationen das nötige Rüstzeug für einen verantwortungsbewussten Umgang mit neuen Technologien zur Verfügung zu stellen.
- Auch in einer zunehmend von Technik geprägten Welt gibt es Menschen, die aus guten Gründen elektronische Dienste nicht in Anspruch nehmen. Ihre Entscheidung ist zu respektieren und darf nicht zu Benachteiligungen führen.

8.1 Videoüberwachung

Das gemeinsam mit dem BSI entwickelte Schutzprofil für Videoüberwachungsanlagen zeigt Wirkung. Der Betrieb einer Videoüberwachungsanlage ist mit genormten Infozeichen anzuzeigen.

Das von mir zusammen mit dem BSI entwickelte „Schutzprofil für Videoüberwachungsanlagen“ stellt technisch-organisatorische Anforderungen an Videoüberwachungsanlagen, die bei der Beschaffung, der Installation und dem Betrieb datenschutzrechtlich beachtet werden müssen. Das Schutzprofil habe ich bereits in meinem 21. TB beschrieben (Nr. 4.2.1), es wurde im Berichtszeitraum um eine englischsprachige Version ergänzt. Das Schutzprofil ist in beiden Versionen auf meiner Internet-Seite unter www.bfdi.bund.de verfügbar.

Nach mehreren Informationsveranstaltungen, bei denen ich alle Ressorts über den Inhalt und die Nutzung des Schutzprofils informiert habe, zeigt es langsam Wirkung. So teilte mir die Bundespolizei mit, dass sie, meiner Anregung entsprechend, künftig nur noch solche Videoanlagen beschaffen wird, die den Anforderungen des Schutzprofils entsprechen. Davon sind auch die im Rahmen des Programms zur Stärkung der inneren Sicherheit (PSIS) vorgesehenen Videoanlagen für die Überwachung der Bahnanlagen und des Flughafens Frankfurt/Main betroffen. Darüber hinaus soll das Schutzprofil als Endnutzeranforderung in das Sicherheitsforschungsprojekt „Sicherheit im offenen Verkehrssystem Eisenbahn (SinoVE)“ unter Federführung der Deutschen Bahn AG einfließen. Dieses Projekt werde ich beratend begleiten.

Bei meinen Beratungen und Kontrollen von Videoüberwachungsanlagen auf Bahnhöfen und Flughäfen hat sich herausgestellt, dass die unterschiedlichsten Hinweisschilder bei der Kennzeichnung der videoüberwachten Bereiche zum Einsatz kommen. Um einen hohen Erkennungswert der Videoüberwachung zu gewährleisten, müssen genormte Hinweisschilder nach DIN 33450 (Video-Infozeichen) angebracht werden (s. Kasten zu Nr. 8.1).

Das inzwischen abgeschlossene Forschungsprojekt „Foto-Fahndung“ des BKA am Mainzer Hauptbahnhof (s. Nr. 6.3; 21. TB Nr. 5.2.6) hatte im Hinblick auf die Erkennungsgenauigkeit ein unbefriedigendes Ergebnis. Gleichwohl werde ich die Entwicklung der Videotechnologie und ihre mögliche Verknüpfung mit Ansätzen zur biometrischen Identifikation von Personen weiterhin aufmerksam beobachten. Von besonderem Interesse dürfte dabei die Weiterentwicklung datenschutzfreundlicher Verfahren sein, etwa NMO-Detektoren (Non Moving Objects) zur Erkennung z. B. herrenloser Gegenstände im Aufnahmebereich von Videoüberwachungssystemen.

Abbildung zu Nr. 8.1

Video-Infozeichen nach DIN 33450

Graphisches Symbol zum Hinweis auf Beobachtung mit optisch-elektronischen Einrichtungen (Video-Infozeichen) vom Deutschen Institut für Normung e. V., DIN

8.2 Verschlüsselung wichtig, aber immer noch nicht selbstverständlich

Eine aktuelle Umfrage bei der Bundesverwaltung zeigt, dass personenbezogene Daten beim Versand per Datenträger immer noch viel zu selten verschlüsselt werden.

Die Vorkommnisse in Großbritannien Anfang des Jahres 2008 als CD mit Namen, Adressen, Geburtsdaten sowie Kontoinformationen von der Steuerbehörde auf dem Postweg verloren gingen, habe ich zum Anlass genommen, mich über die Praxis des Versendens von personenbezogenen Daten auf Datenträgern in Bundesbehörden zu informieren. Die Ergebnisse geben Anlass zur Sorge. So verschickt beispielsweise das Bundesamt für Justiz Daten mit Hinweisen auf Straftaten ungesichert an das italienische Justizministerium. Das Bundesamt für Güterverkehr verschickt Daten über Straf- und Bußgelderverfahren auf CD. Diese Praxis halte ich für nicht hinnehmbar. Gleichwohl habe ich von einer förmlichen Beanstandung zunächst abgesehen, da die festgestellten Mängel in den meisten Fällen inzwischen abgestellt wurden. Im Übrigen wurde deren Behebung kurzfristig zugesichert. Ich werde mich durch Prüfung der entsprechenden Verfahren davon vergewissern, ob diese Zusagen eingehalten werden.

Die Abfrage hat im Einzelnen folgendes Bild ergeben:

Obwohl die Vernetzung innerhalb der Bundesverwaltung sehr weit fortgeschritten ist, ist die Datenübermittlung per Datenträger bei vielen Bundesbehörden nach wie vor die Regel.

Datenträger werden mit anderen Bundesbehörden, Landesbehörden, Stellen in Kommunen und Gemeinden ausgetauscht. Auch grenzüberschreitend werden Datenträger versandt. In Einzelfällen werden Daten auch per Datenträger an Betroffene versandt.

Auch besonders schutzwürdige Daten i. S. v. § 3 Absatz 9 BDSG sind betroffen, etwa Gesundheitsdaten, Daten über Straf- und Bußgeldverfahren, Personaldaten und Beihilfedaten.

Die Übermittlung/Versendung war nur zum Teil abgesichert. So kamen nur vereinzelt Verschlüsselungsprogramme, und zwar mit sehr unterschiedlicher Qualität zum Einsatz, darunter auch völlig unbekannte Verschlüsselungsprogramme und ungeprüfte Eigenentwicklungen.

Der Versand der Datenträger ohne Schutzmechanismen stellt allerdings die überwiegende Mehrzahl dar. Insgesamt lässt sich für die Versendung von Datenträgern und die dabei eingesetzten Sicherungsmaßnahmen folgendes feststellen:

- Verschlüsselung mit Chiasmus bei ca. 10 Prozent der Abfrage,
- Verschlüsselung mit anderen Verfahren bei ca. 30 Prozent,
- keine Verschlüsselung; Postversand ohne Sicherung bei ca. 45 Prozent,
- keine Verschlüsselung; Postversand mit Sicherung z. B. Wertpaket bei ca. 5 Prozent,
- Postversand plus Passwortschutz auf dem Datenträger bei ca. 5 Prozent,
- keine Angaben bzw. ungenügende Angaben bei ca. 5 Prozent.

Maßnahmen zur Sicherung der Integrität der Daten werden in der Regel nicht vorgenommen. Digitale Signaturen werden überhaupt nicht eingesetzt. Das hat zur Folge, dass nachträgliche Änderungen der Daten nicht erkannt

werden können. Zudem beeinträchtigt dieser Mangel die Beweiskraft der übermittelten Informationen.

Bei etwa nur der Hälfte der Behörden existieren – jedoch zum Teil veraltete – Richtlinien, die den Versand von Datenträgern regeln.

Zur Frage einer Sicherungskopie der übermittelten Daten konnte ich folgendes ermitteln:

– 1/3 der Behörden speichert eine 1:1 Kopie der übermittelten Daten.

– 1/3 der Behörden kann die übermittelten Daten aus dem Datenbestand rekonstruieren. Ob dabei Veränderungen an den Datensätzen zwischen dem Zeitpunkt des Versendens und dem Rekonstruktionszeitpunkt erkannt bzw. markiert werden, war nicht festzustellen.

– 1/3 der Behörden verzichtet ganz auf eine Sicherungskopie der übermittelten Daten und kann auch keine Daten rekonstruieren. In diesen Fällen würde das Abhandenkommen eines Datenträgers zu irreversiblen Datenverlusten führen.

Nur etwa die Hälfte der Behörden lagert Datensicherungen (Backups) aus. Der Transport der Daten erfolgt dann allerdings in der Regel durch eigenes Personal. Nur bei ganz wenigen Behörden werden Backup-Datenträger durch „Dritte“ transportiert.

Eine Kontrolle der Vorschriften wurde in der Regel weder durch den behördlichen Datenschutzbeauftragten noch den Sicherheitsbeauftragten oder die Innenrevision durchgeführt.

Ich habe die Umfrage zum Anlass genommen, zusammen mit dem BSI eine Empfehlung zum sicheren Datenträgerversand zu entwickeln, die auch in das IT-Grundschutzhandbuch und den Maßnahmenkatalog einfließen sollen.

8.3 Effektive Datenlöschung

Immer wieder werden Fälle bekannt, bei denen zum Verkauf angebotene gebrauchte Festplatten von PC nicht ausreichend sicher gelöscht werden. Oftmals sind sensible personenbezogene Daten und persönliche Fotos direkt einsehbar oder können ohne großen Aufwand rekonstruiert werden.

Auch ausgemusterte Computer und Festplatten der öffentlichen Verwaltung werden oftmals gegen geringe Gebühr z. B. an Schulen weitergegeben oder über die IT-Altgerätebörse des Bundesverwaltungsamtes (BVA) oder die Auktionsplattform des Zolls zur weiteren Verwendung angeboten. Vor der Weitergabe sind die Festplatten dieser Geräte jedoch sicher zu löschen. Wenn Datenträger mit nicht oder nur unzureichend gelöschten personenbezogenen Daten weitergegeben werden, stellt dies einen schwerwiegenden Verstoß gegen § 9 BDSG dar. Nach dieser Rechtsvorschrift müssen die mit der Datenverarbeitung befassten Stellen gewährleisten, dass Unbefugte keine Kenntnis der personenbezogenen Daten erhalten. Die unbefugte – auch unbeabsichtigte – Weitergabe persönlicher Daten kann als Ordnungswidrigkeit mit einem Bußgeld geahndet werden. Darüber hinaus können sich erhebliche Schadensersatzansprüche ergeben (§§ 7, 8 BDSG).

Die sichere Datenlöschung kann z. B. mittels des vom BSI entwickelten Löschprogramms VS-Clean erfolgen. Dieses Löschtool besitzt eine Zulassung zur Löschung von Festplatten, auf denen Daten bis zur Geheimhaltungsstufe VS-Vertraulich gespeichert wurden. Datenträger mit einem höheren Geheimhaltungsgrad müssen zusätzlich – sofern sie nicht geeignet verschlüsselt sind – immer physisch vernichtet werden. Für die unmittelbare Bundes-, Landes- und die Kommunalverwaltungen ist der Bezug des Löschprogramms über das BSI kostenlos. Für andere Anwender empfiehlt sich z. B. der Einsatz frei erhältlicher Tools (s. Kasten zu Nr. 8.3).

Soweit die Theorie. Wie sieht die praktische Umsetzung aus? Meine Dienststelle hat im Rahmen eines Projektes zusammen mit der Fachhochschule Bonn-Rhein-Sieg 20 PC und Laptops mit Festplatten über die IT-Altgerätebörse des BVA bezogen und die eingebauten magnetischen Datenträger mittels frei erhältlicher Tools zur „Datenrettung“ auf vorhandene oder ggf. rekonstruierbare Inhalte überprüfen lassen. Als vorläufiges Ergebnis kann festgehalten werden, dass auf acht von bisher 15 untersuchten Festplatten personenbezogene Daten gefunden wurden bzw. rekonstruiert werden konnten. Insbesondere enthielten zwei der untersuchten Datenträger detaillierte Informationen. Diese Daten bestehen aus privaten und geschäftlichen Bildern sowie Videos und Textdateien. In den Textdateien konnten verschiedene Namen, Adressen und weitere persönliche Daten gefunden werden. Aus der dienstlichen Nutzung stammen Daten wie persönliche Anschreiben von Bürgern an eine Dienststelle, eine Datenbank mit Adressdaten oder eine Reisekostenabrechnung. Weiter wurden auch private Daten wie Kündigung eines Handyvertrages, Liebesbrief, Familienfotos etc. gefunden.

Mittels der Suchmaschine Google war es im Einzelfall möglich, Personen zweifelsfrei inklusive Informationen über deren Arbeitsplatz, Wohnort, TelefonNummer und E-Mail-Adresse zu recherchieren. Die Ergebnisse lassen zum Teil auch Rückschlüsse über die Familienverhältnisse (Hochzeitsfotos) zu. Von den geprüften Datenträgern waren lediglich die Hälfte sicher gelöscht. Diese alarmierende Quote unterstreicht den hohen Handlungsbedarf.

Ich möchte hier nicht über die Ursachen für diesen Missstand spekulieren. Letztlich ist es auch nicht entscheidend, ob die Daten aus Unkenntnis oder aus Nachlässigkeit nicht oder nicht sicher gelöscht wurden. Letztlich liegt es aber in der Verantwortung der jeweiligen Behördenleitungen, für die Einhaltung datenschutzrechtlicher Bestimmungen zu sorgen. Sie müssen sich – ggf. unter Beteiligung der behördlichen Datenschutzbeauftragten – davon vergewissern, dass personenbezogene Daten in ihrem Verantwortungsbereich hinreichend geschützt sind. Dies gilt auch für die Aussonderung von Datenträgern.

Kasten zu Nr. 8.3

Keine persönlichen Daten auf ausrangierten PC vergessen!

Tipps zur Vermeidung einer bösen Überraschung

Der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt in seiner Orientierungshilfe Sicheres Löschen magnetischer Datenträger (http://www.informationsfreiheit-mv.de/dschutz/informat/magloe/magloe.pdf) das kostenlose Windowsprogramm Eraser (http://www.heidi.ie/node/6). Ein anderes kostenloses Löschtool ist Darik's Boot and Nuke (DBAN), welches unter http://www.dban.org/ im Internet verfügbar ist.

Aber Vorsicht, denn wenn ein System mit der CD gebootet wird, wird jede vorhandene Festplatte gelöscht!

Unter Linux/Unix sind wipe oder das universelle und im Betriebssystem integrierte Tool „dd“ zum Überschreiben mittels Zufallszahlen nutzbar.

Zu beachten ist, dass auch Memory-Sticks und Speicherkarten z. B. aus Mobiltelefonen und Digitalkameras oftmals vertrauliche Daten enthalten und sicher entsorgt oder vor der Weitergabe sicher gelöscht werden müssen. Bei diesen Speichermedien kann ggf. schon das mehrfache Überschreiben zum gewünschten Erfolg führen. Zum sicheren Löschen auf derartigen Datenträgern gibt es auch kommerzielle Lösungen, die auf den einschlägigen Internet-Seiten gelistet sind.

Beim Neukauf von Festplatten empfiehlt sich auch der Abschluss einer Option, die oft mit Keep Your Drive bezeichnet ist und es im Garantiefall ermöglicht, die defekte Festplatte zu behalten.

Also nicht vergessen: Persönliche Daten vor der Weitergabe von Festplatten und anderer Hardware unbedingt sicher und unumkehrbar löschen!

8.4 Verbesserte IT-Sicherheit – aber nicht zu Lasten des Datenschutzes!

Im Regierungsnetz des Bundes, dem Informationsverbund Berlin-Bonn (IVBB), sollen weitere Filter und Schutzmechanismen installiert und das BSI mit neuen Befugnissen ausgestattet werden, um Schadprogramme zu erkennen und zu bekämpfen. Aber nicht alles, was mehr Sicherheit bringen soll, ist auch datenschutzrechtlich hinnehmbar.

Nach wie vor verursacht Schadsoftware, insbesondere Viren, Würmer und Trojaner, erhebliche Schäden. Besonders kritisch ist, dass die Angriffe immer ausgefeilter werden. Weltweit werden dadurch „normale“ PC so manipuliert, dass sie z. B. ohne Zutun des rechtmäßigen Benutzers Spam-E-Mail mit Schadensprogrammen versenden und damit zur Flut der unerwünschten E-Mail beitragen.

Die Angriffe auf die IT-Sicherheit beeinträchtigen nicht nur die ordnungsgemäße Abwicklung von Verwaltungsaufgaben, sondern bringen Gefahren für die Persönlichkeitsrechte der Bürgerinnen und Bürger mit sich. Daher sind Konzepte gefragt, die sowohl den Schutz der Privatsphäre gewährleisten und zugleich die IT-Sicherheit verbessern. Sie sollten bereits beim Systementwurf greifen und nicht erst nachträglich hinzugefügt werden müssen.

Leider wurden in weiten Bereichen von Wirtschaft und Verwaltung auch solche Maßnahmen zur Stärkung der IT-Sicherheit getroffen, die dazu führen, das Nutzerverhalten und sogar die Inhalte der Kommunikation zu registrieren und auszuwerten. Entsprechende Ansätze gibt es auch in der Bundesverwaltung. Im IVBB werden bereits wirksame Mechanismen gegen Spam-E-Mail und Schadprogramme eingesetzt. Gleichwohl sieht der vom BMI vorgelegte „Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes“ vor, dem BSI sehr weitgehende Befugnisse einzuräumen (s. Kasten zu Nr. 8.4). Als zentrale Meldestelle für IT-Sicherheit soll das BSI Informationen über Sicherheitslücken und neue Angriffsmuster sammeln und auswerten sowie Informationen und Warnungen an die betroffenen Stellen oder die Öffentlichkeit weitergeben. Kritisch sehe ich es, dass das BSI die Befugnisse erhalten soll, erheblich stärker als bisher E-Mail nach Schadprogrammen zu durchsuchen, den Zugriff auf Server mit Schadsoftware zu blockieren und die Protokolldateien des IVBB auszuwerten. Damit nehmen auch die Möglichkeiten des BSI zu, auf die Daten der Nutzer des IVBB zuzugreifen.

Bei allem Verständnis für das Anliegen in den gewachsenen, vernetzten IT-Strukturen einheitliche Sicherheitsstandards einzuführen, lege ich großen Wert darauf, dass die zur Risikobegrenzung eingeführten Maßnahmen nicht den Datenschutz der Nutzerinnen und Nutzer beeinträchtigen. Deshalb ist bei der Konzeption von IT-Sicherheitsmaßnahmen zu prüfen, ob datenschutzfreundlichere Ansätze das erforderliche Sicherheitsniveau ermöglichen. Z. B. können einheitlichere und strengere Sicherheitsstandards durch das BSI festgelegt werden. Außerdem können Protokolldateien und E-Mail-Daten vor der Auswertung pseudonymisiert werden. So wäre sichergestellt, dass nicht unnötig Nutzerdaten registriert und damit weitere Überwachungsmechanismen installiert werden.

Die Betreiber der „Netze des Bundes“, aber auch die Verantwortlichen für die übergreifenden Netze der Verwaltung in Europa sind aufgefordert, bei allen Maßnahmen zur Stärkung der IT-Sicherheit auch die Privatsphäre und den Datenschutz der Nutzerinnen und Nutzer zu berücksichtigen.

Kasten zu Nr. 8.4

Das Bundeskabinett hat Anfang 2009 den **Gesetzentwurf zur Stärkung der Sicherheit in der Informationstechnik des Bundes** beschlossen. Mit dem Gesetz sollen dem BSI weitere Befugnisse eingeräumt werden, um Gefahren für die Sicherheit der Informationstechnik des Bundes abzuwehren. Auch wenn das mit dem Gesetzentwurf verfolgte Ziel, die IT-Sicherheit zu verbessern, grundsätzlich anzuerkennen ist, bestehen erhebliche Bedenken gegen

- die Ermächtigung des BSI, die gesamte Datenkommunikation aller Unternehmen, Bürgerinnen und Bürger mit Bundesbehörden ohne Anonymisierung bzw. Pseudonymisierung auszuwerten,
- die vorgesehene Datenübermittlung an Strafverfolgungsbehörden, insbesondere bei nicht erheblichen Straftaten, wenn sie mittels Telekommunikation begangen werden, und an den Verfassungsschutz übermittelt werden und
- den Verzicht auf die Verpflichtung des BSI, ihm bekannt gewordene Sicherheitslücken und Schadprogramme zu veröffentlichen und damit Unternehmen, Bürgerinnen und Bürger vor zu erwartenden Angriffen (Spionage und Sabotage) zu warnen. Offenbar handelt es sich dabei um eine Konsequenz der Einführung der Online-Durchsuchung nach dem BKA-Gesetz (vgl. Nr. 4.3.1).

8.5 Kennzeichnungspflichten – Überlegungen zur Rückverfolgung von personenbezogenen Daten

Verbraucher können sich nicht wirksam gegen die ungewollte Verwendung Ihrer Daten wehren, wenn sie nicht wissen, aus welcher Quelle die Daten stammen. Unternehmen sollten dazu verpflichtet werden, die Herkunft und somit den rechtmäßigen Erwerb der Daten durch spezielle Kennzeichnung zu belegen.

Die Veräußerung von personenbezogenen Daten ist vor allem für den Handel ein zunehmend lukratives Geschäft. Unternehmen, die Kundendaten z. B. bei Bestellvorgängen vom Verbraucher erheben, geben diese oftmals gegen Entgelt, aber ohne explizite Zustimmung der Betroffenen (Opt-In) an andere Unternehmen weiter. Zudem werden Daten unrechtmäßig, also durch gezielte Angriffe von Hackern oder durch Insider entwendet. Um die zweifelsfreie Herkunft und den rechtmäßigen Erwerb von gehandelten Daten nachweisen zu können, wird darüber nachgedacht, personenbezogene Daten bereits bei ihrer Erhebung sicher zu kennzeichnen.

Der „Arbeitskreis Technische und organisatorische Datenschutzfragen (AK Technik) der Konferenz der Datenschutzbeauftragten des Bundes und der Länder“ hat sich im Oktober 2008 mit diesem Thema befasst (vgl. auch Nr. 2.3). Diskutiert wurden hierbei verschiedene technische Möglichkeiten, wie personenbezogene Datensätze zukünftig zum Herkunftsnachweis und zur Nachverfolgung ihrer Verwendung mit elektronischen Kennzeichnungen versehen werden könnten. Auch wenn diese Untersuchung zum Ergebnis kommt, dass eine wasserdichte technische Lösung des Kennzeichnungsproblems derzeit nicht verfügbar ist, wird damit die Forderung nach der Herkunftskennzeichnung von Daten nicht obsolet. Wenn Unternehmen bei der Werbeansprache den Adressaten zukünftig mitteilen müssten, woher die verwendeten Daten ursprünglich stammen, würde dies auch dann die Rechte der Betroffenen stärken, wenn Falschkennzeichnungen nicht sicher ausgeschlossen werden können. Die Betroffenen – aber auch die Aufsichtsbehörden – könnten sich ohne weiteres davon vergewissern, ob die Daten tatsächlich aus der angegebenen Quelle stammen und ob die Voraussetzungen für die Weitergabe und Nutzung der Daten zu Werbezwecken vorliegen.

Ausgangspunkt der Überlegungen des AK Technik war die Forderung, dass für Betroffene nachvollziehbar sein sollte, von wem die Daten erhoben wurden, auf welchem Weg ihre Daten zu Absendern von Werbepost oder anderen Kommunikationspartnern gelangt sind und wer sich dabei ggf. nicht auf die Einwilligung des Betroffenen stützen kann. Dabei können selbst technisch perfekte Verfahren lediglich der Revision dienen. Auch sie können nicht verhindern, dass bei entsprechender krimineller Energie oder bei bewusster Missachtung von Kennzeichnungspflichten Daten unberechtigt weitergegeben werden. Unabhängig von der technischen Realisierung sind zunächst verschiedene Verfahren denkbar:

- Der Ersterheber dokumentiert den Ursprung der Daten und ggf. die Einwilligung des Betroffenen in die Weitergabe. Jeder weitere Nutzer der Daten vermerkt wiederum die Herkunft. Anhand der Herkunftskette ist somit nachvollziehbar, wo die Daten erhoben und an wen sie weitergegeben wurden. Nachteilig ist, dass jeder auch nur kurzfristige Nutzer der Daten dauerhaft Informationen zum verwendeten Datensatz speichern muss.
- Informationen über Herkunft und Einwilligung sind jeweils dem Datensatz beizufügen. Nachteilig ist hierbei, dass neben dem Betroffenen auch der letzte Nutzer der Daten die gesamte Herkunftskette einsehen kann.
- Informationen zur Herkunft und Einwilligung könnten bei einer unabhängigen und vertrauenswürdigen dritten Stelle gespeichert werden. Allerdings würde sich bei einer solchen dritten Stelle ein sehr großer Datenbestand ansammeln und auch diese könnte zudem die Herkunftskette nachvollziehen.

Es ist in jedem Einzelfall abzuwägen, ob es vertretbar ist, für die lückenlose Nachvollziehbarkeit der Herkunftskette von Daten neue Datenbestände zu erzeugen.

Es sind Speicherfristen zu definieren und ggf. elektronische Kennzeichnungsmöglichkeiten, wie die Nutzung von pseudonymen Signaturen oder andere Verfahren, zu prüfen.

In der Diskussion sind auch weitere vor allem technische Verfahren wie elektronische Signaturen, DRM (Digital Rights Management), digitale Wasserzeichen oder Sticky Policy (s. Kasten zu Nr. 8.5), welche jedoch eines gewissen Implementationszeitraums und ggf. einer Weiterentwicklung bedürfen. Sie erscheinen deshalb derzeit nicht so schnell umsetzbar:

Denkbar wären auch manuelle Dokumentationspflichten, wie sie sich etwa im Pelzhandel und in der Landwirtschaft bewährt haben. Hierbei müsste jeder Nutzer von Adressdaten die Verwendung der Daten dokumentieren. Eine solche Lösung ist ohne spezielle Anpassungen bisheriger Verfahren schnell umsetzbar. Sie ist jedoch nicht manipulationssicher und müsste durch Sanktionen gestärkt werden. Ein angedachtes Verfahren mit einem zusätzlichen Datenfeld, mit dem eine ganze Herkunftskette modelliert werden könnte, könnte schnell realisiert werden, auch wenn dieses Verfahren ebenfalls nicht vor Manipulationen schützt und einer unrechtmäßigen Weitergabe der Daten nur bedingt entgegengewirkt werden kann.

Im Ergebnis lässt sich insgesamt festhalten, dass organisatorische Verfahren recht schnell umsetzbar erscheinen, da die eher technisch ausgerichteten Verfahren tieferer Eingriffe in die Hard- und Software bei den Nutzern der Daten bedürfen. Die Kennzeichnung von Datensätzen zur Herkunftsüberprüfung halte ich jedenfalls für zeitnah realisierbar. Weiter zu entwickelnde und zukünftige technische Verfahren könnten die Kennzeichnung von Daten längerfristig sicherer gestalten und nachhaltig vor Manipulationen schützen.

Kasten zu Nr. 8.5

Technische Verfahren zur Kennzeichnung von Daten

– Elektronische Signatur:

  Hierzu muss jede Stelle, die Adressdaten weitergibt, die Datensätze signieren. Der Empfänger der Daten muss dann jeweils die Signaturen auf ihre Gültigkeit hin überprüfen. Trägt ein Datensatz keine Signatur, handelt es sich um ein direkt beim Betroffenen erhobenes Datum bzw. um einen Datensatz, der nicht von einem Zwischenhändler bezogen wurde. Mithilfe von elektronischen Signaturen kann der Herkunftsnachweis so anhand der aufgebauten Signaturkette nachvollzogen werden.

– Digitales Rechtemanagement (DRM):

  Das zum Schutz urheberrechtlich geschützter digitaler Dokumente verwendete DRM beinhaltet ein Wasserzeichen zum Herkunftsnachweis sowie eine Verschlüsselung des Datums. Zudem sollen kryptographische Verfahren die Integrität der Daten sicherstellen und vor unberechtigter Nutzung schützen. Allerdings sind heutige DRM-Verfahren eher auf Audio- und Videodaten sowie Dokumente ausgerichtet und müssten für einen Einsatz im Adresshandel angepasst werden. Zudem ist der Einsatz dieser Technologie mit datenschutzrechtlichen Nebenwirkungen verbunden und erscheint daher kaum geeignet.

– Digitales Wasserzeichen:

  Der Herkunftsnachweis könnte mittels eines digitalen Wasserzeichens im Adressdatensatz integriert werden. Denkbar ist auch der Einsatz so genannter „fragiler Wasserzeichen“, um Manipulationen am Datensatz erkennen zu können. Wegen des geringen Datenvolumens eines Adressdatensatzes erscheint die Unterbringung eines Wasserzeichens jedoch nur schwer möglich. Denkbar wäre jedoch die Markierung ganzer Dokumente. Um bei mehreren vorhandenen Markierungen feststellen zu können, wann welches eingebracht wurde, wäre zudem ein kryptographischer Zeitstempeldienst notwendig.

– Sticky Policy:

  Grundlage für die Nutzung einer Sticky („klebrigen“) Policy ist eine unabhängige dritte Stelle (Tracing und Auditing Authority), die Datenschutzaudits bei Unternehmen durchführt und als Treuhänder fungiert. Kommuniziert ein Nutzer mit einem Diensteanbieter, so findet im Vorfeld eine Datenschutzvereinbarung statt und der Nutzer verschlüsselt seine personenbezogenen Daten, versieht sie mit einer auf Extensible Markup Language (XML, eine Auszeichnungssprache zur Darstellung hierarchisch strukturierter Daten in Form von Textdaten) basierenden Sticky Policy und versendet sie an den Diensteanbieter. Will ein Diensteanbieter einen Datensatz nutzen, so muss er sich an die Tracing Authority wenden und dort den Schlüssel zur Entschlüsselung des Datensatzes anfordern. Die Tracing Authority überprüft nun, ob die Systeme noch mit dem ursprünglich auditierten Zustand konform sind. Diese kann auch alle Anfragen der Dienstleister an sie aufzeichnen und ggf. die Daten auf ein „Verfallsdatum“ der Einwilligung hin überprüfen oder vor der Nutzung die Einwilligung des Betroffenen einholen bzw. ihn hierüber informieren. Problematisch bei dieser Lösung ist in erster Linie die Nutzerakzeptanz, da man nicht davon ausgehen kann, dass jeder Nutzer seinen Datensatz mit einer solchen Policy versehen wird und das System sich derzeit noch im Entwicklungsstadium befindet. Denkbar wäre jedoch die Integrationen eines solchen Prozesses beim Datenerheber. Insgesamt überwiegen bei diesem Verfahren eher die positiven Eigenschaften und rechtfertigen den zu treibenden Aufwand für das Datenschutzaudit.

9 Finanzwesen

9.1 IdentifikationsNummer für steuerliche Zwecke (Steuer-ID) – rechtlicher Rahmen –

Seit dem 1. August 2008 erfolgt der Versand der Mitteilungsschreiben über die zugeteilten Steuer-ID durch das Bundeszentralamt für Steuern (BZSt).

In der Vergangenheit habe ich mehrfach darauf hingewiesen, dass ich die Kennzeichnung der gesamten Bevölkerung der Bundesrepublik Deutschland mit einer eindeutigen Steuer-ID sehr kritisch sehe (vgl. 20. TB Nr. 8.2; 21. TB Nr. 8.1). Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat darauf hingewiesen, dass einheitliche Personenkennzeichen erhebliche Risiken für das Recht auf informationelle Selbstbestimmung bergen (vgl. Kasten zu Nr. 9.1). Besondere Gefahren erwachsen daraus, dass sich aus der Steuer-ID ein Personenkennzeichen entwickeln könnte, über das alle möglichen Datenbestände verknüpft und umfassende Persönlichkeitsprofile erstellt werden könnten. Angesichts der stetig verbesserten technischen Möglichkeiten, zunächst verteilt gespeicherte Daten anwendungsübergreifend zu verknüpfen, sind entsprechende Begehrlichkeiten abzuwehren.

Dies gilt auch für jede Erweiterung der beim BZSt nach § 139b Absatz 3 AO eingerichteten Datenbank (s. Nr. 9.2; 9.3) und insbesondere dann, wenn sensible Daten an das BZSt übermittelt werden sollen. Dies betrifft etwa im Melderegister der Kommunen vermerkte Übermittlungssperren, die einem besonderen Schutz unterliegen. Melderegistersperren werden eingerichtet, wenn vom Betroffenen glaubhaft gemacht werden kann, dass eine Weitergabe der Meldedaten eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen herbeiführt. Meldebehörden dürfen die Datensätze dieser Personen nur übermitteln, wenn hierfür eine eindeutige gesetzliche Grundlage geschaffen wird. Entsprechend habe ich es begrüßt, als im Rahmen des Jahressteuergesetzes 2008 § 139b Absatz 5 AO dahingehend geändert wurde, dass Übermittlungssperren nach dem Melderechtsrahmengesetz und den Meldegesetzen der Länder zu beachten und im Fall einer zulässigen Datenübermittlung ebenfalls zu übermitteln sind.

Im Mai 2008 habe ich beim BZSt einen Informationsbesuch durchgeführt, um mir die bisherigen Verfahrensschritte wie die Übermittlung der über 80 Millionen Meldedaten ab dem 1. Juli 2007 durch die Meldebehörden nach § 139b Absatz 6 AO und die Konsolidierung der Daten sowie die Erörterung der weiteren Bearbeitungsschritte im Zusammenhang mit der mehrmals verschobenen Einführung der Steuer-ID erläutern zu lassen.

Leider lag das von mir mehrfach angemahnte endgültige verfahrensspezifische IT-Sicherheitskonzept zum Redaktionsschluss immer noch nicht vor. Daher konnte ich bisher keine abschließende datenschutztechnische Stellungnahme abgeben.

Ich halte es für sehr bedenklich, dass die beim BZSt zum Zwecke der eindeutigen Identifizierung aller Steuerpflichtigen eingerichtete riesige Datenbank seit Monaten ohne ein angemessenes IT-Sicherheitskonzept betrieben wird. Dieses Vorgehen des BZSt werde ich nach § 25 BDSG als Verstoß gegen § 9 BDSG und Anlage beanstanden, sollte mir nicht Anfang 2009 ein datenschutzrechtlich zufrieden stellendes IT-Sicherheitskonzept vorliegen.

Bei der Anfang August 2008 begonnenen Zusendung der Mitteilungsschreiben des BZSt zur Steuer-ID kam es zu größeren Schwierigkeiten, z. T. mit Auswirkungen auf den Datenschutz. Mich erreichten hierzu viele Eingaben.

So beschwerten sich Betroffene, die vor 1945 in den ehemals deutschen Ostgebieten geboren wurden, darüber, dass in den Mitteilungsschreiben des BZSt der Geburtsort unzutreffend als im Ausland liegend angegeben war, z. B. Polen als Geburtsland bei einem Geburtsort im ehemals dem Deutschen Reich in den Grenzen von 1937 angehörenden Schlesien. Das BMF hat mir hierzu mitgeteilt, in den Meldegesetzen von Bund und Ländern sei nicht vorgeschrieben, dass der Geburtsstaat in das Melderegister einzutragen sei. In vielen Fällen, vor allem in der ehemaligen DDR, sei nicht der historisch zutreffende, sondern der jeweils aktuelle Staat eingetragen worden. Das BMF habe daraufhin sichergestellt, dass keine potentiell von der Vertriebenenproblematik betroffenen Datensätze mehr versandt würden, bis bei den Meldebehörden eine Korrektur erfolgt sei. Auch werde sichergestellt, dass Betroffenen, die bereits ein Mitteilungsschreiben erhalten hätten, ein korrigiertes Schreiben übersandt werde.

Als weitere problematische Fälle sind anzuführen:

In Mitteilungsschreiben des BZSt wurden zum Teil sachfremde Eintragungen wie der Name des Vermieters, der Name des ehemaligen Eigentümers sowie ein Kürzel hinsichtlich der Wohnsituation des Steuerpflichtigen EFH (Einfamilienhaus) oder MFH (Mehrfamilienhaus) aufgenommen. Das BMF teilte mir hierzu mit, das BZSt erhalte diese Angaben von Meldebehörden; es habe daher keinen Einfluss auf die im Mitteilungsschreiben aufgeführten Daten.

Ich habe das BMI als das für das Melderecht zuständige Ressort gebeten, diesen Sachverhalt zu bewerten. Ergebnisse lagen bei Redaktionsschluss noch nicht vor.

Darüber hinaus habe ich das BMF insbesondere unter Berücksichtigung der Entscheidung des Bundesverfassungsgerichtes vom 13. Juni 2007 (1 BvR 1550/03, s. Nr. 9.4) darauf hingewiesen, dass eine gesetzlich normierte abschließende Aufzählung der Stellen, die neben den Finanzbehörden die steuerliche Identifikationsnummer erheben oder verwenden dürfen, datenschutzrechtlich geboten ist.

Das BMF sieht allerdings Schwierigkeiten, die Stellen zu benennen, welche die steuerliche Identifikationsnummer erheben und verwenden dürfen. Mich hat dieses Argument nicht überzeugt. Tatsächliche Schwierigkeiten rechtfertigen es nicht, das verfassungsrechtliche Gebot der Normenklarheit hintanzustellen. Bis zu einer Gesetzesänderung sollte eine abschließende Aufzählung der Stellen zumindest in den Anwendungserlass zur AO erfolgen.

Eine Antwort des BMF hierzu steht noch aus.

Kasten zu Nr. 9.1

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008

Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen

Elektronische Identitäten sind der Schlüssel zur Teilnahme an der digitalen Welt. Die Möglichkeiten der pseudonymen Nutzung, die Gewährleistung von Datensparsamkeit und -sicherheit und der Schutz vor Identitätsdiebstahl und Profilbildung sind wichtige Grundpfeiler moderner Informations- und Kommunikationstechnologien. Darauf hat die Bundesregierung zu Recht anlässlich des Zweiten Nationalen IT-Gipfels im Dezember 2007 (Hannoversche Erklärung) hingewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass der gesetzliche Rahmen für die anonyme oder pseudonyme Nutzung elektronischer Verfahren bereits seit langem vorhanden ist. Beispielsweise hat jeder Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 13 Absatz 6 Telemediengesetz).

Bisher werden jedoch anonyme oder pseudonyme Nutzungsmöglichkeiten nur sehr selten angeboten. Vielmehr speichern Wirtschaft und Verwaltung immer mehr digitale Daten mit direktem Personenbezug. Erschlossen werden diese Datenbestände in der Regel über einheitliche Identifizierungsnummern. Mit der lebenslang geltenden, bundeseinheitlichen Steuer-Identifikationsnummer (Steuer-ID) oder der mit der Planung der Gesundheitskarte zusammenhängenden, ebenfalls lebenslang geltenden Krankenversichertennummer werden derzeit solche Merkmale eingeführt. Auch mit der flächendeckenden Einführung des E-Personalausweises wird jeder Bürgerin und jedem Bürger eine elektronische Identität zugewiesen, mit der sie bzw. er sich künftig auch gegenüber E-Government-Portalen der Verwaltung oder E-Commerce-Angeboten der Wirtschaft identifizieren soll.

Einheitliche Personenkennzeichen bergen erhebliche Risiken für das Recht auf informationelle Selbstbestimmung. So könnte sich aus der Steuer-ID ein Personenkennzeichen entwickeln, über das alle möglichen Datenbestände personenbezogen verknüpft und umfassende Persönlichkeitsprofile erstellt werden. Angesichts der stetig verbesserten technischen Möglichkeiten, zunächst verteilt gespeicherte Daten anwendungsübergreifend zu verknüpfen, wachsen entsprechende Begehrlichkeiten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die effektive Nutzung von Informationstechnik und hohe Datenschutzstandards keinen Widerspruch bilden. Ein datenschutzförderndes Identitätsmanagement kann den Einzelnen vor unangemessener Überwachung und Verknüpfung seiner Daten schützen und zugleich eine moderne und effektive Datenverarbeitung ermöglichen. Entsprechende EU-Projekte wie PRIME (Privacy and Identity Management for Europe) und FIDIS (Future of Identity in the Information Society) werden im Rahmen des 6. Europäischen Forschungsprogramms „Technologien für die Informationsgesellschaft“ gefördert.

Identitätsmanagement sollte auf der anonymen oder pseudonymen Nutzung von elektronischen Verfahren und der dezentralen Haltung von Identifikationsdaten unter möglichst weitgehender Kontrolle der betroffenen Bürgerinnen und Bürger basieren. Datenschutzfördernde Identitätsmanagementsysteme schließen Verknüpfungen nicht aus, wenn die Nutzenden es wünschen oder wenn dies gesetzlich vorgesehen ist. Sie verhindern jedoch, dass unkontrolliert der Bezug zwischen einer elektronischen Identität und einer Person hergestellt werden kann. Unter bestimmten, klar definierten Bedingungen kann mit Hilfe von Identitätsmanagementsystemen sichergestellt werden, dass ein Pseudonym bei Bedarf bezogen auf einen bestimmten Zweck (z. B. Besteuerung) einer Person zugeordnet werden kann.

Identitätsmanagementsysteme werden nur dann die Akzeptanz der Nutzerinnen und Nutzer finden, wenn sie einfach bedienbar sind, ihre Funktionsweise für alle Beteiligten transparent ist, möglichst alle Komponenten standardisiert sind und die Technik von unabhängigen Dritten jederzeit vollständig nachprüfbar ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung daher auf, den Absichtserklärungen des IT-Gipfels Taten folgen zu lassen und den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzutreiben. Sowohl die öffentliche Verwaltung als auch die Wirtschaft sollte die Einführung solcher datenschutzfördernder Systeme unterstützen.

9.2 Was die Abgeltungssteuer mit der Religionszugehörigkeit zu tun hat

Die umfangreiche Datenbank beim Bundeszentralamt für Steuern (BZSt) wird um ein weiteres sensibles Datum, die Religionszugehörigkeit, erweitert.

Ich habe mich unter Hinweis auf § 3a BDSG immer wieder dafür eingesetzt, die bei der Errichtung neuer Datenverarbeitungssysteme zu nutzenden personenbezogenen Daten auf ein Minimum zu beschränken und den Kreis der Zugriffsberechtigten so klein wie möglich zu halten. Beim Unternehmenssteuerreformgesetz 2008 zeigte sich, dass diese Botschaft noch nicht überall angekommen zu sein scheint. An den Beratungen zu dem Entwurf, vor allem zur Einführung der Abgeltungssteuer und den damit zusammenhängenden Änderungen beim Kontenabrufverfahren, habe ich mich intensiv beteiligt. Das Gesetz ist am 18. August 2007 in Kraft getreten (BGBl. I 2007, 1912).

Leider scheint die sich mit der Einführung der Abgeltungssteuer bietende Chance zur Verringerung des Umfangs der Verarbeitung personenbezogener Daten (vgl. 20. TB Nr. 7.3) weitgehend ungenutzt zu bleiben. Zudem sehe ich jede Erweiterung der beim BZSt eingerichteten Datenbank zur Steuer-Identifikationsnummer (vgl. Nr. 9.1) kritisch, vor allem, weil zusätzliche besonders geschützte Daten, wie die Religionszugehörigkeit, aufgenommen werden sollen (s. Nr. 9.3).

Nach § 51a EStG wird ab 2009 auf Kapitalerträge – bei Kirchensteuerpflicht des Empfängers – Kirchensteuer als Zuschlag zur Abgeltungssteuer erhoben. Bis Ende 2010 haben die Steuerpflichtigen ein Wahlrecht, ihre Religionszugehörigkeit freiwillig mitzuteilen. Sie können gegenüber der Bank erklären, dass ihre Kirchensteuer – wie die Steuer auf Kapitalerträge – im Abzugsverfahren von der Bank einbehalten und an das zuständige Finanzamt abgeführt wird. Der Steuerabzug wird danach über das für den Kirchensteuerabzug zuständige Finanzamt an die Religionsgemeinschaft weitergeleitet. Die Alternative ist – wie bisher – die Veranlagung durch das Finanzamt.

Ziel der Reform ist nach der Begründung zu § 51a Absatz 2e EStG jedoch, auch bei der Erhebung der auf die Kapitalerträge anfallenden Kirchensteuer den Steuerabzug grundsätzlich an der Quelle, d. h. bei den Kreditinstituten, vorzunehmen. Dieses Ziel lasse sich nur erreichen, wenn die zum Abzug verpflichtete Stelle in Zukunft in die Lage versetzt werden könne, den Abzug entsprechend der Zugehörigkeit zu einer Religionsgemeinschaft durchzuführen oder zu unterlassen, falls eine entsprechende Mitgliedschaft nicht vorliege. Dies soll, so die Begründung, durch eine elektronische Abfrage der Religionszugehörigkeit beim BZSt erreicht werden. Damit werde den Kirchen das Aufkommen der Kirchensteuer dauerhaft gesichert.

Obwohl § 51a Absatz 2e EStG vorsieht, dass die Bundesregierung zunächst über die Auswirkungen der Wahlmöglichkeiten berichtet und die Erfahrungen evaluiert, präjudiziert die Gesetzesbegründung ein Verfahren, das ich als besonders kritisch betrachte. Ich bin der Auffassung, dass auch weiterhin die Banken nur dann Kenntnis von der Religionszugehörigkeit ihrer Kunden haben sollten, wenn diese damit einverstanden sind.

Letztlich ist zu befürchten, dass die Einführung der Abgeltungssteuer so zu einer umfangreicheren und nicht zu einer reduzierten Verarbeitung personenbezogener Daten führt.

9.3 Jahressteuergesetz 2008 – Ablösung der Lohnsteuerkarte durch ein elektronisches Abrufverfahren

Mit dem Jahressteuergesetz 2008 wurde die rechtliche Grundlage für die Ablösung des Lohnsteuerkartenverfahrens durch ein elektronisches Abrufverfahren geschaffen. Hierzu wird die beim Bundeszentralamt für Steuern (BZSt) errichtete Datei um weitere sensible Daten (Lohnsteuerabzugsmerkmale) ergänzt. Von der zunächst vorgesehenen Einführung des datenschutzrechtlich bedenklichen „Anteilsverfahrens" wurde abgesehen.

Das am 8. November 2007 verabschiedete Jahressteuergesetz 2008 beinhaltet einige datenschutzrechtlich bedeutsame Neuregelungen. Mit § 39e EStG ebnet es den Weg für die Ablösung des Lohnsteuerverfahrens mittels Lohnsteuerkarte durch ein elektronisches Abrufverfahren (ElsterLohn II) ab dem Jahre 2011. Der Arbeitgeber erhält die Lohnsteuerabzugsmerkmale, die ihm die Berechnung der einzuhaltenden Lohnsteuer und der Kirchensteuer der bei ihm beschäftigten Arbeitnehmer ermöglichen, nicht mehr durch die Lohnsteuerkarte, sondern elektronisch beim BZSt. Der Arbeitgeber (bei Beschäftigungsbeginn) erhält die Möglichkeit, die in der Steuer-Datenbank über den jeweiligen Arbeitnehmer beim BZSt gespeicherten Lohnsteuerabzugsmerkmale wie Steuerklasse, Religionszugehörigkeit (auch für Ehepartner und Kinder einschließlich derer Steuer-Identifikationsnummern (Steuer-ID) sowie Höhe der Kinderfreibeträge abzurufen. Dazu hat sich der Arbeitgeber zu authentifizieren und seine Wirtschafts- sowie die Steuer-ID (vgl. Nr. 9.1) und das Geburtsdatum des Arbeitnehmers mitzuteilen. Die Authentisierung erfolgt über das ELSTER-Online-Portal mittels geheim zu haltendem Authentifizierungszertifikat und Passwort. Die Lohnsteuerabzugsmerkmale werden dann nach positiver Prüfung durch das BZSt annähernd vier Millionen Arbeitgebern bereitgestellt. Ein direkter Zugriff des Arbeitgebers auf die Steuerdatenbank erfolgt nicht.

Die Speicherung dieser Daten in einer zentralen Datenbank wirft zusätzliche Fragen auf. So werden zahlreiche Datensätze auf Vorrat angelegt, da auch Personen betroffen sind, die keine Arbeitnehmer sind. Der durch die Vergabe der Steuer-ID an alle Bundesbürger beim BZSt entstandene Datenpool wird damit noch erweitert. Die Vereinbarkeit dieser riesigen Datensammlung mit dem verfassungsrechtlich gebotenen Erforderlichkeitsgrundsatz erscheint zweifelhaft. Außerdem sehe ich die Gefahr, dass die zentrale Datenbank Begehrlichkeiten bei anderen Stellen weckt. So wären die dort gespeicherten Daten sicherlich auch für Sozialleistungsträger oder Strafverfolgungsbehörden von Interesse. Weiter ist zu befürchten, dass diese Erweiterung der Datenbank beim BZSt nicht den Schlusspunkt darstellt, weicht sie doch die erst beim Jahressteuergesetz 2003 erreichte strikte Zweckbindung auf (vgl. dazu 21. TB Nr. 8.1). Schließlich birgt das elektronische Abrufverfahren die Gefahr der missbräuchlichen Verwendung der Arbeitnehmerdaten.

Die datenschutzrechtlichen Bedenken, die von den Datenschutzbeauftragten der Länder geteilt werden (s. Entschließung der 74. Datenschutzkonferenz, Kasten a zu Nr. 9.3), wurden im Gesetzgebungsverfahren leider nicht berücksichtigt.

Auch hinsichtlich der Sicherheit des Authentifizierungsverfahrens über das ELSTER-Portal bin ich nach wie vor skeptisch. Wie ich bereits im 21. TB (Nr. 4.4.1; 8.4) ausführlich berichtet habe, ist zwar gemäß § 87a Absatz 3 AO die Zulassung der qualifizierten Signatur für Steuerpflichtige obligatorisch; daneben kann aber gemäß § 87a Absatz 6 AO unter den näheren Voraussetzungen der Steuerdatenübermittlungs-Verordnung (StDÜV) ein anderes sicheres Verfahren zugelassen werden, das die Authentizität und die Integrität des übermittelten elektronischen Dokuments sicherstellt. Bei der Beurteilung, ob das ELSTER-Authentifizierungsverfahren diesen Anforderungen genügt, ist zu berücksichtigen, dass sich mit der Entwicklung der Technik das Angriffspotential auch auf für Dritte „interessante“ Daten erhöhen wird und deshalb permanent Nachbesserungen des Authentifizierungsverfahrens erforderlich sein werden. Dementsprechend hat die 76. Datenschutzkonferenz (s. Kasten b zu Nr. 9.3) darauf hingewiesen, dass das Verfahren der qualifizierten elektronischen Signatur nach dem Signaturgesetz im Hinblick auf die Authentizität und Integrität elektronisch übermittelter Dokumente derzeit maßgeblich sein müsse. Außerdem müssten die Steuerpflichtigen die Möglichkeit haben, ihre elektronische Kommunikation mit der Finanzverwaltung durch die qualifizierte elektronische Signatur abzusichern.

Erfreulich ist, dass das Vorhaben der ebenfalls durch das Jahressteuergesetz vorgesehenen Einführung des sog. Anteilsverfahrens für Ehegatten nicht weiter verfolgt wurde. Zur Durchführung des Anteilsverfahrens für die Einbehaltung der Lohnsteuer vom laufenden Arbeitslohn sollte auf Antrag beider Eheleute auf jeder Lohnsteuerkarte der Prozentsatz eingetragen werden, der dem Anteil des Arbeitslohns des jeweiligen Ehegatten am Gesamtarbeitslohn beider Ehegatten entspricht. Damit hätte aber der Arbeitgeber deutlich genauere Rückschlüsse auf das Einkommen des jeweils anderen, nicht bei ihm beschäftigten Ehegatten, ziehen können als nach geltendem Recht. Stattdessen sieht das Jahressteuergesetz 2009 nur ein „optionales Faktorverfahren“ vor, welches Ehegatten, die der Steuerklasse IV zuzuordnen sind, anstelle der Kombination Klasse III/V auf freiwilliger Basis beantragen können. Im Unterschied zum Anteilsverfahren erfährt der Arbeitgeber der Ehegatten hierdurch nicht den Prozentsatz in ganzen Zahlen, der dem Anteil des jeweiligen Arbeitslohns am Gesamtarbeitslohn beider Ehegatten entspräche, sondern lediglich die Steuerklasse IV in Verbindung mit einem Faktor zur Ermittlung und Abführung der Lohnsteuer.

Kasten a zu Nr. 9.3

Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2007

Zentrale Steuerdatei droht zum Datenmoloch zu werden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für inakzeptabel, dass die Bundesregierung mit dem Jahressteuergesetz 2008 im Schnelldurchgang ohne ausführliche parlamentarische Beratung die beim Bundeszentralamt für Steuern aufzubauende zentrale Steuerdatei um zusätzliche – teilweise sensible – Daten anreichern will. Zugleich droht die Steueridentifikationsnummer (Steuer-ID) bereits vor ihrer endgültigen Einführung zu einem allgemeinen Personenkennzeichen zu werden.

Der Gesetzentwurf sieht die Ablösung des Lohnsteuerkartenverfahrens durch ein elektronisches Abrufverfahren (ElsterLohn II) ab 2011 vor. Bereits am 9. November 2007 soll das Gesetz abschließend im Bundestag beraten werden. Geplant ist unter anderem, die in Zusammenhang mit der seit dem 1. Juli 2007 vergebenen Steuer-ID errichtete Datenbank um weitere Daten zu ergänzen, etwa um die Religionszugehörigkeit, Ehepartner/Ehepartnerinnen/Kinder und deren Steuer-ID, dazu Angaben über Steuerklassen. Hierbei werden auch zahlreiche Datensätze auf Vorrat aufgenommen, da auch Personen betroffen sind, die (noch) keine Arbeitnehmer/ Arbeitnehmerinnen sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert vom Bundestag und Bundesrat, dieses Vorhaben der Umstellung auf ein elektronisches Verfahren mit dem Jahressteuergesetz 2008 nicht zu beschließen. Folgende Punkte sind datenschutzrechtlich kritisch:

– Der durch die Vergabe der Steueridentifikationsnummer an alle Steuerpflichtigen und damit für alle Einwohnerinnen und Einwohner der Bundesrepublik entstehende Datenpool erhält eine neue Dimension. Zwar sind die Lohnsteuerabzugsmerkmale auch bisher auf der Lohnsteuerkarte vermerkt. Die Speicherung dieser Daten in einer zentralen Datenbank würde aber erhebliche datenschutzrechtliche Fragen aufwerfen. In den zentralen Datenbestand würden die Daten aller Personen mit Lohnsteuerkarten einfließen, also auch von solchen Personen, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Es ist zweifelhaft, ob die Aufnahme dieses Personenkreises dem Erforderlichkeitsgrundsatz entspricht. Nützlichkeitserwägungen sind für eine Datenhaltung auf Vorrat in keinem Fall ausreichend.

- Die Daten würden bundesweit annähernd vier Millionen Arbeitgebern zur Verfügung stehen. Als einzige Sicherung ist dabei vorgesehen, dass nur ein autorisierter Arbeitgeber die Lohnsteuerabzugsmerkmale abrufen kann. Klärungsbedürftig ist allerdings, wie dies sichergestellt werden kann. Zwar ist ein Authentifizierungsverfahren für den Arbeitgeber vorgesehen. Die Frage ist jedoch, ob damit tatsächlich eine rechtswidrige Informationsbeschaffung Dritter auszuschließen ist. Zumindest sollten die Daten aus der zentralen Datenbank nur unter Mitwirkung der Betroffenen abgerufen werden können.
- Die gesetzlich vorgeschriebene Evaluierung des Verfahrens (§ 87a Absatz 6 AO) ist noch nicht erfolgt. Gleichzeitig existieren bereits jetzt Bestrebungen, die Kommunikationsplattform „Elster“ für Nutzungen durch andere Verwaltungszweige zu öffnen (OpenElster). Dies aber bedeutete, dass damit die Steuer-ID auch für die Identitätsfeststellung bei steuer*fremden* Anwendungen herangezogen werden könnte, ohne damit der strikten Zweckbindung nach § 139b Absatz 5 Abgabenordnung zu rein steuerlichen Zwecken Rechnung zu tragen. Diese Zweckbindung kann nach § 139b Absatz 2 AO auch nicht durch die jeweilige Einwilligung der betroffenen Bürgerinnen und Bürger überwunden werden. Mit OpenElster sollen diese Vorkehrungen offenbar aufgeweicht werden, bevor die Steuer-ID überhaupt eingeführt wurde. Allein dies macht deutlich, dass jede Erweiterung des zentralen Datenbestandes kritisch hinterfragt werden muss.

Schließlich ist zu befürchten, dass die vorgesehene Erweiterung der Datenbank beim BZSt nicht den Schlusspunkt darstellt. Die im neuen Datenpool gespeicherten Daten wären auch für Sozialleistungsträger und Strafverfolgungsbehörden interessant. Es gibt zahlreiche Beispiele, dass Daten, die zunächst nur für einen engen Zweck gespeichert werden dürfen, später für viele andere Zwecke verwendet werden: Die für steuerliche Zwecke erhobenen Daten über Freistellungsaufträge werden mit den ebenfalls beim BZSt gespeicherten Daten der Empfänger von BAFöG- und anderen Sozialleistungen abgeglichen. Die Mautdaten, die zunächst nur zur Mautberechnung erhoben wurden, sollen zukünftig auch zur Strafverfolgung verwendet werden. Der zunächst ausschließlich zur Terrorismusbekämpfung und der Bekämpfung der organisierten Kriminalität eingeführte Kontendatenabruf steht heute auch Finanzämtern und anderen Behörden wie z. B. der Bundesagentur für Arbeit über das BZSt offen. Das BZSt enthält so einen einzigartigen aktuellen Datenpool aller Bundesbürgerinnen und -bürger, der wesentliche Meldedaten, Bankkontenstammdaten und Steuerdaten zentral verknüpfen kann.

Kasten b zu Nr. 9.3

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008

Elektronische Steuererklärung sicher und datenschutzgerecht gestalten

Mit dem Steuerbürokratieabbaugesetz (Bundesratsdrucksache 547/08) sollen u. a. verfahrenstechnische Regelungen für die elektronische Übermittlung von Steuererklärungen durch Steuerpflichtige festgelegt werden. Zu diesem Zweck soll § 150 Abgabenordnung (AO) durch Absatz 7 Satz 1 dahingehend ergänzt werden, dass bei Einführung einer Verpflichtung zur elektronischen Abgabe die übermittelten Steuerdaten mit einer qualifizierten Signatur nach dem Signaturgesetz zu versehen sind.

Die Konferenz sieht es kritisch, dass § 150 Absatz 7 Satz 2 Nr. 6 und 7 AO auch vorsieht, zur Erleichterung und Vereinfachung des automatisierten Besteuerungsverfahrens anstelle der qualifizierten elektronischen Signatur ein so genanntes anderes sicheres Verfahren im Benehmen mit dem Bundesinnenministerium zuzulassen oder sogar auf beide Verfahren vollständig zu verzichten. In der Gesetzesbegründung wird darauf verwiesen, dass neben der qualifizierten elektronischen Signatur künftig auch eine Übermittlung der Daten unter Nutzung der Möglichkeiten des neuen elektronischen Personalausweises möglich sein soll.

Bereits in ihrer Entschließung zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren vom 11. Oktober 2006 hat die Konferenz gefordert, Nutzenden die Möglichkeit zu eröffnen, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt daher die vorgesehene Regelung in der AO zur Nutzung der qualifizierten elektronischen Signatur, da dieses Verfahren geeignet ist, die Authentizität und Integrität eines elektronisch übermittelten Dokuments sicherzustellen, und somit die handschriftliche Unterschrift ersetzen kann.

Die Datenschutzbeauftragten des Bundes und der Länder erklären hierzu:

1) Das Verfahren der qualifizierten elektronischen Signatur nach dem Signaturgesetz ist im Hinblick auf die Authentizität und Integrität elektronisch übermittelter Dokumente derzeit alternativlos.
2) Für die Bewertung anderer Verfahren sollte unmittelbar auf die Fachkenntnis unabhängiger Gutachter abgestellt werden. Als Gutachter für die Beurteilung der technischen Sicherheit kämen etwa die Bundesnetzagentur oder das BSI in Frage.
3) Steuerpflichtige müssen auch im elektronischen Besteuerungsverfahren die Möglichkeit haben, die elektronische Kommunikation mit der Finanzverwaltung durch das hierfür geeignete Verfahren der qualifizierten elektronischen Signatur abzusichern.

9.4 Kontenabrufverfahren durch die Finanzämter und andere Behörden

Der Gesetzgeber musste die vom Bundesverfassungsgericht wegen mangelnder Bestimmtheit für verfassungswidrig erklärte Rechtsgrundlage in der Abgabenordnung neu fassen.

Schon im Gesetzgebungsverfahren zum Gesetz zur Förderung der Steuerehrlichkeit (BGBl. I 2003 S. 2928) im Jahre 2003 habe ich u. a. kritisiert, dass § 93 Absatz 8 AO den Kreis der zum Kontenabruf berechtigten Behörden nicht präzise festlege und es daher an der erforderlichen Normenklarheit fehle. Es werde nicht geregelt, welche Behörden zu welchem Zweck eine Kontenabfrage durchführen dürfen. Darüber hinaus habe ich darauf hingewiesen, dass routinemäßige oder anlasslose Abrufe nicht erfolgen dürften. Daher sollten Kontenabrufe nur im Rahmen konkreter Verdachtsmomente erlaubt sein (s. im einzelnen 20. TB Nr. 8.3; 21. TB Nr. 8.2).

Mit den Datenschutzbeauftragten der Länder habe ich gefordert, die Neuregelung vor allem im Hinblick auf das verfassungsrechtliche Gebot der Normenklarheit und Transparenz zu überarbeiten (s. 20. TB Kasten b zu Nr. 8.3).

Mit Beschluss vom 13. Juni 2007 (1 BvR 1550/03) hat das Bundesverfassungsgericht über die Ende 2004 eingereichten Verfassungsbeschwerden, die sich gegen §§ 93 Absatz 7 und 8 AO richteten, entschieden. Während § 93 Absatz 7 AO danach mit dem Grundgesetz vereinbar ist, wurde die Verfassungsmäßigkeit von § 93 Absatz 8 AO wegen des Verstoßes gegen das rechtsstaatliche Gebot der Normenklarheit verneint. Zum einen, so das BVerfG, bestimme § 93 Absatz 8 AO den Kreis der Behörden, die ein Ersuchen zum Abruf von Kontostammdaten stellen können, nicht hinreichend. Zum anderen lege § 93 Absatz 8 AO die Aufgaben, denen ein solches Ersuchen dienen solle, nicht ausreichend fest. Des Weiteren stellte das BVerfG im Hinblick auf §§ 93 Absatz 7 und 8 AO klar, dass Auskunftsverlangen und Kontenabrufe nicht „ins Blaue hinein“ erfolgen dürften. Vielmehr bedürfe es dazu konkreter Anhaltspunkte, allgemeiner Erfahrungswerte oder sonstiger Belege für die Erforderlichkeit der Maßnahme. Schließlich müsse ein routinemäßiger, anlassloser Einsatz der Abfragen verhindert werden und die Möglichkeit bestehen, Missbräuche im Nachhinein durch effektive Datenschutzkontrollen aufzudecken.

Der Gesetzgeber hat dementsprechend § 93 Absatz 8 AO alte Fassung durch insgesamt drei Absätze (§ 93 Absatz 8 bis 10 AO neue Fassung) ersetzt. Aus § 93 Absatz 8 AO ergeben sich mittelbar die Behörden, die zum Kontenabruf berechtigt sind, die Abrufvoraussetzungen und Zweckbestimmungen. So können z. B. durch die Arbeitsverwaltung Kontenabrufe im Rahmen der Überprüfung der Berechtigung zum Bezug von Arbeitslosengeld II erfolgen. § 93 Absatz 9 AO bestimmt, dass der Betroffene grundsätzlich auf die Möglichkeit des Kontenabrufs vorab hinzuweisen und über dessen Durchführung zu benachrichtigen ist, nennt aber auch Ausnahmen von dieser Hinweis- und Benachrichtigungspflicht, etwa soweit die Benachrichtigung die ordnungsgemäße Erfüllung der in der Zuständigkeit des Ersuchenden liegenden Aufgaben gefährden würde. § 93 Absatz 10 AO legt schließlich fest, dass ein Antrag auf Kontenabruf und dessen Ergebnis vom Antragsteller zu dokumentieren sind.

Erneut hat sich im Berichtszeitraum die Anzahl der Kontenabrufe erhöht (vgl. 21. TB Nr. 8.2). Ende 2008 betrug das Abfragevolumen annähernd 200 Abrufe, das Abfragekontingent dagegen bis zu 2000 Abfragen täglich. Ob sich die Zunahme der Zahl der Abrufe weiter fortsetzen wird, bleibt abzuwarten.

Besonderes kritisch sehe ich es, dass das Kontenabrufverfahren nicht nur für öffentlich-, sondern auch für privatrechtliche Zwecke genutzt werden soll. So sieht etwa der Entwurf eines Gesetzes zur Reform der Sachaufklärung in der Zwangsvollstreckung (Bundestagsdrucksache 16/10069) eine Auskunftsmöglichkeit des Gerichtsvollziehers zur Durchsetzung titulierter zivilrechtlicher Ansprüche vor (§ 802 Absatz l ZPO-E).

9.5 Auskunftsanspruch in der Abgabenordnung

Obwohl das BMF zugesagt hat, ein Auskunftsrecht analog § 19 BDSG in die Abgabenordnung aufzunehmen, ist noch immer keine gesetzliche Regelung vorhanden.

Seit vielen Jahren treten die Datenschutzbeauftragten des Bundes und der Länder dafür ein, das von Verfassung wegen gebotene Auskunftsrechts der Betroffenen über die zu ihrer Person gespeicherten Daten auch gegenüber der Finanzverwaltung zu gewährleisten. Aus diesem Grund habe ich mich nachdrücklich für die Aufnahme eines Auskunftsrecht in die AO eingesetzt. Bestärkt werde ich durch einen Beschluss des BVerfG (Beschluss vom 10. März 2008, 1 BvR 2388/0), in dem der Auskunftsanspruch nach § 19 BDSG gegenüber der Finanzverwaltung unmittelbar für anwendbar erklärt wurde. Einer (Finanz-)Behörde, stellt das BVerfG klar, komme kein Ermessen bei der Entscheidung über die Auskunftsgewährung zu. Dies aber hat das BMF bisher stets vertreten.

Diese richterliche Klarstellung ist auch deshalb so wichtig, weil es kaum ein anderes, für die Bürgerinnen und Bürger ähnlich bedeutsames Gebiet hoheitlichen Handelns gibt, das fast 30 Jahre nach Inkrafttreten des BDSG und 25 Jahre nach dem Volkszählungsurteil des BVerfG vergleichbar große datenschutzrechtliche Defizite aufweist wie die AO.

Das BMF machte daraufhin den Vorschlag, § 19 BDSG durch eine Bestimmung der AO „für entsprechend anwendbar“ zu erklären.

Die vorgeschlagene Regelung habe ich zwar im Interesse der Normenklarheit grundsätzlich begrüßt, aber darauf hingewiesen, dass sie aufgrund der unmittelbaren Geltung des § 19 BDSG in der AO nur deklaratorische Bedeutung habe. Keinesfalls dürfe zudem daraus der Schluss gezogen werden, andere Betroffenenrechte, insbesondere §§ 19a bis 21 sowie §§ 3a, 4b und 6 BDSG wären ausgeschlossen, da diese nicht für entsprechend anwendbar erklärt wurden.

Vor diesem Hintergrund hielt ich es jedoch – schon wegen der Eilbedürftigkeit des Gesetzgebungsverfahrens – für nachvollziehbar, dass das BMF „zunächst" ausschließlich die Regelung des Auskunftsrechts vorhatte. Im Entwurf des Jahressteuergesetzes 2009 hätte damit zumindest in der Begründung sehr klar verdeutlicht werden müssen, dass der Auskunftsanspruch nur der Einstieg in eine bereichsspezifische Regelung aller datenschutzrechtlichen Betroffenenrechte ist.

Das BMF hat jedoch im Juni 2008 die Einführung eines Auskunftsrechts in der AO aus dem Gesetzentwurf gänzlich herausgenommen. Zwar sei man sich mit den obersten Finanzbehörden des Bundes und der Länder einig, bereichsspezifische Datenschutzregelungen in der AO zu schaffen, es bestehe aber noch Abstimmungsbedarf.

Die Mehrheit der Länder habe sich daher dafür ausgesprochen, das Auskunftsrecht zunächst im Wege einer bundeseinheitlichen Verwaltungsanweisung zu regeln. Danach soll den Beteiligten auf Antrag Auskunft über die zu ihrer Person gespeicherten Daten erteilt werden, jedoch nur wenn sie ein berechtigtes Interesse darlegen.

Dies sehe ich kritisch, zumal sowohl der Auskunftsanspruch des Betroffenen aus § 19 BDSG, dessen uneingeschränkte Geltung auch für die Finanzverwaltung vom BVerfG festgestellt worden ist, als auch der Anspruch auf Zugang zu deutlichen Informationen nach § 1 Absatz 1 IFG grundsätzlich „voraussetzungslos" besteht. Die Verwaltung darf also weder eine Begründung für die Geltendmachung des Anspruchs verlangen, noch weitere Bedingungen aufstellen, die über den gesetzlichen Rahmen hinausgingen. Es ist deswegen rechtswidrig, wenn in einer internen untergesetzlichen Regelung der Finanzverwaltung die Erfüllung der Ansprüche von einem „berechtigten Interesse" abhängig gemacht würde, was die Gesetze selbst, auf die sich die Betroffenen berufen können, nicht vorsehen. Eine entsprechende Verkürzung der gesetzlichen Betroffenenrechte ist inakzeptabel und würde einer gerichtlichen bzw. verfassungsgerichtlichen Überprüfung mit Sicherheit nicht standhalten. Im Übrigen habe ich unter Hinweis auf die Entschließung des Deutschen Bundestages vom 17. März 2009 (Bundestagsdrucksache 16/12271 – s. Kasten zu Nr. 9.5) erneut aufgefordert, einen § 19 BDSG entsprechenden Auskunftsanspruch unter Einbeziehung der weiteren Betroffenenrechte (s. o.) in die AO aufzunehmen. Eine Antwort des BMF hierauf steht noch aus.

Kasten zu Nr. 9.5

Aus der Entschließung des Deutschen Bundestages zum 21. Tätigkeitsbericht vom 17. März 2009, Bundestagsdrucksache 16/12271

…

5. Der Deutsche Bundestag hat zuletzt in seiner Entschließung zum 20. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die Bundesregierung an ihre Zusage erinnert, den betroffenen auch gegenüber der Steuerverwaltung einen Anspruch auf Auskunft zu den über sie gespeicherten Daten einzuräumen. Gleichzeitig hatte er die Bundesregierung aufgefordert, ihre Prüfungen über die personellen, organisatorischen und haushalterischen Auswirkungen eines solchen Auskunftsanspruchs zeitnah abzuschließen.

Dieser Aufforderung ist die Bundesregierung noch immer nicht nachgekommen. Der Deutsche Bundestag fordert die Bundesregierung deshalb erneut auf, den Auskunftsanspruch des Betroffenen auch in der Steuerverwaltung sicherzustellen.

…

10 Gesundheit und Soziales

10.1 Das Gendiagnostikgesetz: Der Anfang ist gemacht

Die Arbeiten an einem Gendiagnostikgesetz kommen endlich voran.

Genanalysen erlauben inzwischen lange vor dem Ausbruch einer Krankheit Vorhersagen über deren Eintrittswahrscheinlichkeit, selbst wenn dem Betroffenen seine Anfälligkeit für diese Krankheit nicht bekannt ist. Auch lassen Genanalysen Rückschlüsse auf die medizinische Konstellation von Blutsverwandten zu, ohne dass diese an dem Verfahren beteiligt sind. Deshalb habe ich in meinen letzten Tätigkeitsberichten (vgl. 20. TB Nr. 2.6; 21. TB Nr. 13.2) bereits mehrfach auf die Notwendigkeit einer gesetzlichen Regelung von genetischen Untersuchungen hingewiesen.

Die Bundesregierung hat am 27. August 2008 endlich den Entwurf eines Gendiagnostikgesetzes (GenDG) vorgelegt, der zahlreiche datenschutzrechtliche Forderungen erfüllt (Bundestagsdrucksache 16/10532). Allerdings wird der Anwendungsbereich auf genetische Untersuchungen zu medizinischen Zwecken, zur Klärung der Abstammung sowie im Versicherungsbereich und im Arbeitsleben beschränkt. Das Gesetz enthält keine Rechtsvorschriften für genetische Untersuchungen und Analysen sowie den Umgang mit genetischen Proben und Daten zu Forschungszwecken. Dies wird damit begründet, dass es bei der genetischen Forschung um die allge-

meine Erforschung von Ursachenfaktoren menschlicher Eigenschaften gehe, die nicht auf konkrete Maßnahmen gegenüber einzelnen Personen abziele. Das ist zwar generell zutreffend, Ziel der genetischen Forschung ist aber auch, die Wechselbeziehung zwischen genetischen und Umweltfaktoren aufzuklären und konstitutionelle Faktoren zu identifizieren, die dann zu bestimmten An- und Auffälligkeiten führen.

Wird die Forschung nicht in das GenDG einbezogen, richtet sich der Datenschutz für diesen Bereich nach den Bestimmungen des BDSG und der Ländergesetze. Dies ist nicht sinnvoll, da diese Gesetze nur allgemeine Vorgaben enthalten.

Ferner fehlen im Gesetzentwurf Regelungen für vorhandene Gendatenbanken. Pseudonymisierungsverfahren in diesen Datenbanken werden also auch in Zukunft nicht verbindlich vorgeschrieben und auch die Rechte der Betroffenen bleiben hier unklar.

Dagegen begrüße ich die im Gesetzentwurf vorgesehenen Straf- und Bußgeldvorschriften. Die Differenzierung zwischen strafrechtlicher Sanktionierung und Bußgeldbewehrung erfolgt nach dem Gefährdungs- bzw. Missbrauchspotential; so wird die unzulässige Verwendung von genetischen Daten strafrechtlich geahndet, während das unzulässige Verlangen von genetischen Daten lediglich eine Ordnungswidrigkeit darstellt. Diese grundsätzliche Differenzierung erscheint angemessen.

Bei den nun ausstehenden parlamentarischen Beratungen werde ich mich dafür einsetzen, die genannten Regelungslücken zu schließen.

10.2 Gesetzliche Krankenversicherung

10.2.1 Steuerungsmaßnahmen der gesetzlichen Krankenkassen

Versorgungsmanagement ist erwünscht, aber ohne Druck und datenschutzkonform.

Mit der Gesundheitsreform soll die Qualität und Effizienz der gesetzlichen Krankenkassen verbessert werden. Die Kassen streben daher an, Versicherten ein Versorgungsmanagement anzubieten. Von zentraler Bedeutung sind dabei Patientenschulungsmaßnahmen und strukturierte Behandlungsprogramme für chronisch kranke Versicherte. Diese Maßnahmen sollen für die Versicherten jedoch lediglich Angebotscharakter haben. Ihre Teilnahme soll nach dem Willen des Gesetzgebers freiwillig sein und eine eingehende Unterrichtung voraussetzen. Zur Teilnehmergewinnung und Durchführung der Maßnahmen bedienen sich die Kassen vielfach privater Dienstleister und offenbaren diesen teils höchst sensible Gesundheitsdaten ihrer Versicherten. Dies ist datenschutzrechtlich nach dem Sozialgesetzbuch jedoch unzulässig, wenn die Übermittlung ohne Kenntnis und vorherige Einwilligung der jeweiligen Versicherten erfolgt.

So können Versicherte z. B. nach § 137f Absatz 3 Satz 2 SGB V an strukturierten Behandlungsprogrammen, sog. Disease-Management-Programmen (DMP), auf freiwilliger Basis teilnehmen, wenn sie nach umfassender Information durch ihre Krankenkasse schriftlich eine Einwilligung zur Teilnahme an dem Programm und zur Erhebung, Verarbeitung und Nutzung der nach § 266 Absatz 7 SGB V festgelegten Daten erteilen. Zahlreiche Kassen haben die Aufgabe „Information der Versicherten“ sowie „Unterstützungsleistungen zur Gewinnung von Versicherten für DMP“ auf einen privaten Dienstleister übertragen. Dieser wiederum nutzt nicht selten Call-Center zur Aufgabenerledigung. Um die Gewinnung potenzieller Teilnehmer durchführen zu können, werden dem Dienstleister von der Krankenkasse alle Versicherten mit entsprechenden DMP-Indikationen gemeldet, bevor diese in die Datenweitergabe eingewilligt haben. Die Rekrutierungsleistungen des Dienstleisters bestehen u. a. aus bis zu drei Mailings für Versicherte und/oder bis zu drei telefonischen „Nachfass-Aktionen“. Hierbei wird nicht selten Druck auf die Versicherten ausgeübt, sich für ein DM-Programm zu entscheiden, zumal dann, wenn der Dritte durch „Erfolgsprämien“ von der Anzahl der hinzugewonnenen Teilnehmer profitiert.

Die datenschutzrechtliche Problematik liegt darin, dass für die Rekrutierung neuer DMP-Teilnehmer von den Kassen Patientendaten ohne vorherige Kenntnis oder gar Einwilligung der Betroffenen an private Dienstleister übermittelt werden. Darüber hinaus werden die Versicherten mit den massiven nachhaltigen Mail- und Telefonmarketingaktionen derart bedrängt, dass die gesetzlich gewollte Freiwilligkeit stark zu bezweifeln ist.

Die Datenschutzbeauftragten von Bund und Ländern haben daher in ihrer 76. Konferenz am 6./7. November 2008 eine Entschließung hierzu gefasst (hierzu s. Kasten zu Nr. 10.2.1).

Das Bundesgesundheitsministerium unterstützt die Datenschutzbeauftragten in ihrer Auffassung.

Ich habe die Problematik dem Spitzenverband der Krankenkassen mitgeteilt und um Unterstützung für die Umsetzung der datenschutzrechtlichen Eckpunkte gebeten. Eine Antwort steht noch aus.

Kasten zu Nr. 10.2.1

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008

Steuerungsprogramme der gesetzlichen Krankenkassen datenschutzkonform gestalten

Mit der Gesundheitsreform soll über die Einführung von Wettbewerbsmechanismen die Qualität und Effizienz der gesetzlichen Krankenkassen verbessert werden. Die Kassen sind daher bemüht und auch vom Gesetzgeber gehalten, Versicherten ein Versorgungsmanagement anzubieten. Von zentraler Bedeutung sind dabei Patientenschulungsmaßnahmen und strukturierte Behandlungsprogramme für chronisch kranke Versicherte, die jedoch lediglich Angebotscharakter haben dürfen. Ihre Teilnahme soll nach dem Willen des Gesetzgebers freiwillig sein und eine eingehende Unterrichtung voraussetzen. Diese Vorgaben werden von einzelnen Krankenkassen nicht beachtet, wenn sie versuchen, die Versicherten in ihrem Gesundheitsverhalten zu steuern und sie in bestimmte Maßnahmen und Programme zu drängen. Um Teilnehmerinnen und Teilnehmer zu gewinnen und um Maßnahmen durchzuführen, bedienen sich die Kassen vielfach privater Dienstleister und offenbaren diesen teils höchst sensible Gesundheitsdaten ihrer Versicherten. Dies ist datenschutzrechtlich nach dem Sozialgesetzbuch unzulässig, wenn die Übermittlung ohne Kenntnis und vorherige Einwilligung der jeweiligen Versicherten erfolgt. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält die Einhaltung insbesondere der folgenden Eckpunkte bei gesundheitlichen Steuerungsprogrammen der Krankenkassen für unerlässlich:

- Die Krankenkassen dürfen Versichertendaten nur dann zur Auswahl von Personen für besondere Gesundheitsmaßnahmen verwenden, wenn dies gesetzlich ausdrücklich vorgesehen ist. Es muss sich um valide und erforderliche Daten handeln. Mit der Auswahl darf kein privater Dienstleister beauftragt werden.
- Die erstmalige Kontaktaufnahme mit potenziell für eine Gesundheitsmaßnahme in Betracht kommenden Versicherten muss durch die Krankenkasse selbst erfolgen, auch wenn ein privater Dienstleister mit der späteren Durchführung der Gesundheitsmaßnahme beauftragt worden ist.
- Die Versicherten sind vor Übermittlung ihrer Daten umfassend zu informieren. Die Information muss auch den Umstand umfassen, dass ein privates Unternehmen mit der Durchführung betraut werden soll. Soweit die Versicherten ausdrücklich in die Teilnahme eingewilligt haben, dürfen die für die Durchführung der Maßnahme erforderlichen Daten an den Dienstleister übermittelt werden.
- Wenn Versicherte – zu welchem Zeitpunkt auch immer – eindeutig zum Ausdruck bringen, nicht an einer Maßnahme teilnehmen zu wollen oder nicht an weitergehenden Informationen, einer konkreten Anwerbung oder einer fortgesetzten Betreuung interessiert zu sein, ist dies zu respektieren. Weitere Maßnahmen (auch telefonische Überredungsversuche) sind zu unterlassen.

10.2.2 Zusammenarbeit der gesetzlichen Krankenkassen mit privaten Dritten

Gesetzliche Krankenkassen bedienen sich zur Erledigung ihrer Aufgaben in verstärktem Umfang privater Unternehmen und Ärzten, teilweise unter Verstoß gegen den Datenschutz.

Von den Krankenkassen werden private Dienstleistungsunternehmen herangezogen, um z. B. Krankenhausrechnungen zu überprüfen. Private Call-Center führen im Auftrag der Kassen Gesundheitsberatungen für Versicherte durch oder bieten den Versicherten Leistungen der Kasse an. Kassen verlangen von behandelnden Ärzten, ihnen dabei behilflich zu sein, chronisch kranke Versicherte zu identifizieren, die für bestimmte Behandlungsprogramme der Kassen in Betracht kommen. Dabei ist vielfach zweifelhaft, ob die Kasse die jeweilige Aufgabe überhaupt einem Dritten übertragen darf und welche Datenflüsse im Rahmen der Aufgabenerledigung in Gang gesetzt werden dürfen.

Sozialversicherungsträger – und damit auch die Krankenkassen – haben ihre vom Gesetzgeber übertragenen Aufgaben grundsätzlich selbst zu erfüllen. Sie sind deshalb im Regelfall nicht befugt, sie auf Dritte zu delegieren, die sie dann in eigener Verantwortung wahrnehmen. Anders als privatwirtschaftliche Unternehmen darf ein Sozialversicherungsträger nur dann Aufgaben durch einen Dritten durchführen lassen, wenn das Gesetz dies ausdrücklich vorsieht. § 80 SGB X erlaubt unter engen Voraussetzungen eine sog. Datenverarbeitung im Auftrag (s. Kasten a zu Nr. 10.2.2). Diese Sonderform der Datenverarbeitung durch einen Dritten beschränkt sich aber auf manuelle, technische oder sonstige Hilfs- und Unterstützungsleistungen zur Erfüllung der Datenverarbeitungsaufgaben. Diese gesetzlich legitimierte Auftragsdatenverarbeitung ist abzugrenzen von einer Funktionsübertragung, bei der

gesetzliche Aufgaben der Krankenkasse auf einen Dritten übertragen werden und von diesem selbstverantwortlich wahrgenommen werden. Bereits eine eigenständige Entscheidungskompetenz des Dritten oder der Umstand, dass seine Arbeit mit einem Erfolgshonorar vergütet wird, spricht dafür, dass keine Auftragsdatenverarbeitung vorliegt.

Deshalb muss im Einzelfall sorgfältig geprüft werden, ob ein Dritter überhaupt eingeschaltet werden darf. Nach § 197b SGB V können Krankenkassen ihnen obliegende Aufgaben durch Dritte wahrnehmen lassen, wenn dies wirtschaftlicher ist, es im wohlverstandenen Interesse der Versicherten liegt und deren Rechte nicht beeinträchtigt werden (s. Kasten b zu Nr. 10.2.2). Kernaufgaben der Kassen dürfen allerdings nicht Dritten in Auftrag gegeben werden. So dürfen z. B. Beratungs- und Aufklärungsleistungen der Krankenkassen über Rechte und Pflichten der Versicherten nach dem Sozialgesetzbuch, die die Kassen gegenüber ihren Versicherten erbringen müssen (§§ 11 bis 15 SGB I), nicht an Dritte vergeben werden.

Kasten a zu Nr. 10.2.2

§ 80 Abs. 5 SGB X:

Die Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag durch nichtöffentliche Stellen ist nur zulässig, wenn

1. beim Auftraggeber sonst Störungen im Betriebsablauf auftreten können oder
2. die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst. Der überwiegende Teil der Speicherung des gesamten Datenbestandes muss beim Auftraggeber oder beim Auftragnehmer, der eine öffentliche Stelle ist und die Daten zur weiteren Datenverarbeitung im Auftrag an nichtöffentliche Auftragnehmer weitergibt, verbleiben.

Hat die Kasse eine ihr obliegende Aufgabe zulässigerweise an einen Dritten übertragen, stellt sich die Frage, ob und ggf. welche Versichertendaten dazu weitergegeben werden dürfen. Sofern es sich um Angebote an die Versicherten für Patientenschulungsmaßnahmen, besondere Behandlungsprogramme etc. handelt, dürfen Versichertendaten nicht ohne Weiteres dem Dritten übermittelt werden. Hier muss zunächst die Kasse die Einwilligung ihrer Versicherten zum Datentransfer einholen (s. hierzu auch Beitrag unter Nr. 10.2.1).

Bei der Überprüfung von Krankenhausrechnungen durch private Dienstleistungsunternehmen ist der Dienstleister bei der Aufgabenerfüllung an die rechtlichen Grenzen gebunden, die auch für die Krankenkasse selbst gelten (§ 284 SGB V). In manchen Fällen haben die Krankenkassen keine eigene Befugnis zur Datenerhebung, wenn es z. B. um medizinische Fragen und Beurteilungen geht. Hier muss der medizinische Dienst der Krankenkassen nach § 275 SGB V eingeschaltet werden, was dann auch für den Dienstleister gilt. Ihm stehen keine gesonderten Rechte zu.

Ein spezieller Fall der Public Private Partnership hat mich in Form von sog. Arzt-Patienten-Potenziallisten beschäftigt, mit denen Teilnehmer an strukturierten Behandlungsprogrammen gewonnen werden sollen. So hat eine große Krankenkasse niedergelassene Ärzte angeschrieben und jeweils eine Liste der bei ihr versicherten Patienten des betreffenden Arztes beigefügt. Diese Liste sollte der Arzt um die Angaben ergänzen, ob bei dem Patienten eine chronische Erkrankung vorliege und ob er für ein entsprechendes von der Kasse angebotenes Behandlungsprogramm in Frage komme. Diese Vorgehensweise hat zu erheblicher Verunsicherung bei der Ärzteschaft geführt. Zwar sind die Krankenkassen gesetzlich verpflichtet, strukturierte Behandlungsprogramme für Versicherte mit bestimmten chronischen Erkrankungen durchzuführen. Hierzu hat der Gesetzgeber den Kassen die Möglichkeit eröffnet, die Daten auszuwerten, die ihnen zu Abrechnungszwecken von ärztlichen Leistungen und Rezepten zur Verfügung stehen und die in Frage kommenden Versicherten gezielt anzusprechen. Die Kassen dürfen allerdings nur die Daten auswerten, über die sie rechtmäßig verfügen. Auch muss sich die Nutzung auf diejenigen Daten beschränken, die auf einem eindeutigen Auswertungsergebnis beruhen. Diesen Vorgaben entsprach das Verfahren aber nicht. Zum einen enthielten die Potenziallisten auch Angaben über Versicherte, die bei dem angeschriebenen Arzt gar nicht in Behandlung waren, und zum anderen waren dort nicht nur die Versicherten aufgeführt, bei denen von einer entsprechenden Erkrankung ausgegangen werden konnte. Darüber hinaus war zu bemängeln, dass es nicht nur zu einer unzulässigen Übermittlung von Versichertendaten gekommen war, sondern auch die erbetene Rückantwort der Ärzte mit entsprechenden konkreten Angaben über ihre Patienten eine unzulässige Datenerhebung der Kasse darstellte. Die Kasse hat meiner Kritik inzwischen Rechnung getragen und das Verfahren eingestellt.

Kasten b zu Nr. 10.2.2

§ 197b SGB V:

Krankenkassen können die ihnen obliegenden Aufgaben durch Arbeitsgemeinschaften oder durch Dritte mit deren Zustimmung wahrnehmen lassen, wenn die Aufgabenwahrnehmung durch die Arbeitsgemeinschaften oder den Dritten wirtschaftlicher ist, es im wohlverstandenen Interesse der Betroffenen liegt und Rechte der Versicherten nicht beeinträchtigt werden. Wesentliche Aufgaben zur Versorgung der Versicherten dürfen nicht in Auftrag gegeben werden …

10.2.3 Keine Extra-Daten für den Risikostrukturausgleich

Die Praxis einiger gesetzlicher Krankenkassen, im Rahmen des morbiditätsorientierten Risikostrukturausgleichs Gesundheitsdaten ihrer Versicherten zu erheben, ist datenschutzrechtlich unzulässig.

Mit der Begründung, sich um eine möglichst valide Datengrundlage zur Durchführung des Gesundheitsfonds zu bemühen, werden Diagnoseangaben bei abrechnenden Ärzten abgefragt oder die Ärzte werden gebeten, Diagnoseangaben zu konkretisieren oder durch weitere Untersuchungen aufzuzeigen. Nach § 284 Absatz 1 Satz 1 Nummer 14 SGB V ist den Krankenkassen zwar eine Erhebung von Daten erlaubt, die zur Durchführung des Risikostrukturausgleichs (RSA) erforderlich sind. Näheres über Art und Umfang der für die Durchführung des RSA erforderlichen Daten regelt die Risikostrukturausgleichsverordnung (RSAV). Diese sieht aber lediglich vor, dass für die Weiterentwicklung und Durchführung des RSA die Krankenkassen jährlich die versichertenbezogenen Diagnosen aus den Abrechnungsunterlagen für die vertragsärztlichen Leistungen erheben (§ 30 Absatz 1 Satz 1 Nr. 6 RSAV). Zur Abrechnung im Rahmen der vertragsärztlichen Versorgung ist die Übermittlung von Patientendaten zwischen Ärzten und Krankenkassen jedoch nicht vorgesehen. Auch durch die Einholung von Einwilligungen der Versicherten kann dieser gesetzliche Rahmen nicht ausgeweitet werden.

Der Gesetzgeber hat mit Blick auf das Recht auf informationelle Selbstbestimmung eine auf das erforderliche Mindestmaß beschränkte Informationsbasis bei den Krankenkassen angestrebt. Daher sind Versuche, außerhalb des gesetzlich definierten Rahmens Diagnosen zu erlangen, datenschutzrechtlich unzulässig.

Meine Rechtsauffassung wird vom Bundesversicherungsamt als Aufsichtsbehörde über die gesetzlichen Krankenkassen geteilt.

10.2.4 Schwere Verstöße von Krankenkassen bei der Vermittlung privater Zusatzversicherungen

Im Zuge von Kontrollbesuchen habe ich bei zwei gesetzlichen Krankenkassen außergewöhnlich schwere datenschutzrechtliche Verstöße bei der Vermittlung von privaten Zusatzversicherungen festgestellt und in diesem Zusammenhang u. a. auch Strafanträge gestellt.

Nach § 194 Absatz 1a SGB V dürfen gesetzliche Krankenkassen den Abschluss privater Zusatzversicherungsverträge zwischen ihren Versicherten und privaten Krankenversicherungsunternehmen vermitteln. Bei zwei gesetzlichen Krankenkassen (der IKK Weser-Ems und der IKK Hamburg) habe ich in diesem Zusammenhang u. a. unangekündigt die Voraussetzungen und Grenzen zulässiger Vermittlungstätigkeiten kontrolliert und dabei erhebliche Datenschutzverstöße festgestellt.

Beide Krankenkassen hatten entsprechend mit ein und demselben privaten Krankenversicherungsunternehmen, der Signal Krankenversicherung a. G. (Signal Iduna), kooperiert. Zur Vermittlung von privaten Zusatzversicherungen boten diese gesetzlichen Krankenkassen dem privaten Versicherungsunternehmen zumindest über Monate, teilweise auch Jahre hinweg die Möglichkeit, in den Räumlichkeiten und an den Arbeitsplätzen der Kassen über Sozialdaten der gesetzlich Versicherten zu verfügen und diese an sich zu nehmen. Mitarbeitern der privaten Krankenversicherung wurden zum Zwecke der telefonischen Akquise in konkret hierfür elektronisch zusammengestellten Listen Sozialdaten (u. a. Name, Anschrift, Geburtsdatum, Krankenversichertennummer, Telefonnummer) der gesetzlich Versicherten ausgehändigt. Sodann telefonierten die Mitarbeiter der Privatversicherung die genannten Versicherten nach einem „Gesprächsleitfaden“, bzw. speziellen „Coachings“ in einer Weise ab, die den Angerufenen den Eindruck vermitteln sollte, von Mitarbeitern der gesetzlichen Krankenkasse kontaktiert worden zu sein. Den Angerufenen wurde also bewusst suggeriert, von dem besonderen Vertrauensverhältnis zwischen ihnen und „ihrer“ Krankenkasse ausgehen zu dürfen.

Im Zuge dieser Telefonate wurden von den Mitarbeitern des privaten Versicherungsunternehmens zusätzlich umfassende, oftmals äußerst sensible personenbezogene Daten (z. B. „Krebs/darmkrank“, „keine Zähne“, „behindert“, „Sozialhilfe“) erhoben und auf den Listen festgehalten. Außerdem führte eine der geprüften Krankenkasse unter dem Briefkopf des Privatversicherers „Mailing-Aktionen“ zur Bewerbung und Vermittlung privater Versicherungsprodukte durch. Dazu wurden Gesundheitsdaten der gesetzlich Krankenversicherten nach von der privaten Versicherung vorgegebenen Kriterien (z. B. HIV-Infektion, Alkohol-/Drogenmissbrauch, Depressionen, Krebserkrankung, Schlaganfall) als „Leistungsausschlussgründe“ ausgewertet. Betroffene, welche die genannten Voraussetzungen erfüllten, wurden dann nicht angeschrieben.

Damit haben beide Krankenkassen im Zusammenhang mit der Vermittlung privater Zusatzversicherungen den nach § 194 Absatz 1a SGB V zulässigen gesetzlichen Rahmen weit überschritten. Der entsprechende Umgang mit Sozialdaten ihrer Versicherten zu diesem Zweck erfolgte ohne Rechtsgrundlage und somit rechtswidrig. Ferner habe ich erhebliche Mängel bei den zum Schutz der Sozialdaten zu treffenden technischen und organisatorischen Maßnahmen festgestellt. Gegenüber den Vorständen der beiden Kassen habe ich deshalb gemäß § 81 Absatz 2 SGB X i. V. m. § 25 Absatz 1 BDSG insgesamt fünf Beanstandungen ausgesprochen und das Bundesversicherungsamt unterrichtet.

Ob eine solche Vorgehensweise auch bei anderen Krankenkassen praktiziert wird/wurde, habe ich auf Grund begrenzter Personalressourcen und anderer wichtiger Schwerpunktvorhaben im Berichtszeitraum nicht kontrollieren können.

Aufgrund der massiven, über einen langen Zeitraum betriebenen datenschutzrechtlichen Verstöße habe ich sowohl gegen Mitarbeiter beider gesetzlicher Krankenkassen als auch gegen Mitarbeiter des privaten Versicherungsunternehmens bei den zuständigen Staatsanwaltschaften Strafantrag gemäß § 85a Absatz 2 SGB X wegen Vergehen nach § 85a Absatz 1 i. V. m. § 85 Absatz 2 Nummern 1, 2, 3 und 5 SGB X gestellt. In beiden Fällen dauern die Ermittlungen noch an. Angesichts der außergewöhnlichen Schwere der datenschutzrechtlichen Verstöße habe ich darüber hinaus den Ausschuss für Gesundheit des Deutschen Bundestages, die Bundesministerin für Gesundheit und die für das private Versicherungsunternehmen zuständige Datenschutzaufsichtsbehörde informiert.

10.3 Gesetzliche Unfallversicherung

10.3.1 Gutachterregelung

Die seit langem umstrittene Gutachterregelung aus § 200 Absatz 2 SGB VII hat durch das Urteil des Bundessozialgerichts vom 5. Februar 2008 und die Gesetzesinitiative zur Änderung des SGB VII neue Impulse erhalten.

Mit Urteil vom 5. Februar 2008 (s. Kasten a zu Nr. 10.3.1) hat das Bundessozialgericht im Wesentlichen meine seit Langem vertretene Rechtsposition (u. a. 20. TB Nr. 19.1.3) bestätigt und festgestellt, dass § 200 Absatz 2 SGB VII auch für die von den Unfallversicherungsträgern im Laufe eines gerichtlichen Verfahrens eingeholte Gutachten gilt. Damit verbleibt kein datenschutzfreier Raum während eines anhängigen Gerichtsverfahrens. Die seitens der Berufsgenossenschaften erhobenen Bedenken gegen die Anwendung des § 200 Absatz 2 SGB VII in diesem Verfahrensstadium sind nicht durchgreifend, was ich immer hervorgehoben habe.

Kasten a zu Nr. 10.3.1

Kernsätze des Urteils des BSG vom 5. Februar 2008 – B 2 U 8/07 R – zu datenschutzrechtlich relevanten Fragen

- Der Begriff des Gutachtens ist als umfassende wissenschaftliche Bearbeitung einer im konkreten Fall relevanten fachlichen Fragestellung durch den Sachverständigen zu definieren.
- § 200 Abs. 2 SGB VII gilt auch für von den Unfallversicherungsträgern im Laufe eines Gerichtsverfahrens eingeholte Gutachten.
- Ein Rechtsverstoß gegen § 200 Abs. 2 SGB VII führt zu einem Beweisverwertungsverbot des eingeholten Gutachtens.

Datenschutzfreundlich ist auch die Feststellung des Bundessozialgerichts, bei einem Verstoß gegen § 200 Absatz 2 2. Halbsatz SGB VII i. V. m. § 76 Absatz 2 SGB X bestehe grundsätzlich ein Verwertungsverbot des eingeholten Gutachtens, weil das verletzte Widerspruchsrecht das Recht auf informationelle Selbstbestimmung konkretisiere. Es gebe dem Betroffenen die Möglichkeit, einer Übermittlung seiner besonders schutzwürdigen Daten an einen Gutachter zu widersprechen. Dabei ließ das Gericht die Frage offen, ob der gleichzeitige Verstoß gegen das Auswahlrecht nach § 200 Absatz 2 1. Halbsatz SGB VII ebenfalls zu einem Beweisverwertungsverbot führt. In der Praxis ist damit aber für die Betroffenen klargestellt, dass ihre unter Verstoß gegen die Regelungen zum Widerspruchsrecht eingeholten Gutachten nicht verwendet werden dürfen.

Das Bundessozialgericht hat sich auch eingehend mit der Frage befasst, wann begrifflich ein Gutachten im Sinne des § 200 Absatz 2 SGB VII vorliegt und wann lediglich eine beratungsärztliche Stellungnahme. Ein Gutachten liege nur bei einer umfassenden wissenschaftlichen Bearbeitung einer im konkreten Fall relevanten fachlichen Fragestellung durch den Sachverständigen vor, die vornehmlich eine eigenständige Bewertung der verfahrensentscheidenden Tatsachenfragen – wie beispielsweise des Ursachenzusammenhanges – enthalte. Setze sich die schriftliche Äußerung des Sachverständigen im Wesentlichen mit dem eingeholten Gerichtsgutachten auseinander, insbesondere im Hinblick auf dessen Schlüssigkeit, Überzeugungskraft und Beurteilungsgrundlage, sei es lediglich eine beratende Stellungnahme. Damit bestätigt das Bundessozialgericht die im Jahre 2003 zwischen dem Hauptverband der gewerblichen Berufsgenossenschaften, dem Bundesversicherungsamt und mir vereinbarten Kriterien zur Abgrenzung der Beauftragung mit einem Gutachten und der Einholung einer beratungsärztlichen Stellungnahme.

Wie sich in einer Vielzahl von Fällen – auch nach der Entscheidung des Bundessozialgerichts – gezeigt hat, ist das Problem, in welchen Fällen den Versicherten die in § 200 Absatz 2 SGB VII genannten Rechte zustehen, in der Praxis aber immer noch nicht zufrieden stellend gelöst. In diesen Fällen hatten die Berufsgenossenschaften beratende Ärzte mit umfassenden Gutachten zur Zusammenhangsfrage und zur Höhe der Minderung der Erwerbsfähigkeit beauftragt und die Auffassung vertreten, die genannte Regelung sei nicht anzuwenden, da ein beratender Arzt wie ein Mitarbeiter der Berufsgenossenschaft zu betrachten sei. Die Weitergabe der medizinischen Daten eines Versicherten an einen Beratungsarzt sei daher keine Datenübermittlung, und nur diese werde von § 200 Absatz 2 SGB VII umfasst.

Diese Auffassung vertritt auch das Landessozialgericht Nordrhein-Westfalen und auch das Urteil des Bundessozialgerichts lässt eine solche Interpretation zu. Damit wird aber die gesetzgeberische Intention, die Verfahrenstransparenz zu stärken, in ihr Gegenteil verkehrt. Eine Beschränkung des Anwendungsbereichs auf Gutachten eines externen Gutachters ergibt sich nicht aus dem Wortlaut der Vorschrift. Die Auslegung nach dem Zweck der Regelung kann eine solche Auslegung ebenso wenig stützen. Für den Versicherten ist es völlig undurchschaubar,

in welchen Fällen ein Unfallversicherungsträger einen Beratungsarzt mit dem Gutachten beauftragt oder einen externen Gutachter.

Ich halte eine gesetzliche Klarstellung der Regelung des § 200 Absatz 2 SGB VII für überfällig. Dies gilt insbesondere für die Streitfrage, ob ein Gutachten auch dann in den Anwendungsbereich des § 200 Absatz 2 SGB VII fällt, wenn es von einem beratenden Arzt einer Berufsgenossenschaft erstattet wird. Dies gilt insbesondere für die Feststellung, dass die genannten Rechte stets zu gewähren sind, unabhängig davon, welche vertraglichen Beziehungen zwischen dem Unfallversicherungsträger und dem Gutachter bestehen und auch unabhängig davon, in welchem Verfahrensstadium der Unfallversicherungsträger das Gutachten in Auftrag gibt. Nur so lässt sich das mit der Gutachterregelung des § 200 Absatz 2 SGB VII verfolgte Ziel erreichen, die Mitwirkungsrechte der Versicherten zu stärken und die Transparenz der unfallversicherungsrechtlichen Feststellungsverfahren zu erhöhen (s. Kasten b zu Nr. 10.3.1).

Zu meinem Bedauern ist das zuständige Ministerium meinen Vorschlägen bisher nicht gefolgt. Wegen der besonderen Bedeutung der Angelegenheit werde ich mich auch weiterhin dafür einsetzen, dass § 200 Absatz 2 SGB VII in dem von mir vorgeschlagenen Sinne geändert wird.

K a s t e n b zu Nr. 10.3.1

Vorschlag für eine geänderte datenschutzfördernde Fassung des § 200 Absatz 2 SGB VII: (die Änderungen zur geltenden Fassung sind kursiv hervorgehoben)

Vor Erteilung *jedes* Gutachtenauftrages soll der Unfallversicherungsträger dem Versicherten mehrere Gutachter zur Auswahl benennen; der Betroffene ist außerdem auf sein Widerspruchsrecht nach § 76 Absatz 2 des Zehnten Buches hinzuweisen und über den Zweck des Gutachtens zu informieren. *Der Versicherte hat das Recht, selbst einen Gutachter vorzuschlagen. Von dem Vorschlag des Versicherten kann nur aufgrund einer nachvollziehbaren Begründung abgewichen werden. Bei Nichtbeachtung der vorstehenden Regelungen ist das Gutachten zu löschen.*

10.3.2 Einschränkung des Auskunftsverlangens bei Krankenkassen nach § 188 Satz 2 SGB VII

Wird die Einschränkung des Auskunftsverlangens nach § 188 Satz 2 SGB VII nicht beachtet, werden die gesetzlich festgelegten Verantwortungsregelungen verschoben.

Unfallversicherungsträger haben mir gegenüber mehrfach die Auffassung vertreten, medizinische Daten über Vorerkrankungen eines Versicherten, die den Unfallversicherungsträgern von einer Krankenkasse in einem über ihre Erhebungsbefugnis hinausgehendem Umfang übermittelt wurden, müssten erst nach einer von ihnen vorzunehmenden Prüfung gelöscht werden. Die Unfallversicherungsträger nutzen die ihnen unrechtmäßig übermittelten Daten für ihre Ermittlungen und löschen sie erst dann, wenn sie nach ihrer Auffassung zur Bearbeitung eines konkreten Einzelfalles nicht benötigt werden.

Diese von den Unfallversicherungsträgern vertretene Auffassung hat in mehreren Einzelfällen dazu geführt, dass eingeholte Gutachten unter Verwendung unzulässig erhobener Informationen über Vorerkrankungen erstattet wurden und sich damit möglicherweise auf nicht zu verwendende Daten stützten. Dies widerspricht der gesetzgeberischen Wertung des § 188 Satz 2 SGB VII, nach der bereits bei der Datenerhebung der Grundsatz der Erforderlichkeit zu beachten ist. Die Unfallversicherungsträger sollen bereits ihr Auskunftsverlangen auf solche Erkrankungen oder Krankheitsbereiche beschränken, die mit dem Versicherungsfall in einem ursächlichen Zusammenhang stehen können. Ausnahmen von Sollvorschriften sind nur in atypischen Ausnahmefällen zulässig. Sollte daher eine Berufsgenossenschaft grundsätzlich alle Vorerkrankungen erheben und erst nach Erhalt des gesamten Vorerkrankungsverzeichnisses entscheiden, welche Daten sie für die Bearbeitung eines konkreten Einzelfalles für erforderlich hält, steht dies nicht im Einklang mit der gesetzlichen Regelung des § 188 Satz 2 SGB VII. Mit der Speicherung aller Vorerkrankungen und der Übermittlung dieser gesamten Daten an einen Gutachter wird die Regelung unterlaufen.

Ich werde weiterhin auf die korrekte Gesetzesanwendung bei der Erhebung der Vorerkrankungsdaten durch die Unfallversicherungsträger hinwirken.

10.4 Gesetzliche Rentenversicherung Der ärztliche Entlassungsbericht in der medizinischen Rehabilitation – wer darf ihn bekommen?

Der Reha-Entlassungsbericht der Deutschen Rentenversicherung ist ein ärztlicher Brief mit besonderer Bedeutung. Aber nicht jeder, der ein Interesse daran hat, darf ihn erhalten. (s. Kasten zu Nr. 10.4)

Da der Entlassungsbericht sensible personenbezogene Daten enthält, ist es von besonderer Bedeutung, wer den Bericht oder Teile desselben bekommen darf und unter welchen Voraussetzungen er Kenntnis erhält. Zu dieser Thematik liegen mir mehrere Beschwerden vor. Bis 2008 wurde der betroffene Rehabilitand vom Arzt der Reha-Einrichtung beim Abschlussgesprächs gefragt, ob er damit einverstanden sei, dass der Bericht oder Teile desselben an den behandelnden Arzt, die Krankenkasse oder den Medizinischen Dienst der Krankenkassen (MDK) übermittelt würden. Die Übermittlung erfolgte dann oft routinemäßig an die verschiedenen Stellen, ohne dass im jeweiligen Einzelfall geprüft wurde, ob die Kenntnis aller Daten aus dem Bericht für den jeweiligen Empfänger auch erforderlich war.

Kasten zu Nr. 10.4

Der Reha-Entlassungsbericht

- Er dient der Dokumentation und Information über den Behandlungsanlass bei dem Rehabilitanden, den Prozessverlauf der Rehabilitation und das Rehabilitationsergebnis.
- Er umfasst darüber hinaus eine sozialmedizinische Beurteilung des Arztes der Reha-Einrichtung mit einer Aussage über die Leistungsfähigkeit des Rehabilitanden im Erwerbsleben.
- Er ist daher für verschiedene Stellen von Interesse, z. B. für den ambulant behandelnden Arzt, für den Rententräger, die Krankenkasse oder den Medizinischen Dienst der Krankenkassen als Entscheidungsgrundlage z. B. für die Zahlung von Krankengeld.

Ich hielt diese Praxis für bedenklich. Sofern nach den gesetzlichen Vorschriften der Krankenkasse oder dem MDK Informationen aus dem Reha-Entlassungsbericht nicht zustehen, dürfen die Daten auch nicht auf Basis einer Einwilligung offenbart werden. Der Betroffene weiß im Zweifel nicht, dass die Krankenkasse oder der MDK gar keinen Anspruch auf die Daten haben. Auch bei einer restriktiven Übermittlungspraxis bleibt es dem Einzelnen unbenommen, zu einem späteren Zeitpunkt selber die Kasse/den MDK zu informieren. Auf eine routinemäßige Abfrage einer Einwilligungserklärung bei der Entlassung aus der Reha-Einrichtung sollte verzichtet werden.

Bei der Deutschen Rentenversicherung Bund (DRV Bund) habe ich erreicht, dass der Reha-Entlassungsbericht auf Einwilligungsbasis nunmehr nur an den behandelnden Arzt weitergegeben wird. Die Übersendung des Berichts an die Krankenkasse oder den MDK darf nur erfolgen, wenn die Empfänger über eine gesetzliche Erhebungsbefugnis dieser Daten verfügen. Eine Übermittlung des vollständigen Berichts an die Krankenkassen ist nicht zulässig, da der Krankenkasse die Kenntnis des Gesamtberichts nach den Vorschriften im SGB V nicht zusteht. Diese Rechtslage darf nicht durch eine Einwilligung unterlaufen werden. Für die Arbeit der Krankenkasse kann es im Einzelfall jedoch erforderlich sein, bestimmte Daten aus dem Bericht zu erhalten, z. B. dann, wenn der Rehabilitand arbeitsunfähig entlassen wird und das Krankengeld von der Krankenkasse weiter zu zahlen ist. Ebenso kann es erforderlich sein, dass der MDK den Gesamtbericht oder Teile desselben für seine Arbeit benötigt. Diese Fälle sind abschließend im SGB V geregelt. Nur wenn die Erforderlichkeit im Einzelfall gegenüber der DRV Bund dargelegt wird, ist eine Übermittlung zulässig. Eine routinemäßige Übermittlung des Berichts oder Teile desselben darf es jedoch nicht geben. Zudem muss die anfordernde Stelle im Einzelfall die Einwilligung beim Betroffenen einholen.

Wiederholt war klärungsbedürftig, ob die DRV Bund regelmäßig den vollständigen Reha-Entlassungsbericht erhalten darf. Nachdem die DRV Bund nachvollziehbar darlegen konnte, dass sie die Kenntnisnahme des vollständigen Berichts für die Erfüllung ihrer gesetzlichen Aufgaben benötigt, ist dies unter folgenden Bedingungen vertretbar: Es muss zum Einen sichergestellt sein, dass bereits in den Reha-Kliniken nur die erforderlichen Daten erhoben wurden. Darüber hinaus ist sicherzustellen, dass die Zugriffsmöglichkeiten auf den Entlassungsbericht innerhalb der DRV Bund datenschutzgerecht ausgestaltet werden, der Zugriff einzelner Mitarbeiter also nur erfolgt, soweit dies jeweils erforderlich ist.

10.5 Arbeitsverwaltung

10.5.1 Die Jobbörse der Bundesagentur für Arbeit in der Kritik

Verschiedene technische Maßnahmen sollen den Schutz der Teilnehmerinnen und Teilnehmer der Jobbörse gewährleisten (vgl. hierzu Nr. 7.5). In der Praxis zeigten sich aber trotzdem Probleme.

Zwar werden die Bewerberinnen und Bewerber in der Jobbörse nicht namentlich, sondern nur unter einem Pseudonym genannt. Trotzdem können sie in manchen Fällen durch Dritte identifiziert werden. Dies ist insbesondere dann möglich, wenn Beschäftigungsverhältnisse bei früheren Arbeitgebern unter Nennung der genauen Dauer und des Namens des Arbeitgebers veröffentlicht sind. Nachdem ich die BA auf die Problematik hingewiesen hatte, will sie nunmehr sicherstellen, dass die Veröffentlichung eines Bewerberprofils nur nach vorheriger Beratung durch die Vermittlungskraft erfolgt. Zwischen der Vermittlungskraft und dem Bewerber sollen die Details zur Veröffentlichung besprochen und dem Bewerber bei Bedarf ein Ausdruck seines Bewerberprofils ausgehändigt werden. Von einer förmlichen Beanstandung habe ich aufgrund der getroffenen Maßnahmen abgesehen.

In einem anderen Fall beschwerte sich eine Petentin darüber, dass ihre Bewerberdaten in der Jobbörse ohne ihr Wissen und Einverständnis an ebenfalls in der Jobbörse registrierte potenzielle Arbeitgeber weitergegeben worden waren. Die Petentin war Leistungsempfängerin und hatte ihre Bewerberdaten in anonymisierter Form in die Jobbörse eingestellt. Bei jeder Einstellung in der selbst verwalteten Jobbörse muss jedoch gelten, dass Daten nur mit vorherigem Einverständnis der Betroffenen einseitig an Arbeitgeber übermittelt werden dürfen, ohne Unterscheidung zwischen Leistungsempfängern und Nicht-Leistungsempfängern. Sonst könnte praktisch jeder, der sich als Arbeitgeber registrieren lässt, ohne Weiteres an die Daten anonymer Bewerber kommen. In diesem Fall hätte zur Anbahnung eines Beschäftigungsverhältnisses ein förmlicher Vermittlungsvorschlag erstellt werden müssen, sowohl der Arbeitgeber als auch die Bewerberin hätten also schriftlich informiert werden müssen. Dies wäre von der Petentin als Leistungsbezieherin auch hin-

zunehmen gewesen. Der Vermittlungsvorschlag war hier aber unterblieben. Wie die BA einräumt, war die Weitergabe der Bewerberdaten ohne Kenntnis der Petentin datenschutzrechtlich nicht korrekt. Von einer förmlichen Beanstandung habe ich abgesehen, weil die BA meine Rechtsauffassung teilt und die Agentur nachdrücklich auf die Einhaltung der Datenschutzbestimmungen hingewiesen hat.

10.5.2 Erhebung des Migrationshintergrunds von Arbeitsuchenden geplant

Die zur Verbesserung der beruflichen Eingliederung geplante Erhebung des Migrationshintergrunds im Bereich der Arbeitsverwaltung bedarf einer datenschutzkonformen gesetzlichen Regelung.

Im Zusammenhang mit dem Nationalen Integrationsplan der Bundesregierung soll auch die Arbeitsmarktsituation von Personen mit Migrationshintergrund gefördert werden. Eine passgenaue Planung von beruflichen Integrationsmaßnahmen setzt nach Angaben des BMAS eine ausreichende Datenbasis voraus. Allerdings wurden bislang in der Arbeitsverwaltung allein die Staatsbürgerschaft und der Einreisestatus erfasst. Von den in Deutschland lebenden 15 Millionen Menschen mit Migrationshintergrund haben aber acht Millionen die deutsche Staatsbürgerschaft. Auf deren besondere Vermittlungsbedürfnisse könne die BA derzeit nicht ausreichend eingehen. Sie soll daher zukünftig auch den Migrationshintergrund ihrer Kunden erfassen.

In Anlehnung an das Konzept des Mikrozensus von 2005 liegt ein Migrationshintergrund vor, wenn

– die Person nicht auf dem Gebiet der heutigen Bundesrepublik geboren wurde und 1950 oder später zugewandert ist oder

– die Person keine deutsche Staatsangehörigkeit besitzt oder eingebürgert wurde oder die deutsche Staatsbürgerschaft nach § 7 Staatsangehörigkeitsgesetz gesetzlich erworben hat,

– ein Elternteil der Person mindestens eine der unter Nummer 1 oder 2 genannten Bedingungen erfüllt.

Mit Blick auf die Bedeutung der Integration von Menschen mit Migrationshintergrund kann die Nutzung dieser Daten für die Planung von Arbeitsförderungsmaßnahmen durchaus sinnvoll sein. Allerdings ist vor der Einführung einer Registrierungspflicht des Migrationshintergrunds plausibel darzulegen, wie die Datenerhebung zu dem angestrebten Ziel beitragen soll. Aus datenschutzrechtlicher Sicht kommt es darauf an, hier keine „Migrantendatenbank“ zu schaffen, auf die am Ende jeder Vermittler Zugriff hat.

Für vertretbar halte ich es, dass zunächst eine Erhebung und Speicherung nur zu statistischen Zwecken vorgesehen wurde. Demzufolge sollen diese Daten strikt von den operativen, zur persönlichen Beratung und Betreuung geführten Datenbeständen getrennt und nur solange personenbezogen gespeichert werden, wie dies für die statistischen Zwecke erforderlich ist. Die beabsichtigte statistische Verwendung von Daten darf aber grundsätzlich nicht dazu führen, dass die Verwaltung zusätzliche Daten verarbeitet, die für die primäre Aufgabenerfüllung nicht erforderlich sind. Eine entsprechende Ergänzung der Regelung des § 281 SGB III über die Arbeitsmarktstatistiken ist bereits durch das Gesetz zur Einführung Unterstützter Beschäftigung vom 22. Dezember 2008 (BGBl. I 2008 S. 2959) erfolgt.

Darüber hinaus ist in der Diskussion, die Daten über den Migrationshintergrund auch im operativen Geschäft zu Planungs- und Steuerungszwecken zu verwenden. Qualifizierungsmaßnahmen, die auch die migrationsspezifischen Hemmnisse genauer adressieren, sollen nach den Planungen der BA stärker spezialisiert und damit verbessert werden. Das Merkmal „Migrationshintergrund“ soll dabei verdeckt gespeichert werden und somit nicht ohne weiteres zugänglich sein. Im Rahmen der Zuweisung zu konkreten Maßnahmen könnten durch einmalige Verbindung mit dem Merkmal „Migrationshintergrund“ die potentiellen Teilnehmer regional spezifiziert werden. Kritisch wäre allerdings eine generelle längerfristige Speicherung des Migrationshintergrunds unabhängig von einem hierauf beruhenden Förderungsbedarf.

Die Überlegungen im BMAS und in der Arbeitsverwaltung sind noch nicht abgeschlossen. Ich werde die entsprechenden Planungen weiterhin konstruktiv begleiten.

10.5.3 Noch kein neuer Sachstand bei der datenschutzrechtlichen Aufsicht für die Arbeitsgemeinschaften (ARGE)

Die vom Bundesverfassungsgericht für verfassungswidrig erklärte Mischverwaltung muss bis zum 31. Dezember 2010 neu geregelt werden.

Das Bundesverfassungsgericht hat in seinem Urteil vom 20. Dezember 2007 (2 BvR 2433/04) entschieden, dass die ARGE mit der Kompetenzordnung des Grundgesetzes nicht in Einklang stehen und gemäß § 44b SGB II dem Grundsatz eigenverantwortlicher Aufgabenwahrnehmung widersprechen. Dies hat auch Folgen für eine wirksame Datenschutzaufsicht, da es zu Kompetenzkonflikten zwischen BfDI und Landesdatenschutzbeauftragten kommen kann (vgl. hierzu 21. TB Nr. 13.5.4). Bis zu einer gesetzlichen Neuregelung, spätestens am 31. Dezember 2010, dürfen die ARGE wie bisher weitergeführt werden.

Ich habe mit den Landesbeauftragten für den Datenschutz vereinbart, dass für diese Übergangszeit im Interesse einer wirksamen datenschutzrechtlichen

Aufsichtszuständigkeit die bisherige Kontrollpraxis beibehalten wird.

Das BMAS hat inzwischen die Errichtung von sog. ZAG (Zentren für Arbeit und Grundsicherung) aufgrund einer bundesgesetzlichen Rahmenregelung als „Mischbehörde“ sui generis (also gemeinsame Bundes- und Landesbehörde) zur Fortschreibung des bisherigen ARGE-Modells vorgeschlagen. Das Grundgesetz soll so geändert werden, dass durch Bundesgesetz mit Zustimmung des Bundesrates die Leistungsträger BA und Kommunen verpflichtet werden können, ihre Aufgaben einheitlich im ZAG wahrzunehmen. Datenschutzrechtliche Aufsichtsbehörde für die ZAG soll nach diesem Konzept allein der BfDI sein. Fraglich ist allerdings, wie meine Aufsichtszuständigkeit trotz der partiellen Zuständigkeit der Länder/Kommunen rechtlich umgesetzt werden soll.

Die Länder haben sich gegen das vom BMAS erarbeitete Konzept ausgesprochen, insbesondere weil ausreichende Mitgestaltungsrechte der Länder fehlten. Mehrheitlich wird eine Regelung befürwortet, die eine weitgehende Selbständigkeit der ZAG als verfassungsrechtlich abgesicherte Form der Mischverwaltung ermöglicht.

Angesichts dieser konträren Haltungen von Bund und Ländern bleibt abzuwarten, wie und wann der Gesetzgeber den Neuregelungsauftrag des Bundesverfassungsgerichts umsetzt. Dabei wird es auch auf eine eindeutige, sachgerechte Regelung der Aufsichtszuständigkeit im Interesse einer effizienten Datenschutzkontrolle ankommen. Hierzu biete ich gerne meine Mitarbeit an.

10.5.4 Einzelfälle

– *Weitergabe von Gesundheitsdaten an potentielle Arbeitgeber durch die Agentur für Arbeit ohne Wissen und Beteiligung der Kundin.*

  Einer bei der Agentur für Arbeit arbeitslos gemeldeten Petentin war die Arbeitsaufnahme bei einer Zeitarbeitsfirma im Rahmen eines unbefristeten Beschäftigungsverhältnisses gelungen. Die Petentin hatte dabei weder der Zeitarbeitsfirma noch ihrem späteren Arbeitgeber mitgeteilt, dass sie schwer behindert ist. Dies erfuhr der Arbeitgeber jedoch von der Agentur für Arbeit, die der Petentin einen Eingliederungszuschuss für ältere besonders schwer behinderte Menschen bewilligt hatte. Die Agentur für Arbeit hatte dies lediglich dem Arbeitgeber mitgeteilt. Die Petentin hatte weder überhaupt einen Antrag gestellt, noch war sie nachträglich von der Bewilligung informiert worden.

  Hierin liegt ein schwerwiegender Datenschutzverstoß, da es sich bei Gesundheitsdaten um besonders schutzwürdige Daten handelt. Auf die Beschwerde der Petentin hin räumte die Agentur für Arbeit ein, dass zunächst der betroffene Arbeitslose darüber zu informieren ist, bevor dem jeweiligen Arbeitgeber gegenüber die Schwerbehinderung als mögliche Fördervoraussetzung mitgeteilt wird.

  Die Agentur für Arbeit hat gegenüber der Petentin ihr Bedauern zum Ausdruck gebracht und den Vorfall zum Anlass genommen, ihre Mitarbeiterinnen und Mitarbeiter dafür zu sensibilisieren, ohne Einwilligung der Betroffenen gegenüber Dritten keine Hinweise auf die Behinderten- bzw. Schwerbehinderteneigenschaft von Kunden zu geben. Daher habe ich von einer förmlichen Beanstandung nach § 25 BDSG abgesehen.

– *Befunde und Leistungsbild einer von der Agentur für Arbeit veranlassten ärztlichen Untersuchung in Sachbearbeiterhand und elektronischer Akte.*

  Ein Petent beschwerte sich darüber, dass nach einer Untersuchung durch den Ärztlichen Dienst der Agentur für Arbeit neben seinem Leistungsbild auch seine ärztlichen Befunde für seinen Vermittlungssachbearbeiter frei zugänglich waren.

  Gesundheitsdaten sind besonders schutzbedürftig. Daher ist bei der Beurteilung der Erforderlichkeit der Übermittlung von Diagnosedaten ein strenger Maßstab anzulegen. Für die Vermittlung sind nur die Auswirkungen bestimmter Erkrankungen auf die Leistungsfähigkeit bzw. Vermittlungsmöglichkeit eines Kunden relevant. Welche Erkrankung zu der gesundheitlichen Einschränkung geführt hat oder wegen welcher Krankheit ein Kunde in therapeutischer Behandlung ist, ist dagegen in der Regel nicht von Belang.

  Die seit Dezember 2006 in der Agentur für Arbeit verwendeten neuen Formulare für die sozialmedizinischen Gutachten beinhalten dementsprechend eine Unterteilung der gutachterlichen Aussage in einen Teil A mit ausführlicher Darstellung des medizinischen Sachverhaltes mit Verbleib im ärztlichen Dienst und in einen Teil B mit Beschreibung des Leistungsbildes für den Auftraggeber. Im vorliegenden Fall waren jedoch im Vermittlungsbereich zahlreiche nicht zur Aufgabenerfüllung der Agentur für Arbeit erforderliche Daten aus dem Teil A wie z. B. Vorgutachten und Behandlungen durch verschiedene Fachärzte enthalten.

  Von einer förmlichen Beanstandung habe ich im vorliegenden Fall abgesehen, weil die BA meine Rechtsauffassung teilt und die Agentur für Arbeit angewiesen hat, eine Löschung der entsprechenden Gesundheitsdaten des Petenten im Vermittlungsbereich vorzunehmen.

11 Mitarbeiterdatenschutz

11.1 Dringender Handlungsbedarf beim Arbeitnehmerdatenschutz

Eine Reihe von Vorfällen zeigt, dass die Datenschutzkultur in manchen Unternehmen zu wünschen übrig lässt. Insbesondere der Schutz der Arbeitnehmer bedarf größerer Aufmerksamkeit. Deshalb muss das seit langem geforderte Arbeitnehmerdatenschutzgesetz endlich realisiert werden.

Nahezu jeder Arbeitsplatz ist heute mit einem Internet-Zugang ausgestattet, an dem man surfen und auch E-Mail verschicken kann. Wird die Nutzung des Computers protokolliert, sagt das viel über den Arbeitnehmer aus. Mit geringem Aufwand kann heutzutage nahezu der gesamte Büroalltag lückenlos überwacht werden. Texte lassen sich auf Schlagworte hin absuchen, die Zahl der Tastenanschläge und die Fehleingaben geben Auskunft über das Tempo und die Qualität der Arbeit. Mit Netzwerkanalysen können Chefs herausfinden, wer wen im Unternehmen um Rat fragt. Beschäftigtendaten werden nicht mehr nur in Akten, sondern auch in leistungsfähigen Personalinformationssystemen gesammelt, die sich zur Erstellung von Persönlichkeitsprofilen eignen. Immer häufiger kommen offen oder heimlich installierte Videokameras zum Einsatz, die die Überwachung des Arbeits- und Pausenverhaltens ermöglichen.

Das rasante Anwachsen von Datenbeständen, deren fortschreitende Vernetzung und der hohe ökonomische Wert von personenbezogenen Daten multiplizieren das Gefahren- und Missbrauchspotential. Oft werden technische Systeme nicht in erster Linie zur Überwachung der Mitarbeiter eingeführt, sondern zur Kontrolle von Betriebsabläufen, zur Verhinderung von Kundendiebstählen oder zur Sicherung gefährdeter Räume, wie z. B. Kassenbereichen. So nützlich solche Systeme erscheinen, darf es bei ihrem Einsatz keine heimliche Überwachung der Arbeitnehmer geben. Ausnahmen müssen sich auf klar definierte Fälle beschränken, z. B. bei Vorliegen konkreter Verdachtsmomente.

Von besonderer Bedeutung ist eine strikte Zweckbindung bei der Verarbeitung und Nutzung von Arbeitnehmerdaten. Betriebs- und Dienstvereinbarungen, die genau festschreiben, welche Arten der Registrierung und Auswertung von Daten über Beschäftigte erlaubt sind, können zur Rechtsklarheit für alle Beteiligten beitragen. Auch wenn so – bezogen auf das einzelne Unternehmen – ein verbesserter Schutz von Beschäftigtendaten erreicht werden kann, können betriebliche Regelungen klare gesetzliche Vorgaben zum Arbeitnehmerdatenschutz nicht ersetzen.

Es gibt keine speziellen gesetzlichen Regelungen für die Datenerhebung, -verarbeitung und -nutzung in einem Arbeitsverhältnis. Arbeitgeber und Arbeitnehmer müssen mit einer erheblichen Rechtsunsicherheit leben. Das Bundesdatenschutzgesetz mit seinen allgemeinen Regelungen sowie arbeitsrechtliche Vorschriften bieten nur unzureichenden Schutz. Arbeitnehmer und Arbeitgeber müssen sich im Wesentlichen an der zwar umfangreichen, aber lückenhaften und nur schwer erschließbaren Rechtsprechung orientieren.

Kasten zu Nr. 11.1

Forderungen an ein Arbeitnehmerdatenschutzgesetz

- Personenbezogene Daten des Arbeitnehmers dürfen nur erhoben, verarbeitet und genutzt werden, wenn dies zur Begründung, Durchführung, Beendigung oder Abwicklung eines Arbeitsverhältnisses erforderlich oder sonst gesetzlich vorgeschrieben ist.
- Die Datenerhebung erfolgt grundsätzlich beim Arbeitnehmer selbst.
- 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.
- 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 und in welcher Art und Weise sie ausgewertet werden. Dies muss umfassende Auskunfts- und Einsichtsrechte des Arbeitnehmers einschließen.
- Die Rolle des betrieblichen Datenschutzbeauftragten ist zu stärken; seine umfassende Beteiligung vor der Umsetzung betrieblicher Maßnahmen ist sicher zu stellen.
- Dem Betriebsrat ist bei der Bestellung des betrieblichen Datenschutzbeauftragten ein Mitwirkungsrecht einzuräumen.
- Betriebsrat und betrieblicher Datenschutzbeauftragten sind zur engen Zusammenarbeit verpflichtet.

Auch Einwilligungen der Arbeitnehmer können Datenspeicherungen rechtfertigen, wenn sie auf einer freien Entscheidung des Betroffenen beruhen (§ 4a BDSG). Ob die Arbeitnehmer sich im Arbeitsleben aber frei entscheiden können, darf bezweifelt werden. Oftmals erkennen die Betroffenen auch die Tragweite der Einwilligung nicht. Betriebs- und Personalräte können zwar im Rahmen von Mitbestimmungsrechten einen gewissen Einfluss auf die Gewährleistung des Arbeitnehmerdatenschutzes nehmen. Es gibt allerdings nicht überall Arbeitnehmervertretungen und deren Handlungsmöglichkeiten sind begrenzt. Deshalb fordern die Datenschutzbeauftragten des Bundes und der Länder bereits seit Jahren bereichsspezifische Regelungen zum Arbeitnehmerdatenschutz. Der Bundesrat hat am 7. November 2008 (Bundesratsdrucksache 665/08) die Bundesregierung aufgefordert, angesichts der Vorfälle von Arbeitnehmerüberwachung in Unternehmen (Lidl, Telekom) und angesichts der für Arbeitgeber und Arbeitnehmer unübersichtlichen Rechtslage gesetzliche Regelungen zum Arbeitnehmerdatenschutz vorzulegen. Wiederholt hatte auch der Deutsche Bundestag mit großen fraktionsübergreifenden Mehrheiten die Bundesregierung aufgefordert, schnellstmöglich einen Gesetzentwurf zum Arbeitnehmerdatenschutz vorzulegen. Bleibt zu hoffen, dass die Bundesregierung endlich einen entsprechenden Gesetzentwurf vorlegt.

11.2 Angehörige erhalten ein eigenes Antragsrecht bei der Beihilfe

Änderungen im Beihilferecht des Bundes führen endlich zu mehr Datenschutz für Familienangehörige der Berechtigten.

Angehörige eines Bundesbeamten mussten bislang generell ihre Anträge auf Beihilfe im Krankheitsfalle von diesem stellen lassen. Dieses Verfahren führt in bestimmten Konstellationen, z. B. bei getrennt lebenden Familienangehörigen, zu Konflikten.

Bereits in mehreren Tätigkeitsberichten (vgl. zuletzt 18. TB Nr. 18.5.2) hatte ich die damalige Rechtslage kritisiert, nach der allein beihilfeberechtigten Beamten selbst ein Antragsrecht zusteht.

Wie die dort aufgeführten Beispiele deutlich machen, kann dem Recht auf informationelle Selbstbestimmung der Familienangehörigen nur durch ein eigenständiges Antragsrecht angemessen entsprochen werden. Bei den meisten im Beihilfeverfahren erhobenen Daten handelt es sich um Gesundheitsdaten, die nach Artikel 8 der EG-Datenschutzrichtlinie und § 3 Absatz 9 BDSG einen besonderen Schutz genießen. Dieser Schutz muss auch im Verfahren der Beihilfe gewährleistet bleiben. Es leuchtet nicht ein, warum eine Trennung von Beihilfeanspruch, der lediglich dem beihilfeberechtigten Beamten zusteht, und Antragsrecht nicht möglich sein soll. Ein eigenes Antragsrecht volljähriger Familienangehöriger würde die Rechtsposition des Anspruchsberechtigten nicht tangieren. Es ist im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung auch in diesem Bereich geboten.

Bei der Neufassung der Bundesbeihilfeverordnung ist das BMI meiner Auffassung ein Stück entgegengekommen. Um unbillige Härten zu vermeiden, können Beihilfestellen künftig zulassen, dass berücksichtigungsfähige Angehörige oder deren gesetzliche Vertreterinnen oder Vertreter ohne Zustimmung des Anspruchsinhabers die Beihilfe selbst beantragen. Damit ist für diese Fälle ausgeschlossen, dass die besonders geschützten Gesundheitsdaten an den Anspruchsinhaber weitergegeben werden müssen, auch wenn Familienangehörige ein berechtigtes Interesse an der Geheimhaltung haben. Die entsprechenden Regelungen werden mit der Neufassung der Bundesbeihilfeverordnung Anfang 2009 in Kraft treten.

Ich werde die Entwicklung weiter beobachten und die Fälle prüfen, in denen Familienangehörige eigene Antragsberechtigungen verlangt haben. Sollte sich herausstellen, dass die neue Regelung nicht greift, werde ich mich für eine weitergehende Änderung einsetzen.

11.3 Bewerbungsunterlagen sind nach zwei Monaten zurückzugeben oder zu vernichten

Firmen und Behörden dürfen Bewerbungsunterlagen nicht länger als unbedingt nötig behalten. Das Allgemeine Gleichbehandlungsgesetz (AGG) legt hierfür eine Maximalfrist von zwei Monaten fest.

In Bewerbungsunterlagen geben Bewerber umfassend Auskunft über ihre persönliche Situation. Ich habe daher bislang die Auffassung vertreten, dass Bewerbungsunterlagen nach Ablehnung der Bewerbung nicht mehr erforderlich und damit unverzüglich zu löschen bzw. an den Bewerber zurückzugeben sind. Mit dem Inkrafttreten des AGG hat sich die Rechtslage geändert. Das AGG verbietet die Diskriminierung wegen der Rasse, der ethnischen Herkunft, des Geschlechts, der Religion, der Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität. Dieser Schutz vor Diskriminierung erstreckt sich auf das gesamte Arbeitsleben vom Anbahnungsverhältnis bis zur Beendigung und umfasst damit auch das Bewerbungsverfahren. Um sich gegen den Vorwurf, gegen das Benachteiligungsverbot verstoßen zu haben, wehren zu können, sehen es (potenzielle) Arbeitgeber als erforderlich an, die Bewerbungsunterlagen und/oder eine Dokumentation über das Bewerbungsverfahren für einen gewissen Zeitraum aufzubewahren. Dabei stellt sich die Frage, wie lange die Aufbewahrungsfrist höchsten sein darf. Nach dem AGG müssen Ansprüche auf Entschädigung oder Schadenersatz innerhalb einer Zweimonatsfrist geltend gemacht werden (§ 15 Absatz 4 AGG). Der Gesetzgeber hat die kurze zweimonatige Verjährungsfrist von Ansprüchen nach dem AGG mit der Begründung aufgenommen, dass „dem Arbeitgeber nicht zugemutet werden soll, Dokumentationen über Einstellungsverfahren bis zum Ablauf der allgemeinen Verjährungsfrist von drei Jahren aufbewahren zu müssen." Es ist also davon auszugehen, dass eine lange Verjährungsfrist nicht gewollt ist. Deshalb dürfen Bewerbungsunterlagen bei einer ablehnenden Bewerbung in Anlehnung an das AGG für längstens zwei Monate ab Zugang der Ablehnung aufbewahrt werden. Anschließend sind sie dem Bewerber zurückzugeben oder zu vernichten.

11.4 Nicht alle Aufgaben eignen sich für Telearbeit

Die Ausübung beruflicher Tätigkeit am heimischen Arbeitsplatz soll die Vereinbarkeit von Familie und Beruf fördern und persönlichen Notlagen und dienstlichen Notwendigkeiten gleicher Maßen Rechnung tragen. Die Verlagerung dienstlicher Aufgaben in den häuslichen Bereich birgt aber auch Risiken.

Bereits in meinem 18. TB hatte ich dargestellt, dass eine Bearbeitung „besonders schutzwürdiger personenbezogener Daten" (z. B. Gesundheitsdaten, Angaben in Beihilfeanträgen auch für Angehörige, dienstliche Beurteilungen) im Rahmen von Telearbeit besondere Probleme aufwirft, vor allem im Hinblick auf die Kontroll- und Einflussmöglichkeiten der Dienststelle und Missbrauchsmöglichkeiten Dritter. Diese Risiken lassen sich in der Praxis nicht gänzlich vermeiden und sind bezogen auf besonders schützenswerte Daten kaum vertretbar.

Jedoch gibt es auch bei besonders schutzwürdigen personenbezogenen Daten Unterschiede. So können z. B. im Personaldatenbereich Aus- und Fortbildungsdaten oder solche über einzelne Verwendungen durchaus geeignet sein, im Rahmen von Telearbeit verarbeitet zu werden, obgleich es sich auch dabei um Personaldaten und damit um besonders schutzwürdige personenbezogene Daten handelt. Daten über Beurteilungen oder Erkrankungen eignen sich dagegen zur häuslichen Verarbeitung nicht.

Hier wäre das unvermeidbare Restrisiko kaum hinnehmbar. Bei der Bewertung spielt auch eine Rolle, wie hoch das Missbrauchsrisiko bezogen auf die Arbeitsabläufe konkret ist. So ist die voll elektronische Datenverarbeitung ohne Medienbruch anders zu beurteilen als konventionelle Bearbeitung, bei der Akten vom Dienstbüro zum Telearbeitsplatz transportiert, dort bearbeitet und wieder zurück ins Büro geschafft werden. Daher ist in jedem Einzelfall sorgfältig zu prüfen, ob eine Verarbeitung von personenbezogenen Daten in Telearbeit datenschutzrechtlich vertretbar ist.

12 Verkehr

12.1 Verwendung der Mautdaten zur Strafverfolgung?

Auch in diesem Berichtszeitraum hatte ich mich mit der Verwendung von Mautdaten zu beschäftigen.

In meinem letzten Bericht hatte ich über die Absicht der Bundesregierung informiert, durch eine Änderung des Autobahnmautgesetzes (ABMG) die Mautdaten auch zur Verbrechensbekämpfung zu nutzen (21. TB Nr. 12.1). Die Beratungen eines seinerzeit vom BMI vorgelegten Referentenentwurfs sind letztlich ergebnislos verlaufen. Ich gehe davon aus, dass sich bei der Bundesregierung die Einsicht durchgesetzt hat, dass die vorhandenen Mautdaten entweder gar nicht oder nur sehr eingeschränkt für Strafverfolgungszwecke oder zur Gefahrenabwehr geeignet sind und sich deshalb eine Gesetzesänderung erübrigt hat.

Bezüglich der Löschung der Mautdaten hatte ich bei meinem letzten Besuch beim Bundesamt für Güterverkehr (BAG) festgestellt, dass das BAG seine Sicherungskopien unbefristet aufbewahrt. Inzwischen wurde jedoch das von mir geforderte Backup-Löschkonzept umgesetzt. Auch die Sicherungsbänder werden nunmehr einer Löschroutine unterworfen, die beim BAG die Speicherung nur derjenigen Mautdaten gewährleistet, die den Vorgaben des ABMG entsprechen.

12.2 Neues Maritimes Sicherheitszentrum soll Zusammenarbeit verbessern

Die im Zuge der Einrichtung eines Maritimen Sicherheitszentrums in Cuxhaven vorgesehene Weitergabe von Schiffsverkehrsdaten begegnet keinen datenschutzrechtlichen Bedenken.

Seit einigen Jahren hatte ich mit dem BMI und dem BMVBS die Frage erörtert, inwiefern die bei der Wasser- und Schifffahrtsverwaltung (WSV) über den Schiffsverkehr anfallenden Daten generell oder nur im Einzelfall an Sicherheitsbehörden weitergeleitet werden dürfen. Mangels einer ausdrücklichen gesetzlichen Ermächtigungsgrundlage hatte ich erhebliche Bedenken gegen einen generellen Zugang der Bundespolizei zu den bei der WSV vorliegenden personenbezogenen Daten über den Schiffsverkehr.

Anfang 2007 informierte mich das BMVBS über Pläne, in Cuxhaven ein Maritimes Sicherheitszentrum (MSZ) einzurichten. Auslöser des Projekts waren bei großen Havariefällen aufgetretene Koordinationsmängel. Innerhalb dieses MSZ sollen im sog. Gemeinsamen Lagezentrum See (GLZ-See) Behörden des Bundes und der Küstenländer durch umfassenden Informationsaustausch, enge Koordinierung und gegenseitige Unterstützung bei der Wahrnehmung maritimer Sicherheitsaufgaben zusammenarbeiten. Unter Beibehaltung ihrer jeweiligen Zuständigkeiten führt dies zu einer Verzahnung des Maritimen Lagezentrums des Havariekommandos, der Leitstellen der Bundespolizei, des Zolls und der Fischereiaufsicht sowie der Leitstelle der Wasserschutzpolizeien der Küstenländer und der WSV. Zunächst wurde unter meiner Mitwirkung ein Konzept „Einheitliche Datenplattform MSZ“ entwickelt, das regelt, welche Daten insbesondere die WSV einstellen darf und welche Behörden Zugriff auf diese Daten haben.

Ich habe besonderen Wert darauf gelegt, dass die jeweiligen Daten von den verschiedenen Behörden nur für die Zwecke genutzt werden, zu denen sie erhoben wurden; eine Zweckänderung ist nur in gesetzlich vorgegebenen Fällen zulässig. Im Rahmen ihrer gesetzlichen Aufgabenerfüllung sind bestimmte Daten allen Behörden jederzeit verfügbar; darüber hinaus soll eine Datenübermittlung nur zulässig sein im Falle eines polizeilichen, zoll- oder fischereirechtlichen Anfangsverdachts. Auf Basis dieses Konzepts können Schiffsdaten (Name des Schiffs, Reederei, Position und Geschwindigkeit) übermittelt werden. Das BMVBS hat zugesagt, ein Datenschutz- und Informationssicherheitskonzept für das MSZ zu erstellen, in dem die Datenflüsse im GLZ-See in den bestimmten Ereignisfällen dargestellt werden.

Parallel dazu wurde durch die Novellierung des § 9e Seeaufgabengesetz (SeeAufgG) die Rechtsgrundlage für die WSV zur Datenerhebung und -übermittlung geschaffen (BGBl. I 2008 S. 706, 709). Die enumerativ aufgeführten Schiffsverkehrsdaten dürfen an andere öffentliche Stellen übermittelt werden, wenn dies zur Erfüllung von Aufgaben nach dem SeeAufgG (insbesondere zur Abwehr von Gefahren für die Sicherheit des Seeverkehrs sowie die Verhütung von der Seeschifffahrt ausgehender Gefahren und schädlicher Umwelteinwirkungen) erforderlich ist. Darüber hinaus ist die Übermittlung an die Bundespolizei zur Gewährleistung des grenzpolizeilichen Schutzes des Bundesgebietes vorgesehen. Durch diese Regelung ist es gelungen, eine jahrelang streitige Problematik mit einem zufrieden stellendem Ergebnis zu lösen.

12.3 Online-Anbindung der örtlichen Fahrerlaubnisbehörden an das Zentrale Fahrerlaubnisregister des Kraftfahrt-Bundesamtes

Der mit der Einführung der Kartenführerscheine verbundene Aufbau des Zentralen Fahrerlaubnisregisters führte zu gesetzgeberischem Änderungsbedarf.

Seit Jahren (zuletzt 21. TB Nr. 12.5) berichte ich über die datenschutzrechtlichen Probleme bei der Online-Anbindung der örtlichen Fahrerlaubnisbehörden an das Kraftfahrt-Bundesamt (KBA). Das KBA führt das Zentrale

Fahrerlaubnisregister (ZFER), in dem seit dem 1. Januar 1999 die Daten der in Deutschland erteilten allgemeinen Fahrerlaubnisse („Kartenführerscheine“) gespeichert werden. Auch bei den ca. 650 Fahrerlaubnisbehörden (FEB) der Kreise und kreisfreien Städte werden örtliche Fahrerlaubnisregister geführt. Der Datenbestand dieser Register, die sich auf „Kartenführerscheine“ beziehen, muss von den FEB in das ZFER überführt werden; die örtlichen Register sind insofern aufzulösen. Solange nicht alle Führerscheininhaber ihre Fahrerlaubnisse in einen „Kartenführerschein“ umgetauscht haben, bestehen aber die örtlichen Fahrerlaubnisregister mit diesen „alten“ Führerscheindaten fort. Da ein Zwangsumtausch nicht vorgesehen ist, wird dieser Zustand noch lange Zeit andauern. Von den rund 53 Millionen Führerscheininhabern in Deutschland besitzen erst etwa die Hälfte einen „Kartenführerschein“ und sind somit im Bestand des ZFER erfasst.

Nach § 51 StVG haben die FEB dem KBA unverzüglich die zu speichernden oder zu einer Änderung oder Löschung einer Eintragung führenden Daten mitzuteilen. Dabei wird offen gelassen, in welcher Weise diese Mitteilungen zu erfolgen haben. Eine „Mitteilung“ nach § 51 StVG hat zur Folge, dass das KBA diese Informationen selbst zu verarbeiten hat, somit auch für die Richtigkeit der im ZFER eingestellten Daten in vollem Umfang selbst verantwortlich ist. Tatsächlich ist es, wie ich anhand eines Besuches beim KBA festgestellt habe, aber so, dass die FEB im Wege des File Transfers (rd. 88 Prozent der Zugriffe) oder Online-Dialog-Verfahrens (rd. 12 Prozent der Zugriffe) direkt auf den Datenbestand des ZFER zugreifen, wobei das KBA jeden Zugriff protokolliert.

Weder für den direkten Zugriff der FEB auf den Datenbestand des ZFER noch für die vom KBA durchgeführten Protokollierung bestehen entsprechende Rechtsgrundlagen. Mit Blick auf die Bedeutung der im ZFER gespeicherten Daten und die Wichtigkeit der Protokollierung bei der Klärung von Verantwortlichkeiten kann ich nachvollziehen, dass entweder die ZFER-Historie oder die Zugriffsprotokolle langfristig gespeichert werden. Ich habe das BMVBS aufgefordert, endlich ein entsprechendes Gesetzgebungsverfahren einzuleiten. Da die Verantwortung gemeinsam bei Bund und Ländern liegt, sollten die jeweiligen Verantwortlichkeiten gemeinsam definiert und auf normenklare Rechtsgrundlagen gestellt werden.

13 Europa und Internationales

13.1 Europäische Rechtsentwicklung

Die Verzögerung des europäischen Verfassungsprozesses behindert die grundrechtliche Absicherung des Datenschutzes im Europarecht. Ein weiterer Schritt wurde dagegen auf dem Weg zu einem globalen Datenschutz gesetzt.

Nach dem vorläufigen Scheitern des europäischen Verfassungsvertrages einschließlich eines Grundrechtekatalogs (vgl. 21. TB Nr. 3.1) im Jahre 2005 wurde das Vorhaben während der deutschen Ratspräsidentschaft 2007 in reduzierter Gestalt als „Reformvertrag von Lissabon“ verabschiedet. Bundestag und Bundesrat haben auch den Lissabon-Vertrag mit jeweils großer Mehrheit gebilligt, jedoch steht die Unterzeichnung durch den Bundespräsidenten mit Blick auf die anhängigen Klagen beim Bundesverfassungsgericht noch aus.

Sollten auch die Tschechische Republik und Irland zu einem positiven Votum gelangen, könnte auch die Charta der Grundrechte Rechtsverbindlichkeit erlangen, die in den Artikeln I-51 und II-68 ausdrücklich das Grundrecht auf den Schutz personenbezogener Daten garantiert (vgl. im einzelnen 21. TB Nr. 3.1). Die Grundrechtecharta würde über den Umweg eines rechtsverbindlichen Verweises in Artikel 6 Absatz 1 des Unionsvertrages in den Rang vollgültigen Primärrechts erhoben.

Zudem sieht der Lissabon-Vertrag in Artikel 6 Absatz 2 den Beitritt der Union zur Europäischen Menschenrechtskonvention vor, wodurch die bisherige Geltung der Gemeinschaftsgrundrechte als allgemeine Rechtsgrundsätze bestätigt würde.

Die Europaratskonvention 108 und ihre Zusatzprotokolle, insbesondere dasjenige betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr von 2001, bilden auch die Grundlage für eine Initiative der 30. Internationalen Datenschutzkonferenz (s. u. Nr. 13.9) mit dem Ziel eines globalen Datenschutzes und der Festschreibung des Datenschutzes als universelles Menschenrecht. In ihrer von mir unterstützten Entschließung über die Dringlichkeit des Schutzes der Privatsphäre in einer Welt ohne Grenzen fordert die Internationale Konferenz auch die Nicht-Mitgliedstaaten des Europarates auf, der Konvention 108 und dem oben genanten Zusatzprotokoll beizutreten. Die Konferenz sieht im Europaratsübereinkommen zu Recht die geeignete Plattform für das weitere Vorgehen mit dem Ziel eines angemessenen Datenschutzes auf allen Kontinenten. Eine weltweite Einigung auf ihre Grundprinzipien als „Kleinster gemeinsamer Nenner“ würde einen nicht zu unterschätzenden Fortschritt und einen stabilen Ausgangspunkt für künftige Strategien bedeuten.

13.2 Die Datenschutzgruppe nach Artikel 29 der EG-Datenschutzrichtlinie

Die Datenschutzgruppe hat weitere wegweisende Papiere zum Datenschutz verabschiedet.

Die Artikel-29-Gruppe hat im Berichtszeitraum 28 Papiere verabschiedet, die sich erneut mit einer breiten Palette von Themen auseinander setzen (abrufbar auf der Internet-Seite der Europäischen Kommission unter www.ec.europa.eu; vgl. Kasten zu Nr. 13.2). So wurde eine Stellungnahme zum Datenschutz bei Kindern (WP 147) verabschiedet (s. auch o. Nr. 2.9). Ein wegweisendes Arbeitspapier (WP 136) setzt sich mit dem Begriff der personenbezogenen Daten auseinander (s. Nr. 13.2.4).

Breiten Raum in den Diskussionen der Gruppe nahm die Erfassung und Übermittlung von Passagierdaten ein. Im Jahre 2007 wurde das dritte Abkommen zwischen der EU und den USA geschlossen (s. u. Nr. 13.5.2). Im Sommer 2008 wurde zudem ein PNR-Abkommen mit

Australien vereinbart (s. u. Nr. 13.5.1). Eine Überprüfung der Umsetzung des PNR-Abkommens mit Kanada erfolgte im November 2008. Kritisch äußerte sich die Gruppe in dem Arbeitspapier WP 145 zu dem im November 2007 vorgelegten Vorschlag der Europäischen Kommission zu einem europäischen PNR-System (s. u. Nr. 13.5.3).

Fortgesetzt wurden die Arbeiten im Bereich verbindlicher Unternehmensregelungen zur Übermittlung personenbezogener Daten in Länder ohne angemessenes Datenschutzniveau (BCR-Binding Corporate Rules) (s. u. Nr. 13.2.3).

Im Februar 2008 ging meine zweite Amtszeit als Vorsitzender der Artikel-29-Gruppe zu Ende. Eine Wiederwahl nach einer zweiten Amtszeit ist nicht möglich. Zu meinem Nachfolger wurde mein bisheriger Stellvertreter, der Präsident der französischen Datenschutzbehörde, Alexander Türk, gewählt. Neuer Stellvertreter ist der Vorsitzende der niederländischen Datenschutzbehörde, Jacob Kohnstamm.

Kasten zu Nr. 13.2

Die Datenschutzgruppe nach Artikel 29 der EG-Datenschutzrichtlinie

Nach Artikel 29 der EG-Datenschutzrichtlinie 95/46/EG berät die Gruppe, die sich aus den nationalen Datenschutzbeauftragten zusammensetzt, die Europäische Kommission und prüft unter anderem die Umsetzung der Richtlinie in nationales Recht im Sinne einer einheitlichen Rechtsanwendung. Sie nimmt Stellung zum Schutzniveau sowohl in der Gemeinschaft als auch in Drittländern, erstellt Arbeitspapiere, um auf besondere datenschutzrechtliche Probleme aufmerksam zu machen und entwickelt Empfehlungen zum Schutze der Privatsphäre der Bürgerinnen und Bürger der Gemeinschaft.

13.2.1 Gemeinsame Aktivitäten: Europaweite Datenschutzprüfung im Krankenversicherungssektor

Nach Abschluss der Überprüfung im Krankenversicherungssektor wenden sich die europäischen Datenschutzbehörden dem Telekommunikationssektor zu.

Die 2008 abgeschlossene Überprüfung des Krankenversicherungssektors durch die Datenschutzbehörden der EU-Mitgliedstaaten ergab keine Hinweise auf grundlegende Datenschutzmängel. Die Artikel-29-Gruppe sprach allerdings einige grundsätzliche Empfehlungen zur weiteren Stärkung des Datenschutzes aus. So sollten die Unternehmen ihre Kunden besser über die Verarbeitung der Daten informieren. Daten sind zu anonymisieren, soweit sie für wissenschaftliche oder statistische Zwecke verwendet werden.

Wegen der zunehmenden Bedeutung international agierender Unternehmen sind weitere gemeinsame Überprüfungen der europäischen Datenschutzbehörden geplant. Als nächstes werden sie sich den Internet-Providern und Telekommunikationsunternehmen zuwenden. Auf der Basis eines an die Unternehmen übersandten Fragekatalogs sollen ab Frühjahr 2009 Gespräche mit den Firmen sowie gezielte Überprüfungen stattfinden.

13.2.2 Safe Harbor

Die auf dem Safe-Harbor-Seminar im Oktober 2008 vorgestellte EU-Studie beleuchtet Vor- und Nachteile dieses Abkommens.

Auf dem Safe-Harbor-Seminar im Oktober 2008 wurde die zweite im Auftrag der Europäischen Kommission erstellte Studie zur Umsetzung des Safe-Harbor-Abkommens vorgestellt. Die Tatsache, dass inzwischen mehr als 1 600 US-Unternehmen bei der Federal Trade Commission (FTC) für das Safe-Harbor-Programm angemeldet sind, zeugt von der wachsenden Bedeutung dieses Rechtsinstruments für die Übermittlung personenbezogener Daten in die USA. Es stimmt aber bedenklich, dass das Datenschutzniveau der beteiligten Firmen nicht höher ist als zur Zeit der ersten Studie von 2004. So entspreche die von den Firmen überwiegend selbst vorgenommene Zertifizierung in vielen Fällen nicht den Erfordernissen des Abkommens. Zudem lasse häufig das allgemeine Datenschutzniveau in den Firmen zu wünschen übrig, insbesondere was die Unterrichtung der Kunden angeht. Die Selbstregulierung müsse daher dringend durch verstärkte externe Prüfung und Kontrolle seitens der FTC ergänzt werden. Weiterhin müssen Verbraucher und Unternehmen besser über die Beschwerdemechanismen informiert werden.

Angesichts der Globalisierung der Datenströme soll der transatlantische Datenschutzdialog auf andere, den Schutz der Privatsphäre betreffende Themen, ausgedehnt werden, zum Beispiel den Konsumentenschutz und die Einhaltung datenschutzrechtlicher Standards bei sozialen Netzwerken.

13.2.3 Binding Corporate Rules

Die Artikel-29-Gruppe verstärkte ihre Anstrengungen im Bereich der verbindlichen unternehmensinternen Datenschutzregelungen (Binding Corporate Rules, BCR), die ein wichtiges Instrument für die Datenübermittlung in Drittstaaten darstellen.

Verbindliche Unternehmensregelungen stellen ein wichtiges Instrument zur ausnahmsweisen Genehmigung der Übermittlung personenbezogener Daten in Drittstaaten ohne angemessenes Datenschutzniveau dar (Artikel 26 der europäischen Datenschutzrichtlinie 95/46/EG). Nachdem sich das zwischen den europäischen Datenschutzbehörden zur Genehmigung von BCR vereinbarte Verfahren in der Praxis als kompliziert und zeitaufwendig erwiesen hatte, verstärkte die Artikel-29-Gruppe ihre Anstrengungen zur Vereinheitlichung und Vereinfachung des Verfahrens. Als Hilfestellung für Unternehmen bei der Antragsstellung auf Genehmigung von BCR wurde eine Übersicht über die Anforderung an den BCR erarbeitet (WP 153 vom 24. Juni 2008). Zur Erleichterung des Ver-

ständnisses hat die Artikel-29-Gruppe ergänzend einen Rahmen ausgearbeitet, der zeigt, wie eine verbindliche unternehmensinterne Datenschutzregelung aussehen könnte (WP 154 vom 24. Juni 2008). Eine Zusammenstellung häufig gestellter Fragen soll den Antragstellern ein klares Bild von den Anforderungen für die Genehmigungsvoraussetzungen ihrer BCR vermitteln (WP 155 Rev. 01 vom 1. Oktober 2008).

Darüber hinausgehend hat ein Kreis von inzwischen 15 europäischen Datenschutzaufsichtsbehörden einschließlich Deutschlands eine politische Absichtserklärung zur gegenseitigen Anerkennung von BCR abgegeben. Ziel ist es, das Verfahren zur EU-weiten Anerkennung verbindlicher Unternehmensregelungen zu beschleunigen, indem eine positive Entscheidung der federführenden Behörde hinsichtlich der Genehmigungsfähigkeit eingereichter BCR von den anderen Behörden als ausreichende Grundlage angesehen wird, ihrerseits eine zustimmende Entscheidung zu erlassen.

Im Mai 2007 hat die Deutsche Post AG mich gebeten, das Verfahren zur Anerkennung verbindlicher unternehmensinterner Datenschutzregelungen nach den Vorgaben der Artikel-29-Gruppe durchzuführen. Grundlage für die „Privacy Policy der Deutschen Post World Net“ sind im Wesentlichen die Richtlinie 95/46/EG und die Standardvertragsklauseln II (vgl. 20. TB Nr. 14.1.2). Gleichzeitig will die Deutsche Post AG mit der Einführung verbindlicher unternehmensinterner Datenschutzregelungen ein funktionierendes Netzwerk von Datenschutzbeauftragten in den einzelnen Konzernunternehmen einrichten.

Ich unterstütze diese Bemühungen.

13.2.4 Stellungnahme zu personenbezogenen Daten

Die Artikel-29-Gruppe beschäftigte sich mit der Frage, wann Daten als personenbezogen anzusehen sind. Dies ist deshalb von zentraler Bedeutung, weil das Datenschutzrecht nur für personenbezogene Daten gilt.

In der Stellungnahme 4/2007 (WP 136 vom 20. Juni 2007) äußert sich die Artikel-29-Gruppe umfassend zum Begriff der personenbezogenen Daten. Eine Erläuterung dieses Begriffs war notwendig geworden, da es immer wieder Auslegungsschwierigkeiten insbesondere bei der Wirtschaft hinsichtlich dieses zentralen Begriffs der europäischen Datenschutzrichtlinie 95/46/EG gegeben hatte. Die Stellungnahme soll deshalb eine einheitliche Auslegung der Richtlinie bewirken und damit zur Rechtssicherheit beitragen (s. Kasten zu Nr. 13.2.4).

Die Abgrenzungsschwierigkeiten personenbezogener von anonymen Daten werden angesichts der rasanten technologischen Entwicklung immer bedeutsamer. Während in der frühen Phase der elektronischen Datenverarbeitung überwiegend gezielt Daten erhoben und verarbeitet wurden und sich der Personenbezug aus dem Verwendungskontext ergab, entstehen heute vielfältige Daten beiläufig, etwa bei der Erbringung digitaler Telekommunikationsdienste oder bei der Abwicklung elektronischer Zahlungen. Auch bei der Inanspruchnahme des Internets hinterlassen die Nutzer umfangreiche Datenspuren sowohl bei den Netzbetreibern als auch bei den Diensteanbietern. Selbst wenn diese Daten nicht erhoben werden, um die Nutzer persönlich zu identifizieren, entstehen auf diese Weise umfangreiche Datensammlungen, die letztlich auf die Betroffenen zurückgeführt werden können und vielfältige Rückschlüsse auf ihre Interessen, Kommunikationsbeziehungen und soziodemographischen Eigenschaften ermöglichen.

Kasten zu Nr. 13.2.4

Der Begriff der „personenbezogenen Daten“ in der Richtlinie 95/46/EG

Die Richtlinie 95/46/EG definiert in Artikel 2 lit. a den Begriff der „personenbezogenen Daten“ weit und versteht hierunter „*alle Informationen über eine bestimmte oder bestimmbare natürliche Person*“. Die Artikel-29-Gruppe konzentriert sich in ihrer Analyse auf die vier Hauptbausteine der Definition und untermauert diese durch Beispiele aus der Anwendungspraxis europäischer Datenschutzbehörden. Im Folgenden sollen die zentralen Auslegungskriterien dieser Definition erläutert werden:

„*alle Informationen*“: Einbezogen sind Informationen unabhängig von ihrer Art, Inhalt und Form. Es gibt insbesondere keine belanglosen oder freien Daten, welche grundsätzlich nicht unter das Datenschutzrecht fallen.

„*über*“: Die Informationen müssen sich in irgendeiner Form auf die Person beziehen lassen. Der Bezug kann über den Inhalt (Informationen werden über eine bestimmte Person gegeben), über den Verwendungszweck (Daten werden verwendet, um eine Person zu beurteilen, in einer bestimmten Weise zu behandeln oder ihre Stellung oder ihr Verhalten zu beeinflussen) oder über das Ergebnis der Verarbeitung (die Verwendung der Daten hat Auswirkungen auf die Person) hergestellt werden.

„*bestimmte oder bestimmbare*“: Neben einem direkten Personenbezug ist es auch möglich, dass sich Daten indirekt auf Personen beziehen lassen. Selbst wenn der verantwortlichen Stelle die Identität einer Person nicht bekannt ist, kann es sich also um personenbezogene Daten handeln, insbesondere wenn Dritte die Informationen auf eine Person beziehen können. Zweifelsfälle entstehen insbesondere bei der Verwendung pseudonymisierter Daten. Entscheidend ist, dass die Daten bei realistischer Betrachtung unter Einbeziehung des Aufwandes und des Interesses der Person zugeordnet werden können.

„*natürliche Personen*“: Im Sinne der europäischen Datenschutzrichtlinie ist ein Personenbezug nur bei natürlichen Personen (Menschen) möglich; juristische Personen (Körperschaften, z. B. Vereine, Aktiengesellschaften, öffentliche Stellen) werden nicht einbezogen. Ebenso wenig umfasst sind Daten über verstorbene Personen oder ungeborene Kinder.

Vor diesem Hintergrund wurde insbesondere im Zusammenhang mit der Neufassung der Datenschutzrichtlinie für elektronische Kommunikationsdienste (E-Privacy Directive, vgl. Nr. 7.12) intensiv darüber diskutiert, inwieweit IP-Adressen personenbezogen sind.

Sofern die Möglichkeit besteht, derartige Daten direkt oder indirekt einzelnen natürlichen Personen zuzuordnen, unterliegen sie dem Schutz des Datenschutzrechts. Insofern kommt die Artikel-29-Gruppe zum Ergebnis, dass IP-Adressen im Regelfall als personenbezogene Daten anzusehen sind, da sie sich in den meisten Fällen (gegebenenfalls in Zusammenwirkung mit dem Anbieter von Internet-Zugängen) auf den Anschlussinhaber oder den Computer-Nutzer zurückführen lassen. Auch Daten, die – obwohl statistischen Ursprungs – einzelnen Personen zugeordnet werden, etwa um die Bonität eines Bankkunden zu beurteilen (Scoring, vgl. Nr. 3.4.4), sind personenbezogene Daten im Sinne des Datenschutzrechts.

13.3 Europaweite Zusammenarbeit von Polizei- und Sicherheitsbehörden und von Datenschutzkontrollbehörden

Die Zusammenarbeit der Sicherheitsbehörden in der Europäischen Union gemäß dem Haager Programm wird fortgesetzt und intensiviert. Leider wird der europaweite Datenschutz in diesem Bereich nicht gleichermaßen ausgebaut.

Das sog. Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht vom 5. November 2004 (21. TB Nr. 3.2.1), das u. a. den Austausch strafverfolgungsrelevanter Informationen unter den Grundsatz der Verfügbarkeit stellt, ist im Rat der EU weiter vorangetrieben worden. Mehrere einschlägige Rechtsakte wurden endgültig beschlossen bzw. eine politische Einigung hierüber erzielt, ohne dass zuvor eine angemessene Evaluierung bereits bestehender Maßnahmen durchgeführt worden war (s. Kasten zu Nr. 13.3).

Die Umsetzung dieser Rechtsakte wird zu einem erheblich intensiveren Informationsaustausch zwischen den Strafverfolgungs- und sonstigen Sicherheitsbehörden in der EU einschließlich EUROPOL und EUROJUST führen. Dementsprechend wird auch die Gefährdung des Persönlichkeitsbereichs zunehmen, insbesondere von unbescholtenen Personen, die weder Tatbeteiligte, Beschuldigte noch sonstige Verdächtige sind.

Der Austausch von Informationen für Zwecke der Strafverfolgung zwischen den EU-Mitgliedstaaten setzt einen hohen und gleichwertigen Datenschutzstandard in den Mitgliedstaaten voraus, der die Integrität, Vertraulichkeit und Zweckbindung der ausgetauschten Daten sowie eine wirkungsvolle Datenschutzkontrolle gewährleistet. Der am 28. November 2008 vom Rat verabschiedete Rahmenbeschluss zum Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit verarbeitet werden (vgl. Nr. 13.3.1), wird diesen Zielen noch nicht gerecht. Hier bedarf es deutlicher Nachbesserungen. Der Rechtsakt ist das Pendant zur Datenschutzrichtlinie 95/46/EG, die für die Datenverarbeitung im Bereich der Ersten Säule gilt.

Die verstärkte polizeiliche Zusammenarbeit in Europa macht darüber hinaus eine enge datenschutzrechtliche Kooperation der europäischen Datenschutzkontrollinstanzen, in Ergänzung der Artikel-29-Gruppe (s. o. Nr. 13.2) erforderlich. Voraussetzung für die Einsetzung eines entsprechenden Gremiums ist allerdings eine politische Entscheidung des Rates.

Kasten zu Nr. 13.3

Rechtsakte

- Vertrag von Prüm vom 27. Mai 2005 über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration (BGBl. I 2006, 1458), s. u. Nr. 13.3.2,
- „Schwedische Initiative“ (Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der EU), s. u. Nr. 13.3.6,
- Verordnung (EG) 1987 (2006) des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), s. u. Nr. 13.3.4,
- Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), s. u. Nr. 13.3.4,
- Beschluss 2008/615/JI des Rates vom 20. Juni 2008 über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration, s. u. Nr. 13.3.2,
- Beschluss 2008/633/JI des Rates vom 23. Juni 2008 über den Zugang der benannten Behörden der Mitgliedstaaten und von EUROPOL zum VISA-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten, s. u. Nr. 13.3.5.
- Beschluss des Rates zur Errichtung des Europäischen Polizeiamtes (EUROPOL), s. u. Nr. 13.3.3.

Das Haager Programm von 2004 umfasst einen Zeitraum von fünf Jahren, also bis 2009. So hat im Juni 2008 eine hochrangige Gruppe, die sog. Future Group, die noch unter deutscher EU-Präsidentschaft im Jahr 2007 eingerichtet worden war, einen Bericht unter dem Titel „Freiheit, Sicherheit, Privatheit“ vorgelegt, der als Ausgangsbasis für ein Nachfolgeprogramm zum Haager Programm die-

nen könnte. Dort werden alle Aspekte der künftigen europäischen Innenpolitik abgehandelt, für die in Zukunft das Konvergenzprinzip als Leitmaxime gelten soll; dem Datenschutz (privacy) sind allerdings nur zwei von 122 Kapiteln vorbehalten, welche zudem die datenschutzrechtlichen Anforderungen nur unzureichend beschreiben. Der Bericht soll als das sog. Stockholmer Programm unter schwedischem Vorsitz verabschiedet werden. Es bedarf also noch datenschutzrechtlicher Überzeugungsarbeit, um einen verstärkten Schutz der Bürgerrechte auch unter dem Nachfolgeprogramm zu gewährleisten.

13.3.1 Rahmenbeschluss über den Schutz personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Der nach langen Beratungen verabschiedete Rahmenbeschluss ist nur ein erster Schritt auf dem Weg zu einem hohen Datenschutzstandard für die Verarbeitung personenbezogener Daten durch Polizei- und Strafverfolgungsbehörden der EU-Mitgliedstaaten.

Der Rat der Innen- und Justizminister der EU-Mitgliedstaaten hat am 27. November 2008 den Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, verabschiedet. Damit sind nach über drei Jahren Beratungen (21. TB Nr. 3.2.1) erstmals gemeinsame Regelungen zum Datenschutz für die polizeiliche und justizielle Zusammenarbeit in der sog. Dritten Säule der EU beschlossen worden. Das ursprüngliche Ziel, einen hohen und gleichwertigen Datenschutzstandard bei der Verarbeitung personenbezogener Daten durch Polizei- und Strafverfolgungsbehörden zu schaffen, wird aber nicht erreicht.

So erstreckt sich der Anwendungsbereich des Rahmenbeschlusses nur auf die Übermittlung personenbezogener Daten zwischen den Mitgliedstaaten untereinander und zwischen den Mitgliedstaaten und EU-Behörden bzw. EU-Informationssystemen sowie auf die weitere Verarbeitung der erhaltenen Daten in den Mitgliedstaaten. Die Datenverarbeitung von Polizei- und Strafverfolgungsbehörden auf nationaler Ebene bleibt jedoch unberührt, obwohl die übermittelten Daten im Empfängerland mit den dort erhobenen Daten zusammengeführt werden. Es ist deshalb völlig unpraktikabel, für die verschiedenen Datenarten unterschiedliche Datenschutzstandards vorzusehen.

Der Rahmenbeschluss gilt zudem nicht für die Verarbeitung von Daten in Akten, in denen jedoch weiterhin ein großer Anteil der polizeilichen Datenverarbeitung stattfindet.

Des weiteren sieht der Rahmenbeschluss zwar vor, dass es in den EU-Mitgliedstaaten Auskunfts-, Löschungs- und Berichtigungsansprüche für die von der Datenverarbeitung Betroffenen geben muss, überlässt aber die konkrete Ausgestaltung dieser Rechte dem jeweiligen nationalen Gesetzgeber. Ein einheitlicher Datenschutzstandard kann damit nicht erreicht werden.

Ferner fehlen Regelungen für ein unabhängiges Gremium der Datenschutzbeauftragten aus den Mitgliedstaaten, das die Kommission, den Rat und das Europäische Parlament in datenschutzrechtlichen Fragen berät. EU-Rechtsakte zur polizeilichen und justiziellen Zusammenarbeit in Strafsachen können damit auch künftig ohne Beteiligung von Datenschutzgremien auf EU-Ebene verabschiedet werden. Mir ist völlig unverständlich, warum ein entsprechender Vorschlag der Kommission und des Europäischen Parlaments vom Rat nicht übernommen wurde.

13.3.2 Vertrag von Prüm und dessen Überführung in europäisches Recht

Der Vertrag von Prüm über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration, unterzeichnet am 27. Mai 2005 von sieben Mitgliedstaaten, wird seit Dezember 2006 sukzessive umgesetzt (vgl. Kasten zu Nr. 13.3.2).

Kaum war der Vertrag von Prüm durch die ersten Vertragsstaaten ratifiziert und die dazugehörige Durchführungsvereinbarung im Dezember 2006 getroffen worden (vgl. 21. TB Nr. 3.2.2), beschlossen die Justiz- und Innenminister der EU-Mitgliedstaaten im Februar 2007 unter deutscher EU-Präsidentschaft die Regelungen des Prümer Vertrages in das EU-Recht zu überführen. Wesentliche Teile des Prümer Vertrages sollen für alle EU-Mitgliedstaaten gelten. Dies betrifft insbesondere den Austausch von DNA- und daktyloskopischen Daten, Kfz-Daten sowie die Übermittlung von Daten zur Verhütung des Terrorismus. Bereits am 12. Juni 2007 folgte im Rat eine politische Einigung über den Vorschlag für einen entsprechenden Ratsbeschluss, der mit Beschluss des EU-Rates vom 23. Juni 2008 rechtsverbindlich wurde.

Ich hatte Bedenken gegen die Überführung des Prümer Vertrags in den Rechtsrahmen der EU geäußert, weil es im Bereich der Dritten Säule der EU immer noch kein angemessenes Datenschutz-Regime gab. Aber auch der zwischenzeitlich verabschiedete Rahmenbeschluss zum Datenschutz in der Dritten Säule weist gravierende datenschutzrechtliche Defizite auf und gewährleistet daher keinen entsprechenden Schutz (vgl. Nr. 13.3.1). Die rasche Umsetzung der Prüm-Initiative halte ich auch für problematisch, weil in mehreren EU-Mitgliedstaaten überhaupt erst die rechtlichen und technischen Voraussetzungen, z. B. für den Aufbau einer DNA-Datenbank, geschaffen werden müssen. Es macht einen Unterschied, ob der Austausch von DNA- und daktyloskopischen Daten zwischen den sieben ursprünglichen Vertragsparteien mit ähnlicher Rechtstradition und vergleichbarer Praxis oder aber zwischen 27 Mitgliedstaaten abläuft, von denen viele nur über rudimentäre Vorkehrungen sowohl rechtlicher wie auch datenverarbeitungstechnischer Art verfügen. Dies gilt im Grunde auch für die erforderliche Datenschutzinfrastruktur auf Grund des Ratsbeschlusses. Ich habe deshalb vor einer überstürzten Umsetzung des Ratsbeschlusses gewarnt.

Kasten zu Nr. 13.3.2

Der Vertrag von Prüm

Am 27. Mai 2005 haben sieben EU-Mitgliedstaaten (Belgien, Deutschland, Frankreich, Luxemburg, Niederlande, Österreich und Spanien) im rheinland-pfälzischen Prüm einen völkerrechtlicher Vertrag über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration, geschlossen. Nach dem Ort der Unterzeichnung wird dieser Vertrag als „Prümer Vertrag“ bezeichnet.

Kernelement des Vertrages ist die gegenseitige Vernetzung nationaler Datenbanken. So gewähren sich die Polizei- und Strafverfolgungsbehörden dieser Staaten wechselseitig Zugriff auf bestimmte nationale polizeiliche Dateien. Hierzu zählen DNA-Analyse-Dateien, Datenbanken mit elektronisch gespeicherten Fingerabdrücken sowie elektronische Register mit Kraftfahrzeug- und Kraftfahrzeughalterdaten. Die abfragende Stelle erhält innerhalb weniger Minuten unmittelbar und automatisch Kenntnis, ob zu den von ihr abgefragten Daten Informationen in den Dateien der anderen Vertragsstaaten enthalten sind. Insoweit wird jedoch nur angezeigt, dass dort Informationen gespeichert sind („Treffer/Hit“) oder nicht („kein Treffer/no hit“). Es besteht kein unmittelbarer Zugriff auf diese Informationen.

Der Vertrag von Prüm ist kein EU-Abkommen, d. h. keine gemäß den EU-Verträgen (sog. Gemeinschaftsrecht) geschlossene Vereinbarung, die alle EU-Mitgliedstaaten bindet. Da dieser Vertrag aber Bestimmungen enthält, die das Gemeinschaftsrecht inhaltlich betreffen (die sog. Erste und Dritte Säule der EU) war er von Beginn an darauf ausgerichtet, in den Rechtsrahmen der EU überführt, d. h. Bestandteil des Gemeinschaftsrechts zu werden. Unter der deutschen EU-Ratspräsidentschaft ist diese Überführung im Februar 2007 erfolgt.

Die Prüm-Vertragsparteien haben nach Inkraftsetzung des Vertrages im Dezember 2006 sukzessive mit der Aufnahme des Echtbetriebs begonnen, zunächst zwischen Deutschland und Österreich hinsichtlich des Austauschs von DNA- und in 2007 auch von daktyloskopischen Daten. Bis Juli 2007 fand die Umsetzung im DNA-Bereich bereits mit fünf weiteren Staaten statt, während im daktyloskopischen Bereich, bis auf Österreich, ein Austausch nur im Testbetrieb realisiert wurde.

Im September 2008 habe ich mich im BKA über die Umsetzung des Prümer Vertrages informiert. Themen waren der Austausch von DNA- und von daktyloskopischen Daten sowie die Praxis der Protokollierung gemäß Artikel 39 des Vertrages. Dabei habe ich festgestellt, dass Deutschland den DNA-Datenaustausch mit jedem neu hinzukommenden Vertragsstaat zunächst mit einem Initialmassenabgleich der DNA-Profile beginnt, d. h. der inländische Datenbestand mit DNA-Indexdaten wird den anderen Vertragsparteien zum Zwecke des Abgleichs mit dem dortigen Datenbestand zur Verfügung gestellt und umgekehrt. Ich halte diese Praxis mit den Vorgaben des Vertrages für nicht vereinbar, denn ein solcher Massenabgleich ist nur mit DNA-Spurenmaterial vorgesehen (Artikel 4), nicht jedoch mit individuell zurechenbaren Identifizierungsmerkmalen. Im Übrigen halte ich einen solchen Massenabgleich auch für unverhältnismäßig, denn er widerspricht der vertraglich vereinbarten hit/no hit Abfrage im Einzelfall.

Problematisch ist auch das Verfahren zur Feststellung eines Treffers im Falle der Abfrage mit einem DNA-Fundstellendatensatz. Aus datenschutzrechtlicher Sicht muss es sich dabei immer um einen Exakttreffer handeln, der vorliegt, wenn auf beiden Seiten mindestens sechs Genoide (sog. loci) mit den zugrunde liegenden Allel-Werten des DNA-Satzes übereinstimmen. Auch wenn einige Werte durch sog. „Joker“ ersetzt werden, darf dies nicht zu einer Verminderung der Genauigkeit von Treffern führen, denn ansonsten besteht die Gefahr, dass der abgefragte Datensatz einer anderen Person zugeordnet wird. Dies hat auch die Working Party Police and Justice (vgl. Nr. 13.3.8) in ihrer Stellungnahme zu dem Durchführungsbeschluss auf Ratsebene betont und gefordert, im technischen Anhang zu diesem Beschluss ausdrücklich zu regeln, dass jegliche Übereinstimmung eines bestimmten Merkmals, die durch die Verwendung einer „wildcard“ ausgelöst wird, bei der Bestimmung der zumindest sechs loci nicht berücksichtigt werden darf.

Auch beim Abgleich von daktyloskopischen Daten, bei dem allerdings ein endgültiger Treffer durch einen Daktyloskopen bestätigt wird, ist größte Sorgfalt angebracht. Deshalb habe ich aus datenschutzrechtlicher Sicht vorgeschlagen, dass im Annex zu dem Durchführungsbeschluss ein gemeinsamer daktyloskopischer Datentrefferalgorithmus für alle Mitgliedsstaaten, zumindest aber ein Mindestmaß an technischen Trefferregeln festgelegt werden sollte.

Die Gesichtspunkte, die aus datenschutzrechtlicher Sicht beim ursprünglichen Vertrag von Prüm vorgebracht wurden, müssen erst recht bei der Überführung des Vertrages in europäisches Recht berücksichtigt werden, denn hier wird langfristig die DNA- und daktyloskopische Praxis aus 27 EU-Mitgliedstaaten zusammengeführt.

Wegen der dargestellten Probleme ist eine intensive grenzüberschreitende Kooperation der in den Vertragstexten ausdrücklich erwähnten nationalen Datenschutzkontrollinstanzen unerlässlich.

13.3.3 EUROPOL

EUROPOL erhält eine neue Rechtsgrundlage in Form eines Ratsbeschlusses. Darüber hinaus werden seine Aufgaben und Befugnisse erweitert. Diese Gelegenheit wurde nicht genutzt, um die bestehenden datenschutzrechtlichen Defizite zu beheben.

Die EU-Kommission hat am 20. Dezember 2006 den Vorschlag für einen Beschluss des Rates zur Errichtung

des Europäischen Polizeiamtes (EUROPOL) vorgelegt, mit dessen Beratung im Rat zu Beginn des Jahres 2007 begonnen wurde. Dieser Rechtsakt soll an die Stelle des geltenden EUROPOL-Übereinkommens aus dem Jahre 1995 treten, weil er nicht ratifiziert werden muss und somit relativ leicht neuen Anforderungen angepasst werden kann. Der Vorschlag berücksichtigt die drei Änderungsprotokolle zu dem EUROPOL-Übereinkommen, die im März 2007 nach teils jahrelangen Ratifizierungsverfahren in Kraft getreten sind. Zudem soll EUROPOL nunmehr aus dem EU-Haushalt finanziert werden, was dem Europäischen Parlament eine stärkere demokratische Kontrolle über diese Behörde ermöglicht.

Die Bedeutung von EUROPOL wird auch deshalb zunehmen, weil es Zugriff auf europaweite Datenbanken wie das SIS II (Nr. 13.3.4) und das VIS (Nr. 13.3.5) erhalten soll. Die Behörde entwickelt sich auf diese Art zu einer zentralen Informationssammelstelle im Bereich der Dritten Säule der EU, was durch ihre ausdrückliche Benennung in Artikel 88 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) (vgl. Vertrag von Lissabon, s. o. Nr. 13.1) unterstrichen wird.

Die Gemeinsame Kontrollinstanz (GKI) von EUROPOL, die sich am 9. Oktober 1998 als Datenschutzkontrollinstanz für die Polizeibehörde konstituiert hatte, hat gemäß ihrem Auftrag eine umfangreiche Stellungnahme zu dem Vorschlag der Kommission abgegeben. Da mit dem Rechtsakt auch die Aufgaben und Befugnisse für EUROPOL erweitert werden, hat die Kontrollinstanz umfangreiche datenschutzrechtliche Begleitmaßnahmen verlangt. Gefordert werden u. a. eine Pflicht zur Konsultation der Gemeinsamen Kontrollinstanz und verbesserte Rechte für den Betroffenen. Macht ein Betroffener sein Recht auf Auskunft gegenüber EUROPOL geltend, soll in Zukunft auf das für EUROPOL geltende Recht abgestellt werden, ohne Berücksichtigung des nationalen Rechts eines anliefernden bzw. sonst involvierten Mitgliedstaates. Dies wird im Endeffekt zu einer einheitlichen und transparenten Auskunftspraxis bei EUROPOL führen. Damit wird auch die Arbeit des Beschwerdeausschusses (17. TB Nr. 11.3) erleichtert werden, der als letzte Instanz für Beschwerden gegen ablehnende Auskunftsbescheide seitens EUROPOL an Stelle eines Gerichts fungiert (vgl. Artikel 33 Absatz 9 des Ratsbeschluss-Entwurfs). Gleichwohl bleiben die Bestimmungen zum Auskunftsrecht hinter vergleichbaren inländischen Regelungen zurück. So bedarf die Verweigerung einer Auskunft z. B. keiner Begründung.

Der Vorschlag für einen Ratsbeschluss zu EUROPOL konnte vom JI-Rat im Berichtszeitraum wegen der Parlamentsvorbehalte zweier EU-Mitgliedstaaten noch nicht verabschiedet werden. Die Beschlussfassung ist nunmehr für Anfang 2009 geplant; der Ratsbeschluss soll zum 1. Januar 2010 in Kraft treten.

Mit dem Ratsbeschluss werden die Aufgaben und Befugnisse von EUROPOL erweitert. Angemessene Verbesserungen der datenschutzrechtlichen Regelungen sind aber nur bedingt erreicht worden.

Die GKI EUROPOL führt jährlich mindestens einen Kontrollbesuch bei der Polizeibehörde durch (vgl. Nr. 13.3.8). Bei einer datenschutzrechtlichen Kontrolle wurden von deutschen Stellen in das dortige Informationssystem eingestellte Datensätze im Hinblick auf ihre EUROPOL-Relevanz in Frage gestellt. Ich habe daraufhin ebenso wie ein mitbetroffener Landesbeauftragter für den Datenschutz beim BKA und bei den für die Eingabe der Datensätze verantwortlichen Polizeibehörden des Bundes und der Länder eine Kontrolle durchgeführt. Dies führte zur Löschung einiger Datensätze. Im Übrigen habe ich darauf gedrungen, dass das BKA seiner Gesamtverantwortung für die Dateneingabe im Außenverhältnis zu EUROPOL nachkommt, während im Inland die datenschutzrechtliche Verantwortung bei derjenigen Stelle verbleibt, die einen für EUROPOL bestimmten Datensatz an das BKA zwecks Weiterleitung an EUROPOL übermittelt. Dieses Verfahren ergibt sich aus dem Vertragsgesetz zu EUROPOL und es ist in einem gemeinsamen Merkblatt für die beteiligten Stellen zwecks Befolgung festgelegt.

Ich gehe davon aus, dass die Verantwortlichkeit für die Feststellung der EUROPOL-Relevanz einer polizeilichen Erkenntnis nunmehr klargestellt ist und künftig nur solche Datensätze an EUROPOL übermittelt werden, die für dessen Aufgabenerfüllung erforderlich sind.

13.3.4 Schengen

Das Schengener Informationssystem der zweiten Generation (SIS II) ist noch nicht betriebsbereit. Wegen der einschneidenden Änderungen fordere ich eine Auditierung für den nationalen Teil.

Das seit 1995 betriebene Schengener Informationssystem (SIS), seit Anfang 2000 erweitert als SIS I+, konnte nicht, wie für 2007 vorgesehen, durch das seit Langem geplante SIS II abgelöst werden (vgl. Kasten zu Nr. 13.3.4; 21. TB Nr. 3.2.4.1). Die Gründe für die Verzögerung waren vergaberechtlicher und technischer Natur. Hingegen wurden die Rechtsgrundlagen für das SIS II zwischenzeitlich verabschiedet; dies gilt insbesondere für die Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des SIS II (ABl. L 381/4 vom 28. Dezember 2006) sowie für den Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des SIS II (ABl. L 205/63 vom 7. August 2007). Wenn auch das SIS II auf mehreren Rechtsakten beruht, wird es doch seinen Charakter als einheitliches System behalten. Die zuvor genannten Rechtsakte sind zwar juristisch in Kraft getreten, gelten jedoch für die teilnehmenden Mitgliedstaaten erst ab dem Zeitpunkt, der vom Rat mit Zustimmung aller Mitgliedstaaten noch festgesetzt wird. Dies hängt insbesondere von der Betriebsbereitschaft des SIS II ab, die für September 2009 erwartet wird.

Kasten zu Nr. 13.3.4

Das Schengener Informationssystem (SIS)

Das Schengener Informationssystem (SIS) ist das Kernstück der Ausgleichsmaßnahmen für den Wegfall der Binnengrenzkontrollen zwischen den Schengen-Staaten. Es enthält Sach- und Personenfahndungen sowie Ausschreibungen zur Einreiseverweigerung gemäß dem Schengener Durchführungsübereinkommen. Technisch besteht das SIS aus einer zentralen Unterstützungseinheit, dem sog. C.SIS in Straßburg und – als Kopie des Zentralbestandes – den jeweiligen nationalen Teilen in den Schengen-Staaten, dem sog. N.SIS.

Durch die Erweiterung des Schengen-Raumes um die nordischen Länder Dänemark, Finnland, Schweden, Norwegen und Island und dem damit einhergehenden erhöhten Datenvolumen im SIS waren technische Anpassungen erforderlich, die mit der Inbetriebnahme des SIS I+ Anfang 2000 realisiert wurden.

Um den zum 1. Mai 2004 der EU beigetretenen Mitgliedstaaten die Teilnahme am SIS zu ermöglichen, aber auch, um das System an die wachsenden Anforderungen bei der Bekämpfung der grenzüberschreitenden Kriminalität, des internationalen Terrorismus und der illegalen Zuwanderung anzupassen, wurde im Jahr 2001 das SIS II-Projekt begonnen. Das SIS II soll neue Funktionalitäten enthalten, die u. a. Abfragen nach biometrischen Daten, wie Fingerabdrücke und Lichtbilder, ermöglichen.

Da eine Inbetriebnahme des SIS II wegen technischer und logistischer Probleme zum vorgesehenen Einführungstermin nicht möglich war, wurde als Zwischenlösung eine erweiterte Version des SIS I+, dass sog. SISone4all, parallel zum SIS II entwickelt und im Sommer 2007 in Betrieb genommen. Damit konnten die neuen EU-Mitgliedstaaten am Schengener Fahndungsverbund als Voraussetzungen für den Wegfall der Binnengrenzkontrollen teilnehmen. Das SIS II soll, sobald es betriebsbereit ist, das SISone4all ersetzen.

Mit der Inbetriebnahme des neuen SIS wird die datenschutzrechtliche Kontrolle für die technische Unterstützungseinheit und die SIS II-Datenbank in Straßburg auf den Europäischen Datenschutzbeauftragten übergehen, während die Kontrolle des nationalen Systems in Deutschland, des N. SIS II, mir als für das BKA zuständige Kontrollinstanz obliegen wird. Ab diesem Zeitpunkt werden auch die Regelungen der Artikel 92 bis 119 SDÜ (Titel IV) außer Kraft treten, die bisher als Rechtsgrundlage für das SIS dienen. Damit wird die Gemeinsame Kontrollinstanz von Schengen, beruhend auf Artikel 115 SDÜ, ihre Existenzberechtigung verlieren. Bevor das SIS II in Wirkbetrieb gehen kann, bedarf es noch einer technisch komplexen Datenmigration vom geltenden SIS I+ zum SIS II. Ich habe im Hinblick auf die schwerwiegenden Änderungen, die mit dem SIS II verbunden sind, u. a. die Einführung weiterer biometrischer Daten wie Lichtbilder und Fingerabdrücke, eine umfassende Vorabkontrolle der dadurch für den nationalen Teil des SIS II entstehenden Folgen vom BMI bzw. BKA gefordert.

Die erheblichen Verzögerungen beim SIS II hätten bewirkt, dass die zehn neuen Mitgliedstaaten, die der EU im Jahre 2004 beigetreten waren, weiterhin vom Schengen-Raum ausgeschlossen wären. Um auch den Bürgerinnen und Bürgern dieser Staaten die Grenzkontrollen an den EU-Binnengrenzen zu ersparen, hat der JI-Rat am 6. Dezember 2007 beschlossen, die Kontrollen an den Land- und Seegrenzen zu neun der neuen Mitgliedstaaten ab dem 21. Dezember 2007 aufzuheben. Für den Luftverkehr wurde der 30. März 2008 als Stichtag für den Wegfall der Binnengrenzkontrollen bestimmt. Als Zwischenlösung musste jedoch das geltende SIS I+ auf bestehender Plattform zu einem SISone4all-System ausgebaut werden, auf das auch die neuen Mitgliedstaaten lesenden und schreibenden Zugriff erhalten. Am 12. Dezember 2008 ist die Schweiz dem Schengen-Raum beigetreten, so dass der Grenzverkehr zwischen Deutschland und seinen Nachbarstaaten auf dem Landweg frei von Personenkontrollen abläuft.

Der von der Bundesregierung im September 2008 beschlossene Gesetzentwurf zum Schengener Informationssystem der zweiten Generation (SIS II) war bis Redaktionsschluss noch nicht vom Bundestag verabschiedet. Er enthält im Wesentlichen die notwendige Anpassung innerstaatlicher Vorschriften als Konsequenz der o. g. europäischen Rechtsakte zur Einrichtung des SIS II. Bei der Vorbereitung des Gesetzentwurfs habe ich darauf gedrängt, dass die fortlaufende Duplizierung eines Teils des Schengener Fahndungsbestandes für Zwecke des Ausländerzentralregisters (AZR) im Gesetz klargestellt werden sollte. Das BMI hat diesen Vorschlag leider nicht aufgegriffen.

Der Entwurf des SIS-II-Gesetzes enthielt auch eine Anpassung des § 17 Absatz 3 BVerfSchG, eingefügt durch das Terrorismusbekämpfungsgesetz vom 5. Januar 2007 (BGBl. I 2007 S. 2), mit dem den Nachrichtendiensten erstmals die Befugnis zur Ausschreibung von Personen und Sachen in INPOL sowie im SIS eingeräumt wurde (21. TB Nr. 5.1.2). Da die Bezugnahme auf Artikel 99 Absatz 3 SDÜ wegen Aufhebung von Titel IV des Schengener Durchführungsübereinkommens obsolet wird, erfolgt nunmehr eine entsprechende Bezugnahme auf den Beschluss 2007/533/JI des Rates vom 12. Juni 2007 (s. o.). Die Nachrichtendienste haben im Berichtszeitraum mit der Einstellung solcher Ausschreibungen im SIS begonnen. Allerdings erfolgen diese vorerst im Wege der Amtshilfe durch das BKA. Den Diensten steht jedoch ein lesender Zugriff auf ihre Ausschreibungen offen. Ich werde diese Praxis mit Blick auf das Trennungsgebot sorgfältig beobachten.

Das SIS II wird in Folge neuer Funktionalitäten und erweiterter Daten, u. a. weiterer biometrischer Daten (s. o.), zu einem Kernelement der Sicherheitsarchitektur der 25 angeschlossenen Vertragsparteien werden. Damit besteht die Gefahr, dass es sich zu einem zentralen polizeili-

chen Recherchesystem in Europa entwickelt, das wegen seiner komplexen Struktur nur noch schwer von den europäischen Datenschutzinstanzen zu beaufsichtigen wäre. Es gilt deshalb, den Charakter dieses Systems als Ausschreibungs- und Fahndungsdatei zu wahren und die dort gespeicherten Ausschreibungsdaten gegen zweckfremde Nutzung zu schützen. Das SIS II wird Hunderttausenden von Nutzern zugänglich sein. Es bedarf deshalb der engen Zusammenarbeit zwischen dem Europäischen Datenschutzbeauftragten und seinen nationalen Kollegen zur Ausübung der datenschutzrechtlichen Kontrolle auf europäischer und nationaler Ebene.

13.3.5 Zugriff der Sicherheitsbehörden auf das Visa-Informationssystem

Am 23. Juni 2008 hat der Rat der Europäischen Union den Beschluss über den Zugang zum Visa-Informationssystem (VIS) angenommen (ABl. L 218 vom 13. August 2008, S. 129), der mit dem VIS-Zugangsgesetz umgesetzt werden soll. Meine Bedenken gegen das vorgesehene Zugriffsverfahren wurden nicht berücksichtigt.

Nach dem VIS-Zugangsbeschluss soll der Zugriff auf das VIS (s. auch unter Nr. 16.2) nur über zentrale Zugangsstellen in den EU-Mitgliedstaaten erfolgen. Sie prüfen, ob der Zugriff der Sicherheitsbehörden auf das VIS im Einzelfall zur Verhütung, Aufdeckung oder Ermittlung von terroristischen und sonstigen schwerwiegenden Straftaten erforderlich ist. Damit ist ein wesentliches Element des Vorschlags der Kommission (21. TB Nr. 3.2.7), die damit routinemäßige Abfragen der Sicherheitsbehörden der ursprünglich zu administrativen Zwecken erhobene Daten verhindern wollte, erhalten geblieben.

Das Zugriffsverfahren soll nach dem VIS-Zugangsgesetz in der Weise umgesetzt werden, dass die zentralen Zugangsstellen lediglich eine formularmäßige Prüfung der Zugangsvoraussetzungen durchführen, wobei eine Bewertung, inwieweit der VIS-Zugang erforderlich ist, nach Plausibilitätsgründen stattfindet. Eine Prüfung anhand der Sachakten der jeweils zugangsberechtigten Behörde soll nicht erfolgen. In Deutschland wird das Bundesverwaltungsamt (BVA) die Funktion der zentralen Zugangsstelle für das BKA, die Bundespolizei, das ZKA, den BND und den MAD sowie für die Landespolizei Berlin übernehmen. Das Bundesamt für Verfassungsschutz ist zentrale Zugangsstelle für die Verfassungsschutzbehörden des Bundes und der Länder, die Landeskriminalämter für ihre jeweiligen Landespolizeibehörden (Ausnahme Berlin).

Ich habe Zweifel, inwieweit dieses Zugriffsverfahren dem Beschluss über den Zugang zum VIS Rechnung trägt, der eine einzelfallbezogene Erforderlichkeitsprüfung vorsieht. Insbesondere gilt dies im Hinblick auf die dem BVA übertragene Aufgabe einer zentralen Zugangsstelle. Ohne Vorlage der Sachakten wird es nicht in der Lage sein, die Angaben der zugangsberechtigten Stellen im formalisierten Zugangsantrag nachzuprüfen. Im VIS-Zugangsgesetz sollte daher festgelegt werden, wer für die Zulässigkeit der jeweiligen Abfrage im VIS und die zu diesem Zweck an das VIS übermittelten personenbezogenen Daten die datenschutzrechtliche Verantwortung trägt. Dass dies die zentrale Zugangsstelle im Hinblick auf die Umstände der von ihr durchzuführenden Prüfung nicht alleine sein kann, liegt auf der Hand. Die Situation ist vergleichbar mit der Übermittlung personenbezogener Daten an EUROPOL durch die nationale Stelle BKA. Das EUROPOL-Gesetz sieht vor, dass unbeschadet der datenschutzrechtlichen Verantwortung des BKA als nationale Stelle innerstaatlich die eingebende Stelle die datenschutzrechtliche Verantwortung nach dem EUROPOL-Übereinkommen trägt. Eine in dieser Weise aufgeteilte Verantwortlichkeit müsste auch im VIS-Zugangsgesetz normiert werden.

Ein weiteres Problem liegt darin, dass der VIS-Zugangsbeschluss den Sicherheitsbehörden den Zugriff auf das VIS mittels eines einzelnen dort gespeicherten Datums erlaubt. Die unmittelbare Anwendung dieser Regelung hätte zur Folge, dass ein Zugriff zu einer großen Menge an Treffern über Unbeteiligte führen würde. Abgesehen davon, dass eine derartige Streubreite unter datenschutzrechtlichen Gesichtspunkten nicht akzeptabel ist, dürfte es auch nicht im Interesse der Sicherheitsbehörden liegen, unscharfe und nicht verwertbare Informationen aus dem VIS zu bekommen. Ich halte es daher für geboten, im VIS-Zugangsgesetz zusätzlich festzulegen, dass eine Abfrage im VIS nur mit bestimmten Grunddaten wie Vor- und Zuname, Geburtsdatum sowie der Nummer des Reisedokuments zulässig ist.

Beide Anregungen sind von der Bundesregierung nicht berücksichtigt worden. Im Rahmen des parlamentarischen Gesetzgebungsverfahrens werde ich mich für entsprechende Verbesserungen des VIS-Zugangsgesetzes einsetzen.

13.3.6 Umsetzung der „Schwedischen Initiative“ zur Vereinfachung des Informationsaustausches zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten

Die „Schwedische Initiative“ zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU-Mitgliedstaaten ist in innerstaatliches Recht umzusetzen. Dabei muss der verbleibende Spielraum zur Verbesserung des Datenschutzes genutzt werden.

Der Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 (ABl. L 386 vom 29. Dezember 2006 S. 89) über die Vereinfachung des Austausches von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten, die sog. Schwedische Initiative, ist am 30. Dezember 2006 in Kraft getreten (20. TB Nr. 3.3.4). Seine Regelungen sind nun in nationales Recht umzusetzen.

Durch den Rahmenbeschluss sollen die Strafverfolgungsbehörden rechtzeitig Zugang zu Erkenntnissen der Strafverfolgungsbehörden in den anderen EU-Mitgliedstaaten erhalten, um Straftaten und andere kriminelle Aktivitäten zu verhindern und zu verfolgen. Die zentrale Regelung des Rahmenbeschlusses sieht vor, für den Austausch von Informationen und Erkenntnissen mit den Strafverfol-

gungsbehörden anderer Mitgliedstaaten dieselben Bedingungen vorzusehen wie für den Datenaustausch im innerstaatlichen Bereich. Angestrebt wird eine weitere Intensivierung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen. Das Ziel, in der EU einen Raum der Freiheit, der Sicherheit und des Rechts zu schaffen, setzt aber auch voraus, dass in den Mitgliedstaaten ein gleichwertiger Datenschutz auf hohem Niveau besteht. Deshalb ist der Umstand, dass dies mit der Verabschiedung des Rahmenbeschlusses zum Datenschutz in der Dritten Säule (vgl. Nr. 13.3.1) nur in Ansätzen erreicht wird, bei der Umsetzung der „Schwedischen Initiative" zu berücksichtigen, zumal die Verwendung der Informationen sich nach dem Recht des jeweiligen Empfängerstaates richtet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6./7. November 2008 hat hierzu den Gesetzgeber aufgefordert, den bei der Umsetzung verbleibenden Spielraum konsequent zu nutzen und die Befugnisse zur Informationsübermittlung an Strafverfolgungsbehörden anderer EU-Mitgliedstaaten normenklar unter Beachtung des Grundsatzes der Verhältnismäßigkeit gesetzlich zu regeln (s. Kasten zu Nr. 13.3.6).

Kasten zu Nr. 13.3.6

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008

Besserer Datenschutz bei der Umsetzung der „Schwedischen Initiative" zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU-Mitgliedstaaten geboten

Der Rahmenbeschluss des Rates zur Vereinfachung des Informationsaustausches zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten (sog. „Schwedische Initiative") vom 18. Dezember 2006 verpflichtet diese, an die grenzüberschreitende Übermittlung personenbezogener Daten innerhalb der EU keine höheren Anforderungen zu stellen, als auf nationaler Ebene für den Datenaustausch zwischen Polizei- und Strafverfolgungsbehörden gelten. Seine Umsetzung wird zu einem deutlichen Anstieg und zur Beschleunigung des Informationsaustausches und damit zu einer weiteren Intensivierung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen auf EU-Ebene führen. Das erstrebte Ziel, nämlich die Schaffung eines Raumes der Freiheit, der Sicherheit und des Rechts setzt aber auch voraus, dass in den Mitgliedstaaten ein möglichst gleichwertiger Datenschutz auf hohem Niveau besteht. Dies ist bislang nicht erfüllt. Es besteht nach wie vor der aus datenschutzrechtlicher Sicht unhaltbare Zustand, dass die auf EU-Ebene ausgetauschten polizeilichen Informationen in den jeweiligen EU-Mitgliedstaaten unterschiedlichen Datenschutzregelungen hinsichtlich ihrer Verwendung unterworfen sind. Zudem gelten keine einheitlichen Rechte auf Auskunft, Berichtigung und Löschung der Datenverarbeitung für die Betroffenen in den Empfängerstaaten.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, den bei der innerstaatlichen Umsetzung der „Schwedischen Initiative" verbleibenden Spielraum zu nutzen und die Befugnisse zum Informationsaustausch mit den Strafverfolgungsbehörden der EU-Mitgliedstaaten für die nationalen Polizei- und Strafverfolgungsbehörden normenklar und unter Beachtung des Grundsatzes der Verhältnismäßigkeit gesetzlich zu regeln. Dazu zählen insbesondere:

- Ausschluss der gesonderten Erhebung der angefragten Daten durch die Strafverfolgungsbehörden allein um diese zu übermitteln,
- eindeutige inhaltliche Anforderungen, die an ein Ersuchen um Datenübermittlung zu stellen sind, um Überschussinformationen zu vermeiden,
- Regelung enger Voraussetzungen für sog. Spontanübermittlungen, um für den Empfänger nutzlose und damit nicht erforderliche Übermittlungen auszuschließen,
- Nutzung des Spielraums bei der Ausgestaltung der Verweigerungsgründe, um unverhältnismäßige Datenübermittlungen zu verhindern,
- normenklare Abgrenzung der Befugnis zur Übermittlung von Daten zu präventiven Zwekken gegenüber der justiziellen Rechtshilfe,
- vollständige Umsetzung der Datenschutzbestimmungen in Artikel 8 des Rahmenbeschlusses und begrenzende Regelungen zur Weiterübermittlung an Drittstaaten,
- normenklare Bestimmung welche Behörden als zuständige Strafverfolgungsbehörden im Sinne des Rahmenbeschlusses gelten und welche Informationen nur durch Ergreifen von Zwangsmaßnahmen im Sinne des Rahmenbeschlusses verfügbar sind,
- normenklare Bestimmung, welche Informationen nicht vom Rahmenbeschluss erfasst werden, weil sie für die Strafverfolgungsbehörden nur durch das Ergreifen von Zwangsmaßnahmen verfügbar sind.

13.3.7 Kontrolle der EU-Außengrenzen

Die Europäische Kommission veröffentlichte weitere Pläne für ein effizienteres Border Management an den Außengrenzen der Europäischen Union.

Die Kommission hat am 13. Februar 2008 eine Mitteilung an das Europäische Parlament, den Rat und weitere Empfänger veröffentlicht, mit der sie drei Maßnahmen für ein wirksameres Border Management ankündigt:

– Vorbereitung der nächsten Schritte für die Grenzverwaltung in der EU,

– Prüfung der Schaffung eines Europäischen Grenzkontrollsystems (EUROSUR) und

– Bericht über die Evaluierung und künftige Entwicklung der Agentur FRONTEX.

Die Verwirklichung dieser Pläne hätte weit reichende Auswirkungen auf die Bewegungsfreiheit der europäischen Bürgerinnen und Bürger. Zudem würde massiv in deren Persönlichkeitsrechte eingegriffen, denn die Überwachung der EU-Außengrenzen wäre mit einer umfangreichen Erhebung und dem Austausch personenbezogener Daten unter Zuhilfenahme biometrischer Verfahren verbunden.

Deshalb haben sich die Artikel-29-Gruppe (s. o. Nr. 13.2) und die „Working Party on Police and Justice – WPPJ –“ (vgl. Nr. 13.3.8) mit einem gemeinsamen Schreiben und ergänzenden Bemerkungen an die zuständigen Stellen der Kommission gewandt. Darin weisen sie insbesondere auf die schwerwiegenden Folgen des Maßnahmenkatalogs für die Bürgerinnen und Bürger in der EU hin, stellen die Erforderlichkeit der Maßnahmen in Frage und fordern eine umfangreiche Folgenabschätzung des Maßnahmenbündels, insbesondere unter dem Gesichtspunkt des Datenschutzes.

Auch die Europäische Datenschutzkonferenz vom 16. bis 18. April 2008 hat eine Entschließung zu dem Maßnahmenpaket verabschiedet und vor den gravierenden Auswirkungen auf die Rechte der Bürgerinnen und Bürger gewarnt (s. Anlage 10, Nr. 13.8). Ich habe diese Entschließung auch der Bundesregierung zur Kenntnis gebracht, worauf mir der Bundesminister des Innern versichert hat, dass alle zukünftigen Maßnahmen und Systeme in diesem Zusammenhang in Einklang mit Gemeinschaftsrecht, Menschenrechten, internationalem Schutz und auch den Prinzipien des Datenschutzes stehen werden.

Die Initiative der Kommission zum Ausbau der Grenzkontrollen ist auch vor dem Hintergrund nationaler Projekte in diesem Bereich zu sehen. Bereits seit 2004 wird am Flughafen Frankfurt/Main auf freiwilliger Basis ein automatisiertes Grenzabfertigungssystem betrieben (vgl. 20. TB Nr. 5.3.5), bisher als Pilotprojekt, das jedoch laut BMI zum Dauerbetrieb zugelassen werden soll. Seit Kurzem ist ein weiteres Projekt „GAnGEs“ in Vorbereitung (vgl. Nr. 6.4), mit dem ebenfalls Erkenntnisse für eine schnellere Grenzabfertigung mittels Gesichtsfelderkennung gewonnen werden sollen. Gegen mehr Effizienz bei der Grenzabfertigung ist grundsätzlich nichts einzuwenden, denn sie liegt auch im Interesse der betroffenen Passagiere; wenn dies jedoch mit der Speicherung und weiteren Nutzung personenbezogener Daten in Referenzdatenbanken unter Zuhilfenahme Biometrie gestützter Personenidentifizierungsdokumente verbunden ist, müssen die notwendigen datenschutzrechtlichen Vorkehrungen zur Wahrung der elektronischen Identität (vgl. Nr. 6.3) gewährleistet sein.

13.3.8 Tätigkeit der Datenschutzkontrollgremien

Die zunehmende polizeiliche und justizielle Zusammenarbeit zwischen den Mitgliedstaaten der Europäischen Union bedingt auch eine verstärkte grenzüberschreitende datenschutzrechtliche Kooperation.

Die zunehmende grenzüberschreitende polizeiliche und justizielle Zusammenarbeit der zuständigen Sicherheitsbehörden in den EU-Mitgliedstaaten, verbunden mit einem vermehrten Austausch personenbezogener Daten, macht zum Schutz der Bürgerrechte eine bessere grenzüberschreitende Datenschutzkontrolle erforderlich (s. auch Nr. 13.3.). Bei der Kontrolle der EU-weit betriebenen Datenbanksysteme (SIS I+, EUROPOL-Informationssystem, Zollinformationssystem ZIS) wird dies bereits durch die gemeinsamen Datenschutzkontrollinstanzen von Schengen, EUROPOL und ZIS erreicht, teils auch durch den Europäischen Datenschutzbeauftragten (EDPS), u. a. bei Eurodac (vgl. 21. TB Nr. 3.2.8), in Kooperation mit den nationalen Kontrollbehörden. Anzustreben ist eine umfassende Datenschutzkontrolle dieser Datenbanken, die durch Kontrollen auf nationaler Ebene komplettiert wird. Die Kontrollen erfolgen sowohl vor Ort durch gemeinsame Prüfteams, z. B. bei EUROPOL (vgl. 21. TB Nr. 3.2.3.2), als auch koordiniert durch die Kontrollinstanzen mittels umfangreicher Fragebögen (vgl. 21. TB Nr. 3.2.4.2 und Nr. 3.2.5). Auch beim Informationsaustausch zur Durchführung des Vertrages von Prüm haben die nationalen Datenschutzbehörden eine intensive grenzüberschreitende Datenschutzkontrolle vereinbart. Die gemeinsame datenschutzrechtliche Kontrolle muss weiter zunehmen, wenn der Vertrag von Prüm in den EU-Rechtsrahmen überführt und von 27 Mitgliedstaaten vollzogen wird (vgl. Nr. 13.3.2). Nach Inkrafttreten des Vertrages von Lissabon (vgl. Nr. 13.1) dürften die meisten der europaweit oder durch europäische Institutionen betriebenen Datenbanken der datenschutzrechtlichen Kontrolle durch den EDPS unterfallen, der zur Durchsetzung eines gleichwertig hohen Datenschutzniveaus auf die Zusammenarbeit mit den nationalen Datenschutzkontrollinstanzen angewiesen sein wird.

Die nachgehende Datenschutzkontrolle bedarf der Ergänzung durch proaktive Maßnahmen. Datenschutz muss also bereits bei der Entscheidung über die einschlägigen europäischen Rechtsakte und bei der Einrichtung entsprechender Datenbanken berücksichtigt werden. Es bedarf eines Forums der unabhängigen Datenschutzbehörden aus den Mitgliedstaaten, das die datenschutzrechtlichen Belange gegenüber den Entscheidungsträgern auf der

EU-Ebene (Kommission, Rat und Europäisches Parlament) vertritt. Da der Rahmenbeschluss zum Datenschutz in der Dritten Säule (vgl. Nr. 13.3.1) dies nicht vorsieht, hat die Europäische Datenschutzkonferenz bei ihrer Frühjahrstagung im Mai 2007 (vgl. Nr. 13.8) die Einsetzung der Working Party on Police and Justice (WPPJ) beschlossen, die seitdem unter dem Vorsitz des italienischen Kollegen, zu regelmäßigen Sitzungen in Brüssel zusammentrifft. Dieses Gremium befasst sich sowohl mit aktuellen Fragestellungen im Bereich der Dritten Säule, z. B. zum Rahmenbeschluss zum Datenschutz, aber auch mit langfristigen Initiativen für eine intensivere Zusammenarbeit der Datenschutzbehörden der EU-Mitgliedstaaten. Ich trete weiterhin dafür ein, das Forum der Datenschutzbehörden für die Dritte Säule im europäischen Recht zu verankern. Eine entsprechende Einrichtung im Bereich der Ersten Säule, die Artikel-29-Gruppe (vgl. Nr. 13.2.) liefert seit Jahren allgemein anerkannte Impulse für die europaweite Harmonisierung des Datenschutzes und die Koordination der Datenschutzaufsicht. Auch das Forum für die Dritte Säule bedarf einer formellen Grundlage, d. h. einer klaren Aufgabenbeschreibung durch einen europäischen Rechtsakt und sollte mit den erforderlichen finanziellen und organisatorischen Mitteln, z. B. einem Sekretariat, ausgestattet sein.

Die polizeiliche und justizielle Zusammenarbeit in Strafsachen zwischen den EU-Mitgliedstaaten hat auch enorme Auswirkungen auf den Datenschutz in den Ländern. Um den dortigen Landesbeauftragten einen raschen Zugriff auf die aktuelle Rechtsentwicklung in der EU zu ermöglichen, wurde von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Einsetzung eines Unterarbeitskreises Europa im Rahmen des Arbeitskreises Sicherheit beschlossen, der die gemeinsamen Aktivitäten der Datenschutzbeauftragten des Bundes und der Länder koordinieren soll. Dieser Unterarbeitskreis hat seit seiner Einsetzung bereits mehrfach getagt und dabei u. a. Entschließungsentwürfe für die nationale Datenschutzkonferenz ausgearbeitet.

Diese zunehmenden Anforderungen sind nur zu erfüllen, wenn die Datenschutzbehörden auch personell gestärkt werden. Ohne eine verbesserte personelle Ausstattung sehe ich die Gefahr, dass der immer intensivere transnationale Datenaustausch der Sicherheitsbehörden ohne angemessenes datenschutzrechtliches Korrektiv bleibt (vgl. auch Nr. 15.11).

13.4 Deutsch-amerikanisches Regierungsabkommen zur Bekämpfung schwerwiegender Kriminalität

Das nach dem Vorbild des Prümer Vertrages abgeschlossene deutsch-amerikanische Regierungsabkommen über die Zusammenarbeit der Sicherheitsbehörden weist erhebliche datenschutzrechtliche Defizite auf. Insbesondere fehlen subjektive Rechte der Betroffenen auf Auskunft, Berichtigung, Löschung oder Sperrung.

Am 1. Oktober 2008 wurde das deutsch-amerikanische Regierungsabkommen über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität von den Vertragsparteien unterzeichnet. Die USA und Deutschland räumen sich danach einen gegenseitigen Zugriff auf daktyloskopische Daten und DNA-Profile nach dem Muster des Prümer Vertrages (vgl. Nr. 13.3.2), d. h. auf entsprechende Fundstellendatensätze im hit/no-hit-Verfahren ein. Zudem werden die Regelungen des Prümer Vertrages zum Austausch personenbezogener Daten zur Verhinderung von terroristischen Straftaten weitgehend übernommen. Auf eine Übertragung der als Bedingung für diese umfangreichen Zugriffs- und Übermittlungsbefugnisse im Prümer Vertrag geschaffenen Datenschutzregelungen ist jedoch weitgehend verzichtet worden.

Ich habe stets darauf hingewiesen, dass ich mindestens die Vereinbarung eines Datenschutz-Regimes wie nach dem Prümer Vertrag angesichts des sensiblen Datenmaterials und wegen des deutlich niedrigeren Datenschutzniveaus in den USA im vorliegenden Regierungsabkommen für unerlässlich erachte. Insbesondere halte ich es für bedenklich, dass das Abkommen keine subjektiven Rechte der Betroffenen auf Auskunft, Berichtigung, Löschung oder Sperrung enthält. Dieser Mangel wird nicht dadurch ausgeglichen, dass die auf nationaler Ebene bestehenden Rechte der Betroffenen vermittelt durch eine Vertragspartei auf völkerrechtlicher Ebene wahrgenommen werden können. Für die Betroffenen besteht, etwa bei abgelehnten Auskunfts- oder Berichtigungsverlangen, nicht die Möglichkeit, effektiven Rechtsschutz von unabhängigen Stellen gegenüber diesen Entscheidungen zu erlangen. Es entsteht damit eine vergleichbare Situation wie im Zusammenhang mit den von den Vereinten Nationen geführten Listen über Terrorverdächtige (vgl. Nr. 13.6).

Neben diesem grundlegenden Mangel bestehen gegen das Regierungsabkommen auch unter anderen Gesichtspunkten erhebliche Vorbehalte. So werden in den USA polizeiliche Daten über Jahrzehnte gespeichert und es fehlt an einer unabhängige Datenschutzkontrolle. Vor diesem Hintergrund halte ich es nicht für ausreichend, auf den Grundsatz der Erforderlichkeit oder auf das jeweilige nationale Recht bei der Löschung der ausgetauschten Daten abzustellen. Vielmehr wäre es geboten gewesen, Höchst- oder Aussonderungsprüffristen festzulegen. Das Abkommen enthält auch keine gemeinsame Definition terroristischer Straftaten bzw. schwerwiegender Kriminalität als Voraussetzung für den Austausch personenbezogener Daten bzw. den Zugriff auf diese. Es erfolgt hierzu lediglich der Verweis auf das jeweilige nationale Recht. Das Verständnis von „schwerwiegender Kriminalität“ bzw. „terroristischen Straftaten“ dürfte jedoch unterschiedlich sein. Auch die vorgesehenen weiten Öffnungsklauseln hinsichtlich der Verarbeitung der nach diesem Abkommen ausgetauschten Informationen sind zu weit gefasst und aus datenschutzrechtlicher Sicht nicht akzeptabel.

Diese Mängel, auf die auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. April 2008 hingewiesen hat (s. Kasten zu Nr. 13.4), werden auch nicht durch den von der Bundesregierung mittlerweile vorgelegten Entwurf eines Vertrags- und Umsetzungsgesetzes zu dem Regierungsabkommen ausgeglichen. Nach dem Inhalt des Umsetzungsgesetzes soll das BKA in Vertretung für Deutschland zwar verpflichtet werden, auf Antrag des Betroffenen die nach dem Regierungsabkommen bestehenden völkerrechtlichen Ansprüche auf Auskunft, Berichtigung, Sperrung und Löschung gegenüber den USA geltend zu machen. Andererseits soll die Auskunft u. a. bei überwiegenden Geheimhaltungsinteressen ausgeschlossen werden können.

Im Zusammenhang mit der innerstaatlichen Umsetzung des Abkommens ist derzeit noch nicht entschieden, ob unter die daktyloskopischen Daten, auf die den US-Behörden der Zugriff eingeräumt werden soll, auch die Fingerabdruckdaten von Asylbewerbern oder Ausländern nach dem Aufenthaltsgesetz gefasst werden. Im Hinblick auf die Sensibilität daktyloskopischer Daten einerseits und das Fehlen eines angemessenen Datenschutzniveaus in den USA andererseits trete ich nachdrücklich dafür ein, den automatisierten Zugriff auf Fundstellendatensätze daktyloskopischer Daten von Straftätern zu begrenzen.

Die Ressortberatungen zum Entwurf des Umsetzungsgesetzes waren bei Redaktionsschluss noch nicht abgeschlossen.

Kasten zu Nr. 13.4

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008

Unzureichender Datenschutz beim deutsch-amerikanischen Abkommen über die Zusammenarbeit der Sicherheitsbehörden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beobachtet mit Sorge, dass die Datenschutzrechte der Bürgerinnen und Bürger im Rahmen der internationalen Zusammenarbeit der Sicherheitsbehörden immer häufiger auf der Strecke bleiben. Aktuelles Beispiel ist das am 11. März 2008 paraphierte deutsch-amerikanische Regierungsabkommen über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität. Die Konferenz fordert Bundestag und Bundesrat auf, dem Abkommen solange nicht zuzustimmen, bis ein angemessener Datenschutz gewährleistet ist.

Mit dem Abkommen wurde ein gegenseitiger Online-Zugriff auf Fundstellendatensätze von daktyloskopischen Daten und DNA-Profilen im hit/no-hit-Verfahren nach dem Muster des Prümer Vertrages vereinbart. Zudem wurden dessen Regelungen über den Austausch personenbezogener Daten zur Verhinderung terroristischer Straftaten weitgehend übernommen. Eine Übertragung des als Bedingung für diese umfangreichen Zugriffs- und Übermittlungsbefugnisse im Prümer Vertrag geschaffenen Datenschutzregimes erfolgte jedoch nicht.

Die Voraussetzungen, unter denen ein Datenaustausch erlaubt ist, sind nicht klar definiert. Der Datenaustausch soll allgemein zur Bekämpfung von Terrorismus und schwerer Kriminalität möglich sein. Welche Straftaten darunter konkret zu verstehen sind, wird nicht definiert. Es erfolgt hier lediglich der Verweis auf das jeweilige nationale Recht. Damit trifft nach dem Abkommen die USA einseitig eine Entscheidung über die Relevanz der abgerufenen Daten.

Bevor in so großem Umfang zusätzliche Datenübermittlungen erlaubt werden, muss zunächst geklärt werden, warum die bisherigen Datenübermittlungsbefugnisse für die internationale Polizeizusammenarbeit mit den USA nicht ausreichen.

Für die weitere Verarbeitung aus Deutschland stammender Daten in den USA bestehen für die Betroffenen praktisch keine Datenschutzrechte. Das Abkommen selbst räumt den Betroffenen keine eigenen Rechte ein, sondern verweist auch hierzu auf die Voraussetzungen im Recht der jeweiligen Vertragspartei. In den USA werden aber Datenschutzrechte, wie sie in der Europäischen Union allen Menschen zustehen, ausschließlich Bürgerinnen und Bürgern der Vereinigten Staaten von Amerika und dort wohnenden Ausländerinnen und Ausländern gewährt. Anderen Personen stehen Rechtsansprüche auf Auskunft über die Verarbeitung der eigenen Daten, Löschung unzulässig erhobener oder nicht mehr erforderlicher Daten oder Berichtigung unrichtiger Daten nicht zu. Außerdem besteht in den USA keine unabhängige Datenschutzkontrolle. Vor diesem Hintergrund sind die im Abkommen enthaltenen weiten Öffnungsklauseln für die weitere Verwendung der ausgetauschten Daten sowie der Verzicht auf Höchstspeicherfristen aus datenschutzrechtlicher Sicht nicht akzeptabel.

13.5 Fluggastdaten

Seit dem 11. September 2001 werten immer mehr Staaten die von Fluggesellschaften erhobenen Fluggastdatensätze, die sog. PNR-Daten aus. Sie wollen damit Personen mit hohem kriminellem oder terroristischem Gefährdungspotenzial herausfiltern.

Die Verarbeitung dieser Daten stellt einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung in erster Linie unbescholtener Bürgerinnen und Bürger dar. Den Nachweis, dass diese Daten unerlässlich sind, um den Terrorismus oder organisiertes Verbrechen wirksam zu bekämpfen, konnten weder die beteiligten Regierungen noch die EU-Institutionen erbringen.

Im Berichtszeitraum hatte ich mich vor allem mit entsprechenden Vorhaben auf EU-Ebene zu befassen. Bedeutsam waren insbesondere das zwischen den USA und der EU ausgehandelte dritte Abkommen zur Übermittlung von Fluggastdaten (Nr. 13.5.2) und der Vorschlag der Kommission für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdaten zu Strafverfolgungszwecken (Nr. 13.5.3).

13.5.1 Übermittlung von Flugpassagierdaten (PNR)

Globale Standards sind dringender denn je.

Flugreisende geben bei jeder Buchung eine Reihe von Daten an, die die Fluggesellschaft benötigt, um die Reise im gewünschten Umfang durchführen zu können. Dabei handelt es sich etwa um das Datum der Reise, Essenswünsche oder die Art der Bezahlung – Daten, die dann von den Fluggesellschaften in deren Buchungs- und Reservierungssystemen als PNR (Passenger Name Record)-Daten gespeichert werden (s. Kasten a zu Nr. 13.5.1).

Kasten a zu Nr. 13.5.1

Unterrichtung der Fluggäste

Die Artikel-29-Gruppe hat sich in der Vergangenheit wiederholt mit der Frage beschäftigt, wie Verbraucher und Kunden besser über ihre bestehenden Datenschutzrechte unterrichtet werden können. In ihrem Arbeitspapier 151 vom 24. Juni 2008 gibt die Artikel-29-Gruppe den Fluggesellschaften detaillierte Informationen an die Hand, wie sie ihre Passagiere über die Nutzung von Passagierdaten durch staatliche Stellen zu unterrichten haben und wie Fluggäste ihre Rechte wahrnehmen können.

Großen Wert legt die Artikel-29-Gruppe darauf, dass die Passagiere nicht erst beim Einchecken über die Übermittlung der Daten unterrichtet werden, sondern spätestens dann, wenn die Flugbuchung erfolgt. Dabei soll genau aufgeführt werden, wer die Daten anfordernde Stelle ist, auf welcher Rechtsgrundlage die Übermittlung der einzelnen Datenelemente erfolgt und zu welchen Zwecken. Auch soll darüber informiert werden, für wie lange die Daten gespeichert werden, an welche Stellen sie weitergeleitet werden können und wo die Fluggäste weitergehende Auskünfte erhalten.

Staatliche Stellen entwickeln weltweit ein zunehmendes Interesse an diesen Daten. Insbesondere seit den Terroranschlägen 2001 verlangen immer mehr Staaten, dass ihnen Fluggesellschaften Passagierinformationen vorab zur Verfügung stellen. Sie versprechen sich davon zusätzliche Erkenntnisse für die Bewertung des Risikos, das von Reisenden ausgeht. Die Daten werden regelmäßig bei der Einreisekontrolle und vielfach auch für Zwecke der Strafverfolgung und Gefahrenabwehr verwendet. Dazu werden die Daten längerfristig gespeichert und mit anderen Informationssammlungen abgeglichen. Die Fluggesellschaften sollen vor Ankunft – vielfach sogar lange Zeit vor dem Abflug – bestimmte Angaben über ihre Fluggäste an die entsprechenden Behörden übermitteln. Diese von immer mehr Staaten bereits praktizierte Datensammlung bringt vielfältige datenschutzrechtliche Probleme mit sich. So werden die Daten für Zwecke verwendet, für die sie nicht erhoben wurden. Die damit verbundene Durchbrechung des Zweckbindungsgrundsatzes wiegt besonders schwer, weil sie generell für alle Flugreisenden und ohne jeden konkreten Anlass erfolgt.

Ein zweiter Problemkreis ist das Datenschutzniveau im Empfängerstaat, insbesondere wenn dort keine Regelungen existieren, die den Anforderungen an einen angemessenen Datenschutzstandard entsprechen.

Schließlich stellt sich die Frage, wie und durch wen die praktische Umsetzung der Datenschutzanforderungen beim Umgang mit Passagierdaten überprüft wird. Ohne ausreichende Rechtsgrundlage ist eine solche Übermittlung an ausländische Stellen auf keinen Fall zulässig. Deshalb hat die EU mittlerweile mit den USA (s. u. Nr. 13.5.2), mit Kanada und mit Australien PNR-Abkommen zur Übermittlung von Passagierdaten geschlossen. In diesen Übereinkommen ist genau geregelt, welche einzelnen Daten an welche Behörden übermittelt werden, wie lange sie dort gespeichert werden und welche Rechte die betroffenen Fluggäste haben. Korea fordert inzwischen gleichfalls den Abschluss eines solchen Abkommens. Weitere Staaten wie Indien wollen die Fluggesellschaften in naher Zukunft auffordern, Passagierdaten zu übermitteln.

Kasten b zu Nr. 13.5.1

Forderung nach globalen Standards

Angesichts dieser Entwicklung hat die Internationale Datenschutzkonferenz 2007 in Montreal globale Standards bei der Übermittlung von Passagierdaten gefordert und in einer Resolution alle staatlichen und supranationalen Einrichtungen wie IATA und ICAO aufgefordert, sich für den Schutz dieser personenbezogenen Daten einzusetzen. Da die Flugunternehmen die Daten für ihre eigenen Geschäftszwecke erheben, ist eine Rechtsgrundlage für die Übermittlung von Passagierdaten an staatliche Stellen zwingend erforderlich, die auf den Prinzipen der Notwendigkeit, Zweckbindung und Datensparsamkeit beruhen muss. Außerdem sind die Reisenden auf die Datenverarbeitung und ihre Rechte hinzuweisen. Zudem verlangt die Internationale Datenschutzkonferenz, bestehende Abmachungen regelmäßig auf ihre Wirksamkeit zu überprüfen (vgl. Anlage 6).

Auch in der EU gibt es Überlegungen, Passagierdaten im Kampf gegen Terrorismus und schwere Kriminalität zu nutzen (s. u. Nr. 13.5.3; vgl. Kasten b zu Nr. 13.5.1).

13.5.2 PNR USA

Das Datenschutzniveau des 2007 geschlossenen PNR-Abkommens mit den USA bleibt weit hinter dem vorheriger Abkommen zurück.

Im Juli 2007 unterzeichneten die USA und die EU das dritte Abkommen zur Übermittlung von Passagierdaten an das US-Heimatschutzministerium, das als langfristige Übereinkunft das im Jahre 2006 ausgehandelte Interimsabkommen ablöste. Das Abkommen trat in Deutschland mit Wirkung vom 1. Januar 2008 in Kraft. In ihrer Stellungnahme kritisierte die Artikel-29-Gruppe insbesondere, dass die Zweckbindung für die Übermittlung der Daten nach wie vor unzureichend bestimmt ist und dass die Anzahl der Datenelemente erhöht wurde, auch wenn das Abkommen nur noch 19 Datensätze vorsieht, die jedoch den vorherigen Datenforderungen fast völlig entsprechen. Auch werden weiterhin sensible Daten an die USA übermittelt. In besonderen Fällen darf das US-Heimatschutzministerium im Gegensatz zu den früheren Abkommen auch solche sensiblen Daten nutzen. Weiterhin wurde die Speicherfrist von dreieinhalb auf 15 Jahre erhöht, wobei sich die US-Seite vorbehält, auch diese Frist noch zu verlängern. Die Weiterleitung der Passagierdaten an US-Stellen und Empfänger in Drittstaaten ist einfacher geworden und unterliegt nicht länger strengen Datenschutzvorgaben. Zudem sieht die Vereinbarung nicht wie früher eine gemeinsame Überprüfung unter Einbeziehung unabhängiger Aufsichtsbehörden vor.

Nach wie vor ungeklärt ist die Frage der Umstellung auf ein aktives Übermittlungsverfahren, das „Push-Verfahren“, da die USA weiterhin die Daten zusätzlich noch aus den Buchungssystemen abrufen wollen (sog. „Pull-Verfahren“). Besonders unerfreulich ist, dass das neue Abkommen den betroffenen Reisenden keine subjektiven Rechte gewährt und dass jede Änderung der US-Gesetzgebung einseitig Auswirkungen auf das Datenschutzniveau des Abkommens haben kann. Auch wenn das Abkommen eine rechtliche Grundlage für die Übermittlung von Passagierdaten in die USA schafft, hätten sich die europäischen Datenschutzbehörden ein datenschutzfreundlicheres Abkommen gewünscht.

13.5.3 Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdaten (PNR-Daten) zu Strafverfolgungszwecken

Die Realisierung des Rahmenbeschlussvorschlages der Europäischen Kommission zur Verwendung von Fluggastdaten zu Strafverfolgungszwecken würde zu einer weiteren Vorratsspeicherung von Daten überwiegend unbescholtener Personen führen.

Im November 2007 legte die Kommission den Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdaten (PNR-Daten) zu Strafverfolgungszwecken vor. Danach ist vorgesehen, die PNR-Daten über Fluggäste internationaler Flüge in Staaten der Europäischen Union oder von diesen in Drittstaaten in nationalen Datenbanken zu speichern, untereinander auszutauschen, auszuwerten und für Zwecke der Verhinderung und Bekämpfung terroristischer Straftaten und von Straftaten der organisierten Kriminalität zu nutzen. Die Fluggesellschaften sollen verpflichtet werden, zu jedem Fluggast 19 personenbezogene Merkmale an die zuständigen Behörden der Mitgliedstaaten zu übermitteln. Dort sollen sie bis zu 13 Jahren aufbewahrt werden. Die Daten sollen auch an Drittstaaten weiter übermittelt werden können.

Im Falle seiner Umsetzung würde dieser Vorschlag zu einer gigantischen Datensammlung sämtlicher die EU-Grenzen mit dem Flugzeug überquerenden Personen in einer Sicherheitsdatei führen, ohne dass die Betroffenen hierfür einen konkreten Anlass gegeben hätten. Eine Vorratsdatenspeicherung dieser Art würde gegen das in der EU-Grundrechtecharta garantierte Grundrecht auf Datenschutz verstoßen und wäre auch mit dem verfassungsrechtlich garantierten Recht auf informationelle Selbstbestimmung nicht vereinbar. In der Begründung wird nicht dargelegt, aus welchen Gründen die Verarbeitung von PNR-Daten unerlässlich für die Gewährleistung der Sicherheit in den Mitgliedstaaten ist. Insbesondere lässt der Vorschlag der Kommission außer Acht, dass bereits mit der Richtlinie 2004/82/EG (API-Richtlinie) die Fluggesellschaften verpflichtet wurden, den zuständigen Behörden der Mitgliedstaaten Fluggastdaten zu übermitteln (vgl. 20. TB Nr. 3.3.5). Mit dieser Richtlinie, deren Regelungen seit dem Jahr 2008 in innerstaatliches Recht umgesetzt sind (Nr. 13.5.4), ist ein Instrument zur Verbesserung der Einreisekontrolle und zur Bekämpfung der illegalen Einwanderung geschaffen worden, das auch zur Bekämpfung des internationalen Terrorismus und sonstiger schwerwiegender Straftaten genutzt werden kann.

Kritische Stellungnahmen zu dem Kommissionsvorschlag, wie auf europäischer Ebene die gemeinsame Stellungnahme WP 145 der Artikel-29-Gruppe (Nr. 13.2) und der Arbeitsgruppe Polizei und Justiz der Europäischen Datenschutzkonferenz (Nr. 13.3.8) vom 5. und 18. Dezember 2007 sowie auf nationaler Ebene die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. April 2008 (s. Kasten zu Nr. 13.5.3), sind bei den bisherigen Beratungen kaum beachtet worden.

Zwar werden in den zuständigen Ratsarbeitsgremien Überlegungen angestellt, die Speicherfristen für PNR-Daten zu reduzieren und Auskunfts-, Berichtigungs- und Löschungsrechte für die von der Verarbeitung ihrer Daten Betroffenen im Rahmenbeschluss zu normieren. An dem Ziel der Speicherung der Daten aller Flugpassagiere auf Vorrat wird jedoch weiter festgehalten.

Vor diesem Hintergrund begrüße ich es zwar, dass die Bundesregierung noch einen Prüfvorbehalt aufrechterhält. Wegen seiner Unvereinbarkeit mit europäischem und nationalem Verfassungsrecht sollte sie den Rahmenbeschlussvorschlag jedoch in Gänze ablehnen.

Kasten zu Nr. 13.5.3

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008

Keine Vorratsspeicherung von Flugpassagierdaten

Die EU-Kommission hat den Entwurf eines Rahmenbeschlusses des Rates zur Speicherung von Flugpassagierdaten und zu deren Weitergabe an Drittstaaten vorgelegt. Künftig sollen die Fluggesellschaften bei Flügen aus der EU und in die EU zu jedem Fluggast insgesamt 19 Datenelemente, bei unbegleiteten Minderjährigen sechs weitere Datenelemente, an eine von dem jeweiligen Mitgliedstaat bestimmte „Zentralstelle" übermitteln. Die Daten sollen bei den Zentralstellen anlass- und verdachtsunabhängig insgesamt 13 Jahre lang personenbezogen gespeichert werden und zur Durchführung von Risikoanalysen dienen. Unter im Einzelnen noch unklaren Voraussetzungen sollen die Daten an Strafverfolgungsbehörden von Nicht-EU-Staaten (z. B. die USA) übermittelt werden dürfen. Neben Grunddaten zur Person, über Reiseverlauf, Buchungs- oder Zahlungsmodalitäten und Sitzplatzinformationen sollen auch andere persönliche Angaben gespeichert werden. Unklar ist, welche Daten unter „allgemeine Hinweise" gespeichert werden dürfen. Denkbar wäre, dass beispielsweise besondere Essenswünsche erfasst werden.

Mit der beabsichtigten Vorratsspeicherung und der Datenübermittlung wird die EU es auswärtigen Staaten ermöglichen, Bewegungsbilder auch von EU-Bürgerinnen und -Bürgern zu erstellen. In Zukunft besteht die Gefahr, dass Menschen Angst haben werden, durch ihre Reisegewohnheiten aufzufallen.

Die in dem Rahmenbeschluss vorgesehene Vorratsdatenspeicherung von Daten sämtlicher Fluggäste, die EU-Grenzen überschreiten, verstößt nicht nur gegen Art. 8 der Europäischen Menschenrechtskonvention und die Europaratskonvention 108, sondern ist auch mit dem im Grundgesetz verankerten Recht auf informationelle Selbstbestimmung nicht vereinbar. Grundrechtseingriffe „ins Blaue hinein", also Maßnahmen ohne Nähe zu einer abzuwehrenden Gefahr, sind unzulässig.

Der Vorschlag für den Rahmenbeschluss erfolgte, ohne den Nutzen der erst jüngst in nationales Recht umgesetzten Richtlinie 2004/82/EG[1], die bereits alle Beförderungsunternehmen verpflichtet, die Daten von Reisenden an die Grenzkontrollbehörden zu übermitteln, auszuwerten. Hinzu kommt, dass der Vorschlag kaum datenschutzrechtliche Sicherungen enthält. Er bezieht sich nur auf eine bisher nicht bestehende und im Entwurf mit Mängeln behaftete EU-Datenschutzregelung. Diese Mängel wirken sich dadurch besonders schwerwiegend aus, dass in den Drittstaaten ein angemessenes Datenschutzniveau nicht immer gewährleistet ist und eine Änderung dieser Situation auch in Zukunft nicht zu erwarten ist.

Die EU-Kommission hat nicht dargelegt, dass vergleichbare Maßnahmen in den USA, in Kanada oder in Großbritannien einen realen, ernst zu nehmenden Beitrag zur Erhöhung der Sicherheit geleistet hätten. Sie hat die kritischen Stellungnahmen der nationalen und des Europäischen Datenschutzbeauftragten sowie der Artikel 29-Datenschutzgruppe nicht berücksichtigt.

Die Konferenz fordert die Bundesregierung auf, den Entwurf abzulehnen. Sie teilt die vom Bundesrat geäußerten Bedenken an der verfassungsrechtlichen Zulässigkeit der Speicherung der Passagierdaten.

[1] RL 2004/82 EG v. 29. April 2004 Amtsbl. L 261 (2004) S. 24 ff., Richtlinie über die Verpflichtung von Beförderungsunternehmen, Angaben über die Beförderten zu übermitteln

13.5.4 Umsetzung der Richtlinie 2004/82/EG zur Übermittlung von Fluggastdaten

Nach dem deutschen Umsetzungsgesetz müssen die Beförderungsunternehmen mehr Daten an die Bundespolizei übermitteln als von der Richtlinie vorgeschrieben.

Die Richtlinie 2004/82/EG über die Verpflichtung der Beförderungsunternehmen, auf Anfrage Angaben über beförderte Personen vorab an die mit der Personenkontrolle an den Außengrenzen der EU beauftragten nationalen Behörden zu übermitteln, ist in innerstaatliches Gesetz umgesetzt worden.

Im Gegensatz zum Rahmenbeschlussvorschlag der Kommission über die Verwendung von PNR-Daten zu Strafverfolgungszwecken (Nr. 13.5.3) zielt die Richtlinie (vgl. 20. TB Nr. 3.3.5) auf die Verbesserung der Grenzkontrollen und der Bekämpfung der illegalen Einwanderung ab. Der Umfang der zu erhebenden und zu übermittelnden Daten ist auf das dafür Notwendige begrenzt. Zudem sind die Daten nach Durchführung der Grenzkontrollen bei den zuständigen Behörden zu löschen. Zwar geht Deutschland bei der Umsetzung in innerstaatliches Recht über den in der Richtlinie vorgesehenen Datenkatalog hinaus (vgl. 21. TB Nr. 3.3.3). Im Laufe des Gesetzgebungsverfahrens konnte jedoch erreicht werden, dass von den ursprünglichen Plänen abgesehen wurde und nunmehr nur noch das „Geschlecht" sowie die „Nummer des Visums" von den Beförderungsunternehmen an die deutschen Grenzschutzbehörden als zusätzliche Daten über-

mittelt werden müssen. Positiv hervorzuheben ist, dass die Daten ausdrücklich nur zur polizeilichen Kontrolle des grenzüberschreitenden Verkehrs und der Verfolgung der in diesem Zusammenhang begangenen Straftaten verwendet werden dürfen und sowohl bei den Beförderungsunternehmen als auch bei der Bundespolizei binnen 24 Stunden nach Erhebung bzw. Übermittlung gelöscht werden müssen. Die Handhabung des Gesetzes in der Praxis bedarf allerdings noch der datenschutzrechtlichen Überprüfung. Dabei wäre auch festzustellen, inwieweit die Bundespolizei entsprechend der eigenen Aussage nur bei bestimmten „risikobehafteten Flugrouten" die Fluggastdaten erheben wird.

13.6 Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige

Die von den Vereinten Nationen (VN) erstellten Listen über terrorverdächtige Personen und Organisationen, die auch in EU-Recht umgesetzt worden sind, widersprechen elementaren rechtsstaatlichen Anforderungen. Das Urteil des Europäischen Gerichtshofes (EuGH) vom 3. September 2008 hat dies im Wesentlichen bestätigt.

Von Vertretern der Medien und der Wirtschaft bin ich immer wieder auf die gravierenden Menschenrechtsprobleme angesprochen worden, die sich für den einzelnen aus der Aufnahme von Betroffenen in die sog. Terrorlisten der VN bzw. der EU ergeben. Grundlage hierfür bilden Resolutionen der VN, nach denen der VN-Sanktionsausschuss Listen mit unter Terrorverdacht stehenden natürlichen und juristischen Personen und Organisationen aufstellt. Die EU setzt die Listen sowie die daran geknüpften Sanktionsmaßnahmen mittels EG-Verordnungen (VO (EG) Nr. 2580/2001, VO (EG) Nr. 561/2003) um.

Personen, die auf diesen Listen erscheinen, unterliegen umfangreichen Beschränkungen, die von Wirtschafts- und Finanzsanktionen über Einreiseverbote bis hin zum Einfrieren ihrer Gelder und anderer Vermögenswerte reichen. Ein Eintrag in die Listen greift damit nicht nur in das informationelle Selbstbestimmungsrecht ein. Er kann darüber hinaus gravierende existenzielle Folgen haben, wie z. B. die Verweigerung von Sozialleistungen.

Die VN- bzw. EU-Terrorlisten und das Verfahren zu ihrer Aufstellung sehe ich unter verschiedenen Aspekten äußerst kritisch. Fraglich ist schon, ob diese Listen überhaupt geeignet sind, Geldströme, mit denen terroristische Aktivitäten finanziert werden sollen, aufzudecken oder zu stoppen. Hierzu liegt seitens der VN bisher keine Bewertung vor. Zum anderen ist das Listing-Verfahren für die Betroffenen nicht transparent. So sind die VN-Mitgliedstaaten zur Anmeldung entsprechender Fälle verpflichtet. Nach welchen Voraussetzungen dies in den einzelnen Ländern geschieht, ist aber nicht bekannt. Zweifel bestehen insbesondere, ob hierbei überall rechtsstaatliche Kriterien zugrunde gelegt werden. Aufgrund der teilweise nur rudimentären Angaben zu den Personen in den „Terrorlisten" besteht zudem die Gefahr von Verwechslungen. Auch in Deutschland ist es zu solchen Fällen gekommen. So hatte z. B. das Job-Center Berlin-Neukölln aufgrund einer Verwechslung die Zahlung an einen Empfänger von Arbeitslosengeld II, der im Verdacht stand, mit einer auf der „Terrorliste" aufgeführten Person identisch zu sein, für zwei Monate eingestellt. Besonders kritisch ist zu werten, dass gegen die Aufnahme in die Listen kein ausreichender Rechtsschutz besteht. Zwar kann beim VN-Sanktionsausschuss auf entsprechenden Antrag der betroffenen Person unter Einschaltung der nationalen Regierung eine Prüfung des Listeneintrages herbeigeführt werden. Unmittelbarer Rechtsschutz gegen Maßnahmen des VN-Sanktionsausschusses steht dem Betroffenen aber nicht zur Verfügung.

Vor dem Hintergrund dieser Defizite hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits am 16./17. März 2006 in einer Entschließung die Bundesregierung aufgefordert, bei den VN und der EU auf die Einhaltung der rechtsstaatlich gebotenen Standards zu dringen (abrufbar auf meiner Website unter www.bfdi.bund.de). Auch der EuGH hat sich mehrfach mit dem Listing-Verfahren befasst. Mit seinen Urteilen vom 12. Dezember 2006 (T-228/02) und vom 11. Juli 2007 (T-327/03) hat das Europäische Gericht erster Instanz die Aufnahme des Klägers in die vom Rat erstellten Listen jeweils für nichtig erklärt. Auch das jüngste Grundsatzurteil des EuGH vom 3. September 2008 (C-402/05P und C-415/05P) kommt zu dem Ergebnis, dass die EG-Verordnungen, mit denen die VN-Liste in EU-Recht überführt werden, wegen Verstoßes gegen das Grundrecht auf effektiven gerichtlichen Rechtsschutz und das Grundrecht auf Eigentum nichtig seien. Nach seiner Auffassung müsse die Aufnahme von Personen und Organisationen in die „Terrorlisten" der EU begründet und die Begründung den Betroffenen mitgeteilt werden. Nur so könnten diese in die Lage versetzt werden, darüber zu entscheiden, ob sie gerichtlichen Rechtsschutz gegen den Listeneintrag in Anspruch nehmen wollen.

Ich begrüße es, dass auf EU-Ebene ein Verfahren verabschiedet wurde, wonach gelistete Personen über die Aufnahme in die Listen informiert werden müssen, ihnen auf Antrag die Gründe für das Listing mitzuteilen sind und ihnen die Möglichkeit eingeräumt werden muss, dem Rat Unterlagen zu ihrer Entlastung vorzulegen.

Im Hinblick auf das o. a. Urteil des EuGH vom 3. September 2008 dürften diese Maßnahmen jedoch nicht ausreichen. Für einen derartigen Eingriff in die Persönlichkeitsrechte bedarf es einer speziellen, besonders begründeten und hinreichend normenklaren Rechtsgrundlage, die den vom EuGH unterstrichenen rechtsstaatlichen Anforderungen umfassend Rechnung trägt.

13.7 Datenübermittlungen des Bundeskriminalamtes an Behörden der Russischen Föderation

Bei der Übermittlung personenbezogener Daten im polizeilichen Nachrichtenaustausch mit öffentlichen Stellen der Russischen Föderation und den damit zusammenhän-

genden Dokumentationspflichten beim Bundeskriminalamt (BKA) habe ich einzelne Mängel festgestellt.

Im Rahmen eines datenschutzrechtlichen Kontroll- und Beratungsbesuches habe ich die Übermittlung personenbezogener Daten an Behörden der Russischen Föderation überprüft. Als Prüfungsmaßstab habe ich dabei den Rechtsrahmen zugrunde gelegt, der durch § 14 Bundeskriminalamtsgesetz (BKAG) sowie durch das deutsch-russische Regierungsabkommen über Zusammenarbeit bei der Bekämpfung von Straftaten von erheblicher Bedeutung vom 3. Mai 1999 (BGBl. II 2004 S. 861) vorgegeben wird.

Die Prüfung hat Zweifel daran entstehen lassen, inwieweit das BKA die nach Maßgabe des § 14 Absatz 7 BKAG vorzunehmende Prüfung der Zulässigkeit von Datenübermittlungen an Drittstaaten im Zusammenhang mit dem Datenaustausch mit russischen Stellen sachgerecht durchgeführt hat. Gemäß § 14 Absatz 7 Satz 7 BKAG hat eine Datenübermittlung zu unterbleiben, wenn durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt werden, insbesondere weil im Empfängerland ein angemessener Datenschutzstandard nicht gewährleistet ist. Dies setzt voraus, dass neben Angaben, die eine Einschätzung der Interessenlage des jeweiligen Betroffenen erlauben, auch Erkenntnisse über das in dem betreffenden Drittstaat bestehende Datenschutzniveau vorliegen. Entsprechende Informationen fehlten dem BKA aber bezüglich der Russischen Föderation. Auch der mir übergebene Länderbericht zu Russland enthielt keine entsprechenden Angaben. Dies halte ich für ein Manko, vor allem im Hinblick darauf, dass der Gesetzgeber das Fehlen eines angemessenen Datenschutzniveaus im Empfängerland als Ausschlussgrund für eine Datenübermittlung besonders herausgehoben hat. Ich halte es daher für geboten, dass bei allen Polizeibehörden des Bundes – nach dem Bundespolizeigesetz (BPolG) und dem Zollfahndungsdienstgesetz (ZFdG) gelten vergleichbare Regelungen – Erkenntnisse zum Datenschutzniveau des Drittstaates vorliegen, an den polizeiliche Daten übermittelt werden sollen.

Bei meinem Kontrollbesuch stellte sich auch heraus, dass die jeweilige Datenübermittlung zwar im jeweiligen Vorgang im Zusammenhang mit der laufenden Sachbearbeitung vermerkt wird. Dies wird aber der Aufzeichnungspflicht (§ 14 Absatz 7 Satz 3 BKAG) nicht gerecht. Sie stellt eine zusätzliche Verfahrenssicherung bei Datenübermittlungen an öffentliche und nicht-öffentliche Stellen in Drittstaaten dar und dient vor allem der datenschutzrechtlichen Eigen- und Fremdkontrolle. Vor diesem Hintergrund halte ich es für angebraucht, die Aufzeichnungen über Datenübermittlungen an Drittstaaten gesondert zu führen und aufzubewahren – wie dies auch gemäß § 33 Absatz 2 BPolG vorgesehen ist –, um die betreffenden zugrunde liegenden Vorgänge in angemessener Zeit sachgerecht unter datenschutzrechtlichen Gesichtspunkten überprüfen zu können.

Für problematisch halte ich zudem die im BKA geübte Praxis, die zu Erkenntnisanfragen von russischen Polizeidienststellen übermittelten personenbezogenen Daten unterschiedslos in der Datei „Kriminalaktennachweis – KAN“ zu speichern, versehen mit einer zehnjährigen Aussonderungsprüffrist. Besonders kritisch sehe ich diese Praxis bei Fällen, in denen aus der Erkenntnisanfrage der russischen Stellen keine Anhaltspunkte ersichtlich sind, dass sich die betreffende Person in Deutschland aufgehalten hat, bzw. dass deutschen Polizeidienststellen in irgendeiner Weise Erkenntnisse zu dieser Person vorliegen könnten, und in denen der Abgleich mit den beim BKA geführten Dateien folglich auch zu keinem Treffer führte. Auch halte ich die generelle Vergabe einer zehnjährigen Aussonderungsprüffrist, die sich offenbar ausschließlich an der Schwere der Straftat orientiert, die dem Betreffenden von den russischen Strafverfolgungsbehörden zur Last gelegt wird, nicht verhältnismäßig.

Bis Redaktionsschluss hat sich das BKA noch nicht abschließend zu den von mir aufgeworfenen Fragestellungen geäußert.

13.8 Die Europäische Frühjahrskonferenz

Die Konferenz der Datenschutzbeauftragten der Europäischen Union befasste sich vor allem mit Überlegungen zum Datenschutz in der Dritten Säule sowie mit neuen Herausforderungen angesichts weiterer Überwachungsmöglichkeiten von Reisenden.

Die Frühjahrskonferenz der europäischen Datenschutzbehörden vom 9. bis 11. Mai 2007 in Larnaka/Zypern behandelte schwerpunktmäßig aktuelle Probleme der sog. Dritten Säule des Vertrages über die Europäische Union. Zur Anwendung des Verfügbarkeitsprinzips bei der Strafverfolgung betonte die Konferenz die Notwendigkeit der Schaffung eines umfassenden Rahmens zur Beurteilung der datenschutzrechtlichen Aspekte in Zusammenhang mit der Nutzung dieses Prinzips. Kommission, Rat und Europäisches Parlament werden aufgefordert, alle Vorschläge zur Verfügbarkeit personenbezogener Daten kritisch zu überprüfen. Verfügbarkeitsgrundsatz und Datenschutz in der Dritten Säule sind auch Gegenstand der „Erklärung von Zypern“ (s. Anlage 9; s. o. Nr. 13.3.1). Schließlich richtete die Konferenz die Arbeitsgruppe Polizei und Justiz (Working Party Police and Justice (WPPJ)) ein (s. o. Nr. 13.3.8).

Auch die Frühjahrskonferenz vom 16. bis 18. April 2008 in Rom befasste sich eingehend mit der polizeilichen und justiziellen Zusammenarbeit in Europa sowie mit verschiedenen Initiativen der Europäischen Kommission zur verbesserten Kontrolle von Personen, die in das Schengen-Gebiet ein- oder ausreisen wollen (sog. Border Management). In ihrer „Erklärung von Rom“ (s. Anlage 10) warnt die Konferenz vor unverhältnismäßigen Eingriffen und spricht sich für eine klare Zweckbindung der bei Grenzkontrollen erhobenen Daten aus. Kritisch wird auch das zugrunde liegende Konzept beurteilt, Reisenden zu misstrauen, indem man ausgewählte „vertrauenswürdige“ Reisende von den anderen separiert (s. o. Nr. 13.3.7), weil eine derartige Praxis letztlich eine Diskriminierung der auf Grund intransparenter Kriterien als nicht vertrauenswürdig eingeschätzten Personen darstellt.

13.9 Die Internationale Datenschutzkonferenz

Die Internationale Datenschutzkonferenz hat auch im Berichtszeitraum wichtige Entschließungen zu aktuellen datenschutzpolitischen und datenschutzrechtlichen Fragestellungen angenommen.

Die **29. Internationale Datenschutzkonferenz** fand vom 25. bis 28. September 2007 in Montreal, Kanada, unter dem Thema „Privacy Horizons – Terra Incognita“ statt. Neben den unabhängigen Datenschutzbehörden umfasste der Teilnehmerkreis auch Staaten ohne unabhängige Datenschutzkontrollorgane, internationale Organisationen, Nichtregierungsorganisationen sowie Vertreter aus Wissenschaft und Industrie. Angesichts des zunehmenden Zugriffs auf Passagierdaten von Regierungsstellen zu Zwecken der Justizverwaltung und des Grenzschutzes forderte die Konferenz in einer Entschließung zum Schutz von Passagierdaten die Vereinbarung verbindlicher globaler Standards (s. Anlage 6; Kasten b zu Nr. 13.5.1). Die Konferenz betonte in einer weiteren Entschließung über die Entwicklung internationaler Standards die Notwendigkeit effektiver, universal akzeptierter internationaler Datenschutzstandards für die Anwendung und den Einsatz neuer und bestehender Technologien und sprach sich zu diesem Zweck für eine enge Zusammenarbeit mit der Internationalen Organisation für Normung (ISO) aus.

Die 30. Internationale Datenschutzkonferenz wurde vom 15. bis 17. Oktober 2008 vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gemeinsam mit der französischen Datenschutzbehörde, der Commission Nationale de l’Informatique et des Libertés (CNIL), in Straßburg ausgerichtet (s. a. u. Nr. 15.7). Unter dem Motto „Der Schutz der Privatsphäre in einer Welt ohne Grenzen“ diskutierten ca. 600 Teilnehmer aus 53 Staaten die technologischen, politischen und rechtlichen Herausforderungen an den Datenschutz. Da Nutzer sozialer Netzwerke sich häufig nicht der drohenden Schäden bewusst sind, die aus der umfassenden Verbreitung ihrer eigenen Daten und der Daten Dritter im Internet resultieren können, betonte die Konferenz in einer Entschließung die besondere Verantwortung der Anbieter sozialer Netzwerke. Die Anbieter werden aufgefordert, die Nutzer besser zu informieren, indem sie einerseits Anleitungen zur Nutzung personenbezogener Daten geben und andererseits den Zugang zu vollständigen Nutzerprofilen einschränken (s. Anlage 7, s. a. o. Nr. 7.3). In einer Entschließung zum Schutz der Privatsphäre von Kindern im Internet forderte die Konferenz die Betreiber von Websites auf, ihre Datenschutzpolitik den besonderen Bedürfnissen von Kindern anzupassen. Darüber hinaus sollten die nationalen Gesetzgeber die Sammlung, Verwendung und Mitteilung personenbezogener Daten von Kindern einschränken sowie geeignete Bestimmungen für den Fall von Verstößen treffen (s. Anlage 8). Die Konferenz erneuerte durch die Annahme der „Entschließung zur Erarbeitung internationaler Standards zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten“ ihren bereits im Jahre 2005 in der sog. Erklärung von Montreux formulierten Appell, ein rechtlich bindendes, universelles Rechtsinstrument auszuarbeiten (s. o. Nr. 13.1). Bis zur 31. Internationalen Datenschutzkonferenz, die im Herbst 2009 in Madrid stattfindet, soll eine Arbeitsgruppe einen gemeinsamen Vorschlag zur Erstellung internationaler Normen zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten vorlegen. Mit dem Ziel der Förderung des weltweiten Datenschutzbewusstseins soll die Einrichtung eines Internationalen Tages oder einer Woche für den Schutz der Privatsphäre durch eine Arbeitsgruppe untersucht werden.

14 Andere Bereiche

14.1 Übermittlung von Gesundheitsdaten an Versicherungen

Auskünfte aus der Gesundheitsakte von Wehrpflichtigen und Berufssoldaten an externe Stellen dürfen nur bei Vorliegen einer differenzierten Schweigepflichtentbindungserklärung erteilt werden.

Versicherungen und auch öffentliche Arbeitgeber verlangen im Rahmen von Risiko- und Leistungsprüfungen in der Regel Schweigepflichtentbindungserklärungen, um von behandelnden Ärzten und anderen maßgeblichen Stellen Auskünfte zur Gesundheit der Betroffenen zu erlangen.

Viele Soldaten wissen nicht, dass im Institut für Wehrmedizinalstatistik und Berichtswesen der Bundeswehr in Andernach Gesundheitsdaten über die Dienst- und Verwendungsfähigkeit von Soldaten lange Zeit zentral aufbewahrt werden, nämlich bei Wehrpflichtigen bis zur Beendigung der Wehrpflicht, also bis zur Vollendung des 45. bzw. 60. Lebensjahres (§ 3 Absatz 3 bis 4 Wehrpflichtgesetz (WPflG)), für Berufssoldaten und ehemalige Soldaten sogar bis zum Ablauf des 90. Lebensjahres (§ 29 Absatz 9 Soldatengesetz (SG) i. V. m. § 5 Absatz 3 Satz 3 der Rechtsverordnung über die Führung der Personalakten vom 31. August 1995 (BGBl. I 1995, 1159)).

§ 29 Absatz 4 SG schließt grundsätzlich die Weitergabe dieser sensiblen Gesundheitsdaten an Stellen außerhalb des Geschäftsbereichs des Bundesministeriums der Verteidigung aus. Sie ist nur möglich, wenn der Betroffene selbst eine entsprechende Schweigepflichtentbindungserklärung erteilt. An die Wirksamkeit einer solchen Erklärung sind aber strenge Maßstäbe anzulegen.

Wie ich aus Eingaben weiß, war vielen Soldaten, insbesondere Wehrpflichtigen, aufgrund der oftmals pauschalen Formulierung nicht bewusst, dass die Versicherungen hierdurch auch Auskunft über ihre in Andernach gespeicherten Gesundheitsdaten erhalten haben, ebenso, dass diese Daten überhaupt derart lange gespeichert sind.

Diese Praxis der Auskunftserteilung widerspricht dem Beschluss des Bundesverfassungsgerichts vom 23. Oktober 2006 (1 BvR 2027/02), demzufolge eine formularmäßige und zum Teil sehr allgemein umschriebene Erklärung das Interesse des Betroffenen an einem wirksamen informationellen Selbstschutz erheblich beeinträchtigt (vgl. 21. TB Nr. 9.6).

Das BMVg hat ein neues Formular einer Schweigepflichtentbindungserklärung nach den Vorgaben des Gerichts erstellt. Das Institut in Andernach erteilt inzwischen nur noch Auskünfte bei Verwendung dieses Formulars. Die neue Praxis ist datenschutzrechtlich nicht zu beanstanden.

14.2 Unzureichender Datenschutz in einer Auslandsvertretung

Die Prüfung einer Botschaft im Frühjahr 2008 machte eine Reihe von erheblichen Defiziten deutlich und führte zu Beanstandungen.

Im 20. TB (Nr. 23.1 und 23.2) hatte ich über Mängel bei der Aktenführung in einer Botschaft und Probleme bei der Wahrung der Diskretion in Auslandsvertretungen berichtet. Die vor diesem Hintergrund erfolgte eingehende Prüfung einer Botschaft im Berichtszeitraum erbrachte eine Reihe datenschutzrechtlich kritischer Feststellungen und führte zu einigen Beanstandungen. Das Auswärtige Amt hat hierauf rasch reagiert und ist in den meisten Punkten meinen Anregungen bereits gefolgt.

Der mit meiner Unterstützung 2002 in Kraft getretene „Runderlass Datenschutz“ (s. 20. TB Nr. 23.1) regelt für alle Auslandsvertretungen die Umsetzung einschlägiger datenschutzrechtlicher Vorgaben, etwa des BDSG. Leider zeigte die Kontrolle, dass die konkrete Umsetzung vor Ort unzureichend war:

– Entgegen dem deutlichen Wortlaut des Runderlasses war der Kanzler der Botschaft zugleich behördlicher Datenschutzbeauftragter. Da der Kanzler auch Personalangelegenheiten wahrnimmt, sind damit erhebliche Interessenkonflikte vorprogrammiert. Die Verantwortung für die Verarbeitung sensibler personenbezogener Daten (vor allem Personaldaten) ist daher von einer datenschutzrechtlichen Zuständigkeit organisatorisch und personell zu trennen.

  Ich habe die Beauftragung des Kanzlers mit dem Amt des behördlichen Datenschutzbeauftragten als Verstoß gegen § 4f Absatz 2 Satz 1 BDSG und damit erheblichen Mangel beanstandet und das AA gebeten, alle Auslandsvertretungen in diesem Sinne zu überprüfen. Das AA hat inzwischen einen neuen Datenschutzbeauftragten in der geprüften Botschaft ernannt und überdies im Hinblick auf die Größe der Botschaft auf meine Anregung hin auch einen Stellvertreter.

– Eine weitere Beanstandung habe ich im Hinblick auf die mangelnde Führung des Verzeichnisses der Datenverarbeitungsanlagen ausgesprochen. Hier ist das AA aufgefordert, die gesetzlichen Vorgaben in allen Auslandsvertretungen datenschutzgerecht umzusetzen, um den behördlichen Datenschutzbeauftragten einen Überblick über die Verarbeitung personenbezogener Daten in der Dienststelle zu geben. Auch der Runderlass weist ausdrücklich auf § 18 Absatz 2 Satz 1 BDSG hin.

  Nach § 18 Absatz 2 Satz 2 BDSG haben öffentliche Stellen für ihre automatisierten Verarbeitungen die Angaben nach § 4e BDSG z. B. die Zweckbestimmung der Datenerhebung und -verwendung, sowie die Rechtsgrundlage der Verarbeitung schriftlich festzulegen. Da dies in der Botschaft nicht erfolgt war, habe ich auch hier eine Beanstandung ausgesprochen. Das AA ist nun dabei, das vom Bundesministerium der Finanzen unter meiner Beteiligung hierfür entwickelte Verfahren DATSCHA (Datenschutzanwendung in der Bundesfinanzverwaltung) in den Auslandsvertretungen zu nutzen.

  Das AA hat zugesagt, die Umsetzung des Runderlasses ab sofort intensiv zu überprüfen und entsprechende Schulungen in den Auslandsvertretungen durchzuführen. Ich werde diese Maßnahmen aufmerksam begleiten.

– Das Problem der Wahrung der Diskretion bei der mündlichen Darstellung von Sachverhalten durch betroffene Antragsteller ist, obwohl vom AA zugesagt (s. 20. TB Nr. 23.2), nach wie vor nicht gelöst. In der geprüften Botschaft sind sowohl in der Visa-Stelle als auch in der Botschaftszentrale Räume mit mehreren Schaltern eingerichtet, die den Besuchern gleichzeitig als Warteräume dienen. Umstehende sind in der Lage, den Gesprächen, die entweder über Telefonhörer oder Mikrofone geführt wurden, zu beträchtlichen Teilen zu folgen. Selbst bei vorhandenen Diskretionsräumen, auf die im Übrigen nicht hingewiesen wurde, waren zumindest in der Nähe der Türen die Gespräche mitzuhören.

  Von einer Beanstandung habe ich abgesehen, um dem AA die Gelegenheit zu geben, eine Bestandsaufnahme in allen Auslandsvertretungen mit dem Ziel durchzuführen, vorhandene Mängel, wenn dies wirtschaftlich vertretbar ist, abzustellen. Jedenfalls sind Hinweisschilder anzubringen, die deutlich auf die Möglichkeit der diskreten Behandlung einer Angelegenheit in einem separaten Raum hinweisen.

15 Aus meiner Dienststelle

15.1 Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Viele Datenschutzthemen berühren den Bund und die Länder gleichermaßen. Umso wichtiger ist es, dass die unabhängigen Datenschutzbeauftragten des Bundes und der Länder mit einer Stimme reden. Das wichtigste deutsche Koordinationsgremium für Datenschutzangelegenheiten ist die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die zweimal jährlich tagt.

Im Jahr 2008 habe ich den Vorsitz vom Thüringer Landesbeauftragten für den Datenschutz übernommen. Am 3. und 4. April 2008 habe ich meine Länderkolleginnen und Länderkollegen nach Berlin in das Pergamonmuseum eingeladen. Die Herbstsitzung fand am 6. und 7. November 2008 im Bonner Haus der Geschichte statt. Über die Ergebnisse dieser Sitzungen, aber auch derjenigen aus 2007 habe ich bereits in den vorangegangenen Kapiteln an verschiedenen Stellen berichtet. Eine Auswahl der von der Konferenz gefassten Entschließungen ist in diesem Bericht abgedruckt. Sämtliche Entschließungen

sind zudem über meinen Internet-Auftritt unter www.bfdi.bund.de abrufbar.

15.2 Europäischer Datenschutztag

Zahlreiche Aktivitäten anlässlich des vom Europarat im Jahr 2007 ausgerufenen Europäischen Datenschutztages

Der Europarat hat im Jahr 2007 den Ersten Europäischen Datenschutztag ausgerufen. Dieser Tag soll dazu beitragen, das Bewusstsein für den Datenschutz bei den Bürgerinnen und Bürgern in Europa zu erhöhen. Der Europäische Datenschutztag findet jährlich am 28. Januar statt, weil an diesem Datum im Jahr 1981 die Europaratskonvention 108 zum Datenschutz erstmals unterzeichnet wurde. Alle mit dem Datenschutz befassten Stellen in Europa sind aufgerufen, sich durch Aktionen an diesem Tag zu beteiligen und die im Interesse des Schutzes der Privatsphäre notwendigen Grenzen darzustellen.

Aus Anlass des Ersten Europäischen Datenschutztages haben die Datenschutzbeauftragten des Bundes und der Länder neben eigenen dezentralen Aktionen am 29. Januar 2007 in Berlin gemeinsam eine zentrale Veranstaltung durchgeführt. Mit Blick darauf, dass die Innere Sicherheit zu diesem Zeitpunkt ganz oben auf der politischen Agenda stand, lautete das Thema der Veranstaltung „Die Balance zwischen Freiheit und Sicherheit – Wie schützt der Staat die Freiheit?“. Die Veranstaltung sollte die Gefahren ausufernder Datenverarbeitungen zu Sicherheitszwecken beleuchten und an die Verantwortlichen in der Politik appellieren, die Balance zwischen Freiheit und Sicherheit nicht noch stärker aus dem Gleichgewicht geraten zu lassen. Nachdem zunächst Bundesinnenminister Dr. Schäuble und Professor Dr. Simitis in Eingangsreferaten ihre unterschiedlichen Standpunkte vorgetragen hatten, ging es in der anschließenden Podiumsdiskussion um die Frage, ob angesichts immer neuer Überwachungsinstrumente die Freiheiten der Bürgerinnen und Bürger durch den Staat noch ausreichend geschützt sind.

Beim Zweiten Europäischen Datenschutztag im Jahr 2008 hatte sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf das Schwerpunktthema Datenschutz im Leben von Schülern und Jugendlichen verständigt. Unter dem Motto „Datenschutz macht Schule“ fanden bundesweit dezentrale Veranstaltungen mit Schülerinnen und Schülern von unterschiedlichen Bildungseinrichtungen statt. Die dabei angesprochenen Themen reichten vom Datenschutz in sozialen Netzwerken, Datenschutz in der Telekommunikation bis zu datenschutzrechtlichen Fragen im Zusammenhang mit Bewerbungsverfahren.

Ich selbst habe zusammen mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit am 28. Januar 2008 eine Veranstaltung in der Robert-Jungk-Oberschule in Berlin zum Thema „Web 2.0 – Datenschutz 2.0“ durchgeführt. Dabei sollte vor allem Schülerinnen und Schülern, aber auch der interessierten Öffentlichkeit die wachsende Bedeutung des Datenschutzes im Zusammenhang mit sozialen Netzwerken verdeutlicht werden. Nachdem sich die Schülerinnen und Schüler zunächst in verschiedenen Arbeitsgruppen mit der Problematik befasst hatten, wurde das Thema anschließend noch in einer Podiumsdiskussion mit Teilnehmern aus den Bereichen Medien, Personalwirtschaft, Internet-Dienste und Datenschutzkontrolle behandelt.

Bei Redaktionsschluss waren die Planungen für die Gestaltung des Dritten Europäischen Datenschutztages am 28. Januar 2009 in vollem Gange. Als amtierender Vorsitzender der Konferenz der Datenschutzbeauftragten des Bundes und der Länder habe ich eine gemeinsame zentrale Veranstaltung in Berlin vorbereitet, in deren Mittelpunkt die Bedeutung des Beschäftigtendatenschutzes unter dem Titel: „Die ideale Angestellte, der genormte Arbeitnehmer. Wie viel darf mein Arbeitgeber über mich wissen?“ steht.

15.3 25 Jahre Volkszählungsurteil

Auch 25 Jahre nach seiner Verkündung ist das Volkszählungsurteil des Bundesverfassungsgerichts immer noch aktuell.

Am 15. Dezember 2008 jährte sich die Verkündung des so genannten Volkszählungsurteils des Bundesverfassungsgerichts zum 25. Mal. Mit dieser bedeutenden Entscheidung wurde das Grundrecht auf informationelle Selbstbestimmung als Ausfluss des allgemeinen Persönlichkeitsrechts und der Menschenwürde erstmals höchstrichterlich als Verfassungsrecht anerkannt und damit ein Meilenstein für den Datenschutz gesetzt. Das Urteil stellte den mit Abstand wichtigsten Beitrag der Rechtsprechung zum Datenschutz in Deutschland dar.

Die Datenschutzbeauftragten des Bundes und der Länder erinnerten mit einer gemeinsamen Veranstaltung an die 25. Wiederkehr der Geburtsstunde des Rechts auf informationelle Selbstbestimmung. Zusammen mit den Landesdatenschutzbeauftragten von Baden-Württemberg und Rheinland-Pfalz als Mitorganisatoren hatte ich für den 15. Dezember 2008 zu der Festveranstaltung „25 Jahre Volkszählungsurteil/Datenschutz – Durchstarten in die Zukunft“ in den Bürgersaal des Karlsruher Rathauses eingeladen. Neben einem Rückblick auf die letzten 25 Jahre sollte auch die Zukunft des Datenschutzes diskutiert werden. Nahezu 200 Gäste waren der Einladung gefolgt und hörten mit großem Interesse den Festvortrag des Präsidenten des Bundesverfassungsgerichts, Herrn Professor Dr. Papier (s. Kasten zu Nr. 15.3 mit einigen Kernaussagen aus seiner Rede). Als Zeitzeugen kamen der ehemalige Präsident des Bundesverfassungsgerichts, Herr Professor Dr. Benda, der persönlich als Vorsitzender des 1. Senats am Volkszählungsurteil mitgewirkt hatte, und Herr Professor Dr. Simitis als renommierter Datenschutzexperte und damaliger Hessischer Datenschutzbeauftragter zu Wort. Das Veranstaltungsprogramm sah ferner eine Podiumsdiskussion vor, an der Vertreter aus den Bereichen Politik, Wissenschaft und Gesellschaft, aber auch einer nichtstaatlichen Organisation beteiligt waren. Neben einer Retrospektive, die auch die Bürgerrechtsbewegung in der ehemaligen DDR und das Aufgreifen des Volkszählungsurteils in den neuen Bundesländern umfasste, wurden in der Diskussionsrunde vor allem die Perspektiven für den Datenschutz beleuchtet.

Kasten zu Nr. 15.3

Aus dem Festvortrag von Herrn Professor Dr. Papier anlässlich der Veranstaltung zum 25. Jahrestag der Verkündung des Volkszählungsurteils

… Die Privatisierung der Informationstechnologie hat im Zusammenwirken mit der Globalisierung die Zahl potentieller „Big Brother“ so unübersichtlich werden lassen, dass aus datenschutzrechtlicher Sicht anarchische Zustände eher zu drohen scheinen als ein totalitärer Überwachungsstaat. …

… Lassen Sie mich zu einer weiteren Entwicklungslinie kommen, die allerdings dem staatlichen Datenschutz zu widersprechen scheint: Sie beruht auf dem „Konzept der informierten Öffentlichkeit“. In Verfolgung dieses Konzepts wurde in den letzten Jahren mit der deutschen Arkantradition gebrochen, nach der Behördenakten – außer für die Beteiligten – grundsätzlich der Geheimhaltung unterlagen. Nun gibt es auf Bundes- oder Landesebene Gesetze, die jedermann den Zugang zu Umweltinformationen, zu gesundheitsbezogenen Verbraucherinformationen oder allgemein zu jeder amtlichen Information gewährleisten. … Das „Konzept der informierten Öffentlichkeit“ … zielt vielmehr darauf ab, die „res publica“ Wirklichkeit werden zu lassen, dass heißt, durch mehr Transparenz der Verwaltung und einen verbesserten Informationszugang der Bürger den demokratischen Meinungs- und Willensbildungsprozess zu stärken. Damit korrespondiert das Informationszugangsrecht für Jedermann – jedenfalls auf einer abstrakten Ebene – mit dem Recht auf informationelle Selbstbestimmung. Wie bereits erwähnt, hat ja gerade auch das „Volkszählungsurteil“ den Zusammenhang zwischen Datenschutz und Ausübung demokratischer Freiheitsrechte deutlich aufgezeigt. …

… Damit steht das Recht auf informationelle Selbstbestimmung im Vergleich zur Zeit des „Volkszählungsurteils“ vor neuen Herausforderungen. Sie haben ihren Grund allerdings nicht nur in der Art der drohenden Gefahren, sondern auch in den revolutionären Veränderungen der Informations- und Kommunikationstechnologie. Es ist dabei anzuerkennen, dass der Staat – schon um seiner grundrechtlichen Pflicht zum Schutz von Leib, Leben oder Freiheit zu genügen – diese technischen Veränderungen bei der Gefahrenbekämpfung und Verfolgung von Straftaten nicht unberücksichtigt lassen kann. Gleichwohl dürfen bei der Ausbalancierung von Freiheit und Sicherheit die Gewichte nicht grundlegend verschoben werden. …

… Zum 25. Jahrestag des „Volkszählungsurteils“ sorge ich mich jedenfalls mehr davor, dass wir uns zu einer privaten Überwachungsgesellschaft internationalen Ausmaßes verwandeln, und dies weitgehend auch noch völlig freiwillig. …

… Würden alle diese irgendwo auf der Welt über uns gespeicherten Informationen zusammengeführt, ließe sich sehr leicht ein „Persönlichkeitsprofil“ von jedem von uns erstellen. Dadurch würde der im „Volkszählungsurteil“ für unzulässig befundene „Super-Gau des Datenschutzes“ Wirklichkeit werden, allerdings herbeigeführt durch die Hände Privater. …

… Denn die genannten Grundrechte verpflichten den Staat, im Ausgleich mit konkurrierenden Freiheitsrechten ein angemessenes Schutzregime zu schaffen und durchzusetzen sowie sich auf internationaler Ebene für ein solches Regime einzusetzen. Dabei wird sich der Staat häufig nicht mit bloßen Selbstverpflichtungen Privater begnügen dürfen, sondern wird selbst eine verbindliche Ordnung konstituieren müssen, um der grundrechtlichen Werteordnung auch im Privatrechtsverkehr Geltung zu verschaffen. Die nun von der Bundesregierung geplante Einführung des Einwilligungsprinzips für den Datenhandel sowie eines – allerdings freiwilligen – Datenschutzauditverfahrens mit Gütesiegel scheinen daher nahezu geboten zu sein, um dem objektiven Gehalt des Rechts auf informationelle Selbstbestimmung endlich auch im privaten Bereich hinreichend Rechnung zu tragen.

15.4 Bad Godesberger Symposien zum Datenschutz in der Telekommunikation und im Internet

Die Reihe der Herbstsymposien des BfDI wurde fortgesetzt.

Die Funktion der Suchmaschinen als digitale Gatekeeper, also „Torhüter“ der digitalen Welt, und damit ihre zugangssteuernde und potentiell meinungslenkende Wirkung beleuchtete der Leipziger Medienwissenschaftler Professor Marcel Machill beim VIII. Symposium im November 2007. Für ein Impulsreferat zur Online-Durchsuchung konnte der frühere Bundesinnenminister Gerhard Rudolf Baum gewonnen werden, der vor dem Bundesverfassungsgericht erfolgreich die Regelung der Online-Durchsuchung im nordrhein-westfälischen Verfassungsschutzgesetz angegriffen und damit eine der grundlegenden Karlsruher Entscheidungen zur Fortbildung des Datenschutzrechtes angestoßen hat (s. hierzu u. a. Nr. 2.1, 4.1 ff.). Die Frage nach der verfassungsrechtlichen Entwicklung und der Herausbildung neuer Grundrechte griffen der Hessische Datenschutzbeauftragte Professor Michael Ronellenfitsch und Dr. Klaus Abmeier aus dem Bundesministerium der Justiz in ihren Referaten auf.

Ich habe beim VIII. Symposium auf die Bedrohung der Privatsphäre hingewiesen, die exemplarisch durch die Ausweitung der Telekommunikationsüberwachung, die

Online-Durchsuchung und die Vorratsdatenspeicherung belegt wird. Die Privatsphäre ist heute im Kern bedroht. Effektive Gegenstrategien müssen deshalb bei der Technologie, aber auch bei rechtlichen, politischen und wirtschaftlichen Steuerungsmöglichkeiten ansetzen. Im Ergebnis geht es dabei auch um die Entwicklung einer globalen Ethik des Informationszeitalters, in deren Mittelpunkt die Bewahrung und Entwicklung der individuellen Selbstbestimmung steht.

Das IX. Symposium im November 2008 befasste sich u. a. mit der Marktentwicklung vor dem Hintergrund der Revision der europarechtlichen Vorgaben zum Telekommunikationsrecht sowie Fragen des Datenschutzes und der Kundenakquise im Mobilfunk.

Ich habe die Überlegungen der Europäischen Kommission begrüßt, mit der Novellierung der E-Privacy-Richtlinie eine Informationspflicht der Telekommunikationsunternehmen zu schweren Datenschutzverstößen einzuführen (vgl. Nr. 7.12). Damit erhalten die Betroffenen die Chance, schadensbegrenzende Maßnahmen zu treffen. Ferner kann eine solche Informationspflicht auch die Einstellung zum Datenschutz positiv verändern. Mit der Informationspflicht wird das Unternehmen gezwungen, die Verantwortung dafür zu übernehmen, wenn in seinem Verantwortungsbereich etwas schief gegangen ist. Die Informationspflicht wird die datenschutzrechtliche Sensibilität in den Unternehmen und damit auch die Anstrengungen stärken, durch Optimierung von Datenschutz und Datensicherheit „Pannen“ und Datenmissbrauch gar nicht erst entstehen zu lassen.

15.5 Zusammenarbeit mit den behördlichen Datenschutzbeauftragten

Der von mir initiierte regelmäßige Erfahrungsaustausch mit den behördlichen Datenschutzbeauftragten der obersten Bundesbehörden liefert wichtige Anregungen

Der von mir vor einigen Jahren initiierte Erfahrungsaustausch mit den Datenschutzbeauftragten der obersten Bundesbehörden ist inzwischen zu einer festen Institution geworden. Er bietet die Möglichkeit zur Information über datenschutzrechtliche Entwicklungen, zur Erörterung gemeinsamer Probleme sowie zur Diskussion offener Rechtsfragen und dient damit der Unterstützung der Datenschutzbeauftragten bei ihrer verantwortungsvollen Aufgabe. Auch im Berichtszeitraum wurde der Erfahrungsaustausch, an dem unverändert großes Interesse besteht, fortgesetzt.

Neben einer ausführlichen Unterrichtung über aktuelle Entwicklungen im Datenschutzrecht, insbesondere über BDSG-Änderungen, neue Gesetzentwürfe sowie Gerichtsentscheidungen und ihre Auswirkungen war die Situation der behördlichen Datenschutzbeauftragten in ihren jeweiligen Dienststellen ein Schwerpunkt. Dabei wurden Erfahrungen zum Arbeitsanfall bzw. zum Umfang der Freistellung sowie der Unterstützung durch weitere Mitarbeiterinnen und Mitarbeiter ausgetauscht. Die behördlichen Datenschutzbeauftragten berichteten über eine allgemein zufrieden stellende Situation, auch wenn in Einzelfällen der Eindruck entstanden sei, dass infolge von Einsparungen im Personalhaushalt Belange des Datenschutzes bisweilen nicht ausreichend berücksichtigt würden. Aus der Tatsache, dass es nur vereinzelt zu Problemen bei der Freistellung der behördlichen Datenschutzbeauftragten gekommen ist, kann geschlossen werden, dass zumindest die obersten Bundesbehörden der von der Bundesregierung anerkannten Pflicht zur teilweisen oder völligen Freistellung von anderen Aufgaben (vgl. 20. TB Nr. 2.4; 21. TB Nr. 2.6) gerecht werden.

Erörtert wurden auch die organisatorische Zuordnung in der jeweiligen Dienststelle und Fragen der Kompatibilität der Funktion als Beauftragter für den Datenschutz mit gleichzeitig übertragenen anderen Aufgaben. Beim Thema Datensicherheit standen das neue Datenschutzkapitel im IT-Grundschutz-Katalog des Bundesamts für Sicherheit in der Informationstechnik sowie Fragen des datenschutzgerechten Löschens von Datenträgern im Vordergrund (vgl. 21. TB Nr. 4.8 sowie o. Nr. 8.3). Weitere wichtige Themen waren die Ausgestaltung eines Verfahrens zur Leistungsfeststellung im Rahmen des neuen Bundesbesoldungsgesetzes und rechtliche Fragen im Zusammenhang mit der Aufgabenverlagerung auf externe Stellen durch Outsourcing oder Auftragsdatenverarbeitung (vgl. 21. TB Nr. 2.5 sowie o. Nr. 2.5).

Ich werde die behördlichen Datenschutzbeauftragten in ihrer wichtigen Funktion bei der Verwirklichung des Datenschutzes in ihrer Dienststelle auch weiterhin aktiv unterstützen, sowohl durch Beratungen im Einzelfall als auch durch Fortsetzung des regelmäßigen Erfahrungsaustausches.

15.6 Zusammenarbeit mit den Aufsichtsbehörden

Die wachsenden Herausforderungen an den Datenschutz und das komplexe Datenschutzrecht machen den Austausch von Informationen und die Abstimmung von rechtlichen Bewertungen zwischen den Aufsichtsbehörden immer wichtiger.

Über die vielgestaltige Datenschutzaufsicht in Deutschland und die daraus folgenden Konsequenzen habe ich bereits mehrfach berichtet (vgl. 21. TB Nr. 2.2). Die Zusammenarbeit der verschiedenen Aufsichtsbehörden wird immer wichtiger, weil diese oft vor den gleichen Rechtsproblemen stehen oder bestimmte Sachverhalte die Zuständigkeit verschiedener Aufsichtsbehörden betreffen. Dies war zum Beispiel bei der Mitarbeiterüberwachung durch die Firma Lidl der Fall (vgl. hierzu auch unter Nr. 11.1). Für eine wirksame und überzeugende Datenschutzaufsicht ist es deswegen unerlässlich, dass nicht nur Informationen zügig ausgetauscht, sondern auch rechtliche Fragestellungen möglichst gemeinsam bewertet werden und – soweit erforderlich – auch eine Absprache über ein gemeinsames Vorgehen erfolgt. Diese Aufgabe fällt für den nicht-öffentlichen Bereich dem sog. Düsseldorfer Kreis und seinen Arbeitsgruppen zu, in denen ich neben den Aufsichtsbehörden der Länder vertreten bin (zur Konferenz der Datenschutzbeauftragten des Bundes und der Länder vgl. Nr. 15.1).

Der Düsseldorfer Kreis hat im Berichtszeitraum nicht nur zu den beiden Gesetzesvorhaben der Bundesregierung zur Änderung des BDSG Stellung genommen, sondern auch ein Positionspapier zum internationalen Datenverkehr und eine Handreichung zur rechtlichen Bewertung von Fallgruppen zur internationalen Auftragsdatenverarbeitung beschlossen (abrufbar auf meiner Website unter www.bfdi.bund.de). Daneben hat er eine Reihe weiterer wichtiger Beschlüsse gefasst (vgl. Kasten zu Nr. 15.6).

Kasten zu Nr. 15.6

Beschlüsse des Düsseldorfer Kreises in den Jahren 2007/2008:

- Erhebung von Positivdaten zu Privatpersonen bei Auskunfteien
- Mahnung durch Computeranruf
- Anwendbarkeit des Bundesdatenschutzgesetzes auf Rechtsanwälte
- Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring
- Internet-Portale zur Bewertung von Einzelpersonen
- Keine fortlaufenden Bonitätsauskünfte an den Versandhandel
- Datenschutzkonforme Gestaltung sozialer Netzwerke
- Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet
- Novellierung des Bundesdatenschutzgesetzes in den Bereichen Adresshandel, Werbung und Datenschutzaudit

abrufbar über meine Website unter www.bfdi.bund.de

15.7 Die Internationale Datenschutzkonferenz 2008

Vom 15. bis 17. Oktober 2008 richtete ich gemeinsam mit meinem französischen Kollegen (Commission Nationale de l'Informatique et des Libertés (CNIL)) die 30. Internationale Datenschutzkonferenz in Straßburg aus.

Unter dem Motto „Der Schutz der Privatsphäre in einer Welt ohne Grenzen" kamen vom 15. bis 17. Oktober 2008 Vertreter aus Wirtschaft, Politik und Wissenschaft mit den Datenschutzbeauftragten aus aller Welt im Gebäude des Europarats in Straßburg zusammen, um die technologischen, politischen und rechtlichen Herausforderungen an den Datenschutz zu diskutieren und Vorschläge zu beraten, wie ihnen angemessen begegnet werden kann (s. o. Nr. 13.9). Den festlichen Rahmen der Konferenz bildete ein Galadinner in Baden-Baden.

15.8 Öffentlichkeitsarbeit

Neue Informationsmaterialien und Gespräche vor Ort: Information und Beratung von Bürgerinnen und Bürgern

Der Stellenwert des Datenschutzes nimmt auf Grund immer umfassenderer Datensammlungen und der mit den technologischen Entwicklungen einhergehenden Risiken für die Privatsphäre stetig zu. Deshalb ist es natürlich, dass sich immer mehr Bürgerinnen und Bürger mit Fragen an mich wenden und um Empfehlungen bitten, wie Sie Ihre persönlichen Daten vor Missbrauch schützen können.

Sie nutzen verstärkt die Möglichkeit, sich auf meiner Website (www.bfdi.bund.de) zu informieren. Die Neugestaltung dieses Internet-Angebots ist gut angenommen worden. Das belegen die steigenden Nutzerzahlen (s. Kasten zu Nr. 15.8).

Auf der Startseite bekommt man schnell einen aktuellen Überblick über das Geschehen im Datenschutz. Besonders häufig wurden Seiten unter der Rubrik Öffentlichkeitsarbeit aufgerufen. Aktuelle Pressemitteilungen wurden auf diesem Wege schnell einer breiten Öffentlichkeit zugänglich gemacht.

Neben meinem Internet-Angebot stelle ich den anfragenden Bürgerinnen und Bürgern die Informationsschriften und Faltblätter selbstverständlich auch weiterhin in Papierform zur Verfügung.

Im Berichtszeitraum wurde eine neue Info 2 zum Informationsfreiheitsgesetz veröffentlicht. Diese Broschüre soll allen Interessierten die Möglichkeit geben, sich schnell und umfassend über ihre Rechte auf freien Zugang zu amtlichen Informationen öffentlicher Stellen zu informieren und diese zielgerichtet wahrzunehmen. Sie enthält neben Erläuterungen zum Informationsfreiheitsgesetz des Bundes und praktischen Tipps für die Antragstellung eine Zusammenstellung der Informationsfreiheitsgesetze des Bundes und – soweit vorhanden – der Länder, der entsprechenden Regelungen der Europäischen Union sowie weiterer damit in Zusammenhang stehender Rechtsvorschriften wie das Umweltinformationsgesetz und das Verbraucherinformationsgesetz.

Der Tagungsband zum Symposium „Biometrie und Datenschutz – Der vermessene Mensch" enthält die auf dem Symposium vom 27. Juni 2006 gehaltenen Vorträge und dokumentiert die anschließende Diskussion.

Daneben sind im Berichtszeitraum einige neue Arbeitshilfen zu technischen Themen erschienen, wie zum Protection Profile – Software zur Verarbeitung von personenbezogenen Bilddaten und datenschutzrechtliche Grundlagen bei der Auftragsdatenverarbeitung/Outsourcing in der öffentlichen Verwaltung.

Zudem wurden die Info 1 – Bundesdatenschutzgesetz – Text und Erläuterung – und Info 4 – Die Datenschutzbeauftragten in Behörde und Betrieb – aktualisiert.

Am Tag der offenen Tür der Bundesregierung war der BfDI wieder mit einem Informationsstand vertreten, um die Bürgerinnen und Bürger vor Ort über die Themen Datenschutz und Informationsfreiheit zu informieren und Fragen zu beantworten. Hier bestand die Gelegenheit, sowohl Besucherinnen und Besucher auf die Gefahren und Chancen bei der Datenverarbeitung hinzuweisen, sie auf ihre Rechte aufmerksam zu machen und für die Themen Datenschutz und Informationsfreiheit zu sensibilisieren, als auch Fragen zu beantworten und über aktuelle Frage-

stellungen mit den Besucherinnen und Besuchern zu diskutieren. Seit 2002 präsentiere ich meine Aufgaben und mein Tätigwerden am Tag der offenen Tür der Bundesregierung und jedes Jahr kommen mehr Bürgerinnen und Bürger gezielt an meinen Stand, um ihre Fragen zu stellen und ihre Anliegen vor Ort zu diskutieren.

Insbesondere trägt meine Pressestelle mit dazu bei, dass Ereignisse mit Datenschutzbezug meine Bewertung finden und über die Medien in die breite Öffentlichkeit getragen werden, um dort Beachtung zu finden. Dies geschieht u. a. durch Pressemitteilungen, die bei Bedarf herausgegeben werden und die oft auch nützliche Tipps für den täglichen Umgang mit Daten beinhalten.

Ohne die zahlreichen unmittelbaren Kontakte zu Pressevertretern aller Medien wäre die Sensibilisierung der Öffentlichkeit für das Thema „Datenschutz“ ein wesentlich schwierigeres Unterfangen. Ich lege daher großen Wert darauf, dass die Pressestelle den Vertreterinnen und Vertretern der Medien mit Rat und Tat zur Verfügung steht.

Ebenso tragen sicherlich meine Artikel, die ich zu verschiedenen Themenbereichen, wie z. B. der Videoüberwachung oder dem neuen BKA-Gesetz, für die Tagespresse und Fachpublikationen geschrieben habe, dazu bei, die Wahrnehmung des Datenschutzes in der Öffentlichkeit zu stärken.

Kasten zu Nr. 15.8

Nutzerzahlen der Internet-Seite www.bfdi.bund.de:

	2008	2007
Seitenaufrufe (gesehener Traffic)	3.847.543	2.353.119
Seitenaufrufe (nicht gesehener Traffic)*	3.528.632	3.926.474
Seitenaufrufe gesamt	7.376.175	6.279.593

* Nicht gesehener Traffic ist Traffic, welcher im Wesentlichen von Robots, insbesondere zur automatisierten Auswertung durch Suchmaschinen verursacht wurde.

15.9 Mehr Präsenz in der Bundeshauptstadt

Mein Verbindungsbüro in Berlin hat sich bereits nach kurzer Zeit bewährt.

Für eine verstärkte Präsenz meiner Dienststelle in Berlin wurde ein Verbindungsbüro eingerichtet, das seinen Betrieb Anfang 2008 aufgenommen hat. Seine Aufgaben bestehen in der Koordinierung und Wahrnehmung von Terminen, insbesondere in den Ausschüssen des Deutschen Bundestages sowie in den Sitzungen der Bundesressorts in Berlin. Dazu wurden keine neuen Planstellen bzw. Stellen geschaffen, vielmehr wurden bestimmte bislang in Bonn wahrgenommene Funktionen nach Berlin verlagert. Personell ist das in der Friedrichstraße 50 in Berlin-Mitte untergebrachte Verbindungsbüro zurzeit mit einem Leiter und sechs Mitarbeiterinnen bzw. Mitarbeitern ausgestattet.

Es kann festgehalten werden, dass sich das Verbindungsbüro hervorragend bewährt hat. Seit Inbetriebnahme konnten sehr viel mehr Termine in Berlin wahrgenommen werden als früher, wodurch eine wirkungsvollere und direktere Teilnahme am politischen Geschehen in der Bundeshauptstadt erreicht wird. Den Referaten konnten dadurch zeitaufwändige Dienstreisen zur Terminwahrnehmung erspart werden.

Es hat sich auch gezeigt, dass es dringend erforderlich ist, eine Vertretung aller Organisationseinheiten des BfDI in Berlin zu gewährleisten. Die noch nicht repräsentierten zwei Referate sind ebenfalls für Aufgabenbereiche zuständig, die zum politischen Kernbereich zählen. Zudem habe ich meinen persönlichen Dienstort mittlerweile nach Berlin verlagert.

15.10 BfDI als Ausbildungsbehörde

Referendare und Praktikanten

Auch in den letzten zwei Jahren war erneut großes Interesse an Praktikumsaufenthalten in meiner Dienststelle festzustellen. Insbesondere von Studierenden der Rechtswissenschaften und Rechtsreferendaren, die sich für Fragen des Datenschutzes und der Informationsfreiheit interessierten und praktische Kenntnisse erwerben wollten.

Insgesamt haben im Jahre 2007 und 2008 zehn Studierende und Referendare Teile ihrer Ausbildung in meinem Hause absolviert. Darüber hinaus konnte ich neun Anwärterinnen und Anwärtern des gehobenen Dienstes in der allgemeinen inneren Verwaltung die Möglichkeit bieten, ihr Pflichtpraktikum in meiner Dienststelle abzuleisten.

Angesichts der uneingeschränkt positiven Erfahrungen werde ich – trotz begrenzter räumlicher und personeller Kapazitäten – auch künftig alle Möglichkeiten nutzen, an der Ausbildung mitzuwirken.

15.11 Zusätzliches Personal dringend erforderlich

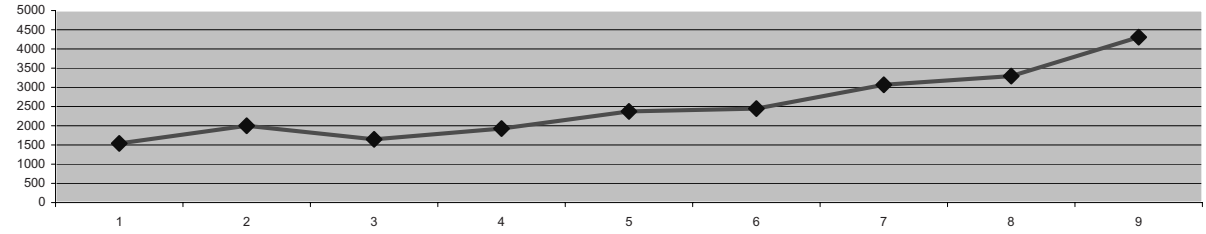
Gesetzliche Aufgaben können mit dem vorhandenen Personal nicht mehr angemessen und in vollem Umfang erledigt werden.

In meiner Dienststelle ist der Aufgaben- und Arbeitsanfall seit Jahren kontinuierlich stark angestiegen. Die personelle Ausstattung hat mit dieser Entwicklung nicht Schritt gehalten, so dass im Ergebnis die Zahl der Planstellen und Stellen, die für die Erledigung der gesetzlichen Aufgaben zur Verfügung stehen, inzwischen deutlich zu gering bemessen ist. 50 Planstellen und 17 Stellen für Tarifbeschäftigte stehen haushaltsmäßig meiner Dienststelle zur Verfügung. Hiermit sind rd. 20 Funktionen der Infrastrukturdienste (überwiegend einfacher und mittlerer Dienst) und der IT-Administration (in Zugleichfunktion mit Datenschutzaufgaben) stellenmäßig unterlegt. Obwohl sich die Zahl der Bürgereingaben wie auch das gesamte Dokumentenaufkommen in den zurückliegenden Jahren mehr als verdoppelt haben, muss dieser enorme Anstieg mit dem vorhandenen Personal bewältigt werden (s. Kasten zu Nr. 15.11).

Kasten zu Nr. 15.11

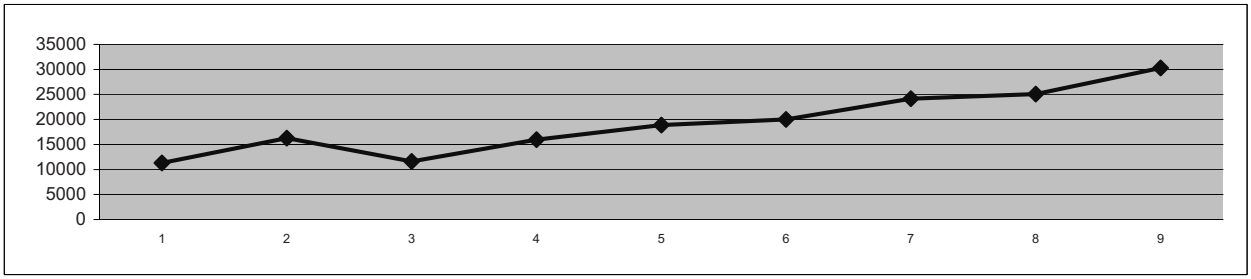
EINGABEN / PETITIONEN

Jahr	2000	2001	2002	2003	2004	2005	2006	2007	2008
Anzahl	1541	2000	1647	1927	2376	2449	3067	3295	4309



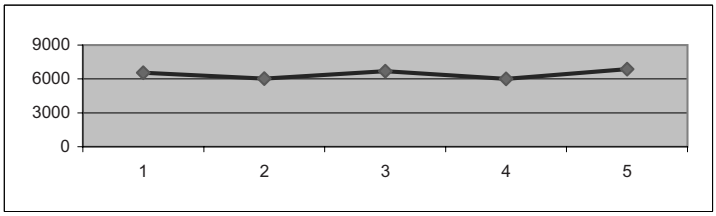
DOKUMENTENAUFKOMMEN (Eingänge, Ausgänge, Intern)

Jahr	2000	2001	2002	2003	2004	2005	2006	2007	2008
Anzahl	11320	16267	11594	15940	18876	20020	24132	25056	30303



TELEFONBERATUNGEN

Jahr					2004	2005	2006	2007	2008
Anzahl					6555	6031	6686	5997	6872



Durch die geschilderte Situation sind deutlich spürbare Engpässe und Verzögerungen bei der Wahrnehmung gesetzlicher Aufgaben im Datenschutz und auch im IFG-Bereich entstanden. Eine strikte Priorisierung hat dazu geführt, dass einzelne Bereiche zurzeit nicht angemessen „betreut“ werden können; ein Rückgang der Kontrolldichte ist die Folge. Dies kann – auch vor dem Hintergrund aktueller Ereignisse im Bereich des Datenschutzes und der ständig wachsenden Zahl datenschutzrelevanter IT-Verfahren – so nicht weiter hingenommen werden. Die Zahl und der Umfang datenschutzrechtlicher Prüfungen sind zu erweitern, damit Umsetzungsdefizite des Datenschutzrechts abgebaut und zunehmenden Risiken Rechnung getragen werden kann. Es darf dabei auch nicht außer Acht gelassen werden, dass die neue Qualität der Datenverarbeitung auf europäischer Ebene (Stichworte sind hier z. B. die Dienstleistungsrichtlinie, Nr. 3.4.1 und Schengen Nr. 13.3.4) zusätzliche Anforderungen an die datenschutzrechtliche Begleitung der Vorhaben und an die Kontrolle der Einhaltung gesetzlicher Vorgaben stellen.

Dienststelleninterne Maßnahmen konnten die Lage nur ansatzweise entspannen: So wurde z. B. ein Servicebüro eingerichtet, das den Referaten u. a. für die Bearbeitung von Eingaben unterstützend zur Verfügung steht und so zu einer Entlastung beiträgt. Zudem wurden im Rahmen der Optimierung der Ablauf- und Aufbauorganisation in der Dienststelle des BfDI und zur besseren Nutzung vorhandener Personalressourcen Organisationseinheiten umstrukturiert, Projektgruppen gebildet und ein Verbindungsbüro in Berlin eingerichtet (s. unter Nr. 15.9).

16 Wichtiges aus zurückliegenden Tätigkeitsberichten

1. 21. TB Nr. 7.1.1 zum **Gesetz zur Umsetzung aufenthalts- und asylrechtlicher Richtlinien der Europäischen Union**

   Das Gesetz ist nach intensiven Diskussionen am 28. August 2007 in weiten Teilen in Kraft getreten. Durch das Gesetz wird neben der Umsetzung von elf EU-Richtlinien in nationales Recht die Reform des Ausländerrechts weitergeführt. Meine Bedenken gegenüber den durch § 15 AZRG gewährten stufenlosen automatisierten Zugriffsmöglichkeiten von Polizeivollzugsbehörden und Staatsanwaltschaften auf das Ausländerzentralregister (AZR) wurden leider nicht berücksichtigt. Gleiches gilt für meine Kritik an der Speicherung von Lichtbildern Drittstaatsangehöriger und Staatsangehöriger der EU im allgemeinen Datenbestand des AZR gemäß § 3 Nr. 5° AZRG.

   Die bereits in meinem 20. TB (Nr. 6.1.4) dargelegten Zweifel an der Europarechtskonformität einer generellen Speicherung der Daten von Unionsbürgern im AZR wurden jedoch zwischenzeitlich vom EuGH bestätigt. Nach der Entscheidung vom 16. Dezember 2008 im Vorabentscheidungsverfahren (C-524/06) kann ein Register zur Unterstützung der mit der Anwendung aufenthaltsrechtlicher Vorschriften betrauten Stellen zwar durchaus erforderlich sein, die Speicherung und Verarbeitung der personenbezogenen Daten von Unionsbürgern, die sich in Deutschland aufhalten, rechtfertigen aber weder statistische Zwecke noch die Kriminalitätsbekämpfung. Ich habe das BMI dringend gebeten, die Daten der EU-Bürger für unzulässige Verwendungen wie die Bekanntgabe an Polizei und Justiz zu sperren und zu prüfen, ob sie gespeichert bleiben dürfen. Der Gesetzgeber ist aufgerufen, das AZRG entsprechend den Vorgaben des EuGH zu ändern.

2. 20. TB Nr. 6.2.3; 21. TB Nr. 7.1.4 zum **europäischen Visa-Informationssystem (VIS):**

   Im europäischen Visa-Informationssystem (VIS) sollen alphanumerische und biometrische Daten (Lichtbild, Fingerabdrücke) über Visa-Antragsteller gespeichert werden. Nunmehr stehen mit der formalen Verabschiedung der Verordnung (EG) Nr. 767/2008 vom 9. Juli 2008 (VIS-Verordnung) und dem Beschluss 2008/633/JI des Rates vom 23. Juni 2008 über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum VIS (VIS-Zugangsbeschluss) die rechtlichen Rahmenbedingungen fest. Zu begrüßen ist, dass die VIS-Daten gemäß Artikel 23 VIS-Verordnung nicht – wie von der Bundesregierung gewünscht – zehn, sondern lediglich fünf Jahre lang gespeichert werden sollen. Ergebnis eines Kompromisses zwischen Rat und Europäischem Parlament ist weiter, dass die nationalen Sicherheitsbehörden keinen Online-Zugriff auf das VIS erhalten, sondern ausschließlich über die nationalen Schnittstellen zugreifen dürfen (vgl. dazu Nr. 13.3.5).

   Da die Regelungen der VIS-Verordnung im Hinblick auf die sog. „Warndatei" nach Auffassung des BMI nicht weit genug reichen, wird derzeit auf nationaler Ebene an einer zusätzlichen „Einlader- und Warndatei" gearbeitet (vgl. Nr. 5.6). Das europäische VIS wird voraussichtlich im Jahr 2009 den Betrieb aufnehmen.

3. 21. TB Nr. 7.1.3 zur **Datenerhebung zu Forschungszwecken ohne Rechtsgrundlage:**

   Mittlerweile liegt der von mir angemahnte Entwurf des Gesetzes zur Verbesserung der Bekämpfung von Visumsmissbrauch und Schleusungskriminalität vor, in dessen Rahmen in § 24a AZRG-E die Verwendung personenbezogener Daten für wissenschaftliche Zwecke geregelt werden soll.

   Datenschutzrechtliche Bedenken bestehen hiergegen nicht. Daher hielt ich im Vorgriff auf diese Forschungsklausel es für vertretbar, das Projekt durchzuführen.

4. 16. TB Nr. 5.8 zum **Suchdienstedatenschutzgesetz (SDDSG):**

   Nachdem ich in der Vergangenheit mehrfach das Fehlen einer bereichsspezifischen Rechtsgrundlage für die Datenverarbeitung der nationalen Suchdienste bemängelt hatte, begrüße ich den sich nunmehr im Gesetzgebungsverfahren befindlichen Entwurf eines Suchdienstedatenschutzgesetzes (SDDSG), der die aufgezeigte Lücke schließt. Kritisch sehe ich jedoch den vorgesehenen Ausschluss des datenschutzrechtlichen Grundsatzes der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) im Hinblick auf seinen möglichen Präzedenzcharakter. Zwar sind die Suchdienste wegen der häufigen Namensgleichheiten zur Identitätsfindung auf eine Vielzahl von Daten angewiesen, einen Ausschluss der Anwendbarkeit des § 3a BDSG macht dies aber nicht zwingend notwendig. Das Gesetz war bei Redaktionsschluss noch nicht verabschiedet.

5. 21. TB Nr. 8.3 zum **Entwurf des Zweiten Gesetzes zur Änderung des Vierten Buches Sozialgesetzbuch und anderer Gesetze, wie z. B. des Schwarzarbeitsbekämpfungsgesetzes (SchwarzArbG):**

   Wie angekündigt, habe ich die Arbeit der Finanzkontrolle Schwarzarbeit (FKS) aufmerksam begleitet. So habe ich zum Entwurf des Zweiten Gesetzes zur Änderung des Vierten Buches Sozialgesetzbuch und anderer Gesetze, wie z. B. des Schwarzarbeitsbekämpfungsgesetzes (SchwarzArbG) Stellung genommen. Datenschutzrechtliche Bedenken gegen die in § 17 Absatz 1 Nummer 1 SchwarzArbG-E vorgesehene Erweiterung des Zugriffs der Polizeivollzugsbehörden des Bundes auf die zentrale Datenbank werden von mir nach ergänzenden Ausführungen in der Begründung zur Erforderlichkeit dieser Zugriffe nicht mehr geteilt. Dort wird u. a. ausgeführt, dass § 17 Absatz 1 Nr. 3 SchwarzArbG den Polizeibehörden

der Länder ein Auskunftsrecht aus der zentralen Datenbank einräumt. Daher sei es sachgerecht und erforderlich, auch der Bundespolizei und dem BKA in Anbetracht ihrer Zuständigkeit für die Bekämpfung der Schleusungskriminalität den Zugriff auf die Datenbank zu ermöglichen. Dem habe ich mich angeschlossen.

6. 20. TB Nr. 16.1.3; 21. TB Nr. 13.5.3 zum **Erhebungs- und Leistungssystems A2LL bei der BA:**

   Bereits mehrfach habe ich über die Einführung des Erhebungs- und Leistungssystems A2LL bei der BA berichtet. Die Implementierung eines Zugriffsberechtigungs- und Protokollierungskonzeptes für A2LL ist nunmehr erfolgt. Damit verfügt das für die Leistungsberechnung genutzte Programm A2LL über klar definierte, abgestufte Zugriffsberechtigungen, womit sichergestellt ist, dass die Mitarbeiterinnen und Mitarbeiter der BA nur auf die Daten zurückgreifen können, die für die jeweilige Sachbearbeitung erforderlich sind. Außerdem wird die bundesweite Nutzung auf den Datenbestand nun lückenlos protokolliert. Ich werde das Programm A2LL weiterhin im Blick behalten.

7. 21. TB Nr. 13.5.5 zur **unzulässigen Datensammlung der BA über die Nutzer der BA-Internet-Plattform:**

   Ich hatte bereits über eine unzulässige Datensammlung der BA über die Nutzer der BA-Internet-Plattform berichtet. An der von der BA geübten Praxis, bei Recherchen nach Stellenangeboten in den Internet-Centern der BA den Verlauf der jeweiligen Nutzung für den Zeitraum von 180 Tagen zu speichern, hatte ich die fehlende Unterrichtung des Nutzers über Umfang, Dauer und Zweck der Erhebung, Verarbeitung und Nutzung seiner Daten kritisiert. Die Speicherung dieser Daten ist nur mit schriftlicher Einwilligung zulässig. Dieser Auffassung ist die BA inzwischen gefolgt: Die Neufassung der Nutzerordnung enthält eine zukünftig zu verwendende ausdrückliche Einwilligungserklärung zur Erhebung der Nutzerdaten.

8. 21. TB Nr. 19.2 zum **Zentralen Vorsorgeregister bei der Bundesnotarkammer:**

   Bei meiner Überprüfung des Zentralen Vorsorgeregisters bei der Bundesnotarkammer habe ich bis auf einige wenige Hinweise in technisch-organisatorischer Hinsicht keine datenschutzrechtlichen Mängel festgestellt. Insbesondere hat sich bestätigt, dass die vorherige Einwilligung des Bevollmächtigten in die Speicherung der Daten zu seiner Person in der Praxis der Regelfall ist. Wichtig war mir auch die Feststellung, dass die Zweckbindung der Daten eingehalten wird. Sie dürfen ausschließlich im Rahmen von Betreuungsverfahren durch die zuständigen Gerichte genutzt werden.

9. 21. TB Nr. 15.1 zum **Online-Angebot „Öffentliche Petition“:**

   Ich habe über das Vorhaben des Petitionsausschusses des Deutschen Bundestages berichtet, Mechanismen zu erarbeiten, die verhindern, dass Diskutanten und Mitzeichner des Online-Angebots „Öffentliche Petition“ von Internet-Suchmaschinen erfasst werden. Dies ist seit dem Frühjahr 2007 umgesetzt.

   Den Mitzeichnungsseiten des Bereichs „Öffentliche Petition“ im Internet wurde hierzu ein Meta-Tag hinzugefügt, der die Auswertung der Mitzeichnerlisten durch Suchmaschinen verhindert. Darüber hinaus hat der Deutsche Bundestag eine neue datenschutzgerechte Version des Verfahrens „Öffentliche Petition“ entwickelt.

10. 21. TB Nr. 16.1 zum **Projekt HERKULES:**

    Mit dem Projekt HERKULES will das Bundesministerium der Verteidigung (BMVg) nahezu seine gesamte Informationstechnik outsourcen. Die technischen und organisatorischen Schutzmaßnahmen sollen im Datenschutzkonzept HERKULES und dem übergreifenden IT-Sicherheitskonzept HERKULES spezifiziert werden. Beides soll mir nach Fertigstellung zugeleitet werden.

    Das Verfahren werde ich weiterhin aufmerksam begleiten.

11. 21. TB Nr. 16.2 zur **Privatisierung der bundeseigenen Kleiderkasse:**

    Ich hatte darüber berichtet, dass bei der Privatisierung der bundeseigenen Kleiderkasse der Bundeswehr umfangreiche Datenbestände von aktiven und ehemaligen Bundeswehrangehörigen an die privatrechtlich organisierten Nachfolgegesellschaften übermittelt worden sind, ohne im Vorfeld die Erforderlichkeit hierfür sorgfältig zu prüfen. Die Daten waren dann zu Werbezwecken eingesetzt worden, wogegen sich Petenten gewandt hatten. Meiner Aufforderung, die Mängel im Umgang mit den Kundendaten der ehemaligen Kleiderkasse zu beheben, ist das BMVg durch die Erstellung eines Datenschutzkonzeptes, was sich derzeit noch in der Prüfung befindet, nachgekommen.

12. 21. TB Nr. 17.2 zum **Vertragslosen Zustellungsverkehr:**

    Ich hatte dargelegt, dass die „offene“ Zusendung amtlicher Schriftstücke im Rahmen des Vertragslosen Zustellungsverkehrs mit dem Ausland in das Recht auf informationelle Selbstbestimmung der Betroffenen eingreift und deshalb einer gesetzlichen Grundlage bedarf. Leider gibt es hier trotz des mittlerweile mit dem BMJ erzielten grundsätzlichen Einvernehmens zum Handlungsbedarf noch immer keine konkreten Ergebnisse. Ich mahne angesichts der langen Zeitdauer ein Tätigwerden nunmehr dringend an.

13. 21. TB Nr. 13.1.3 zu **Entlassungsberichten aus Rehabilitationseinrichtungen:**

Schon mehrfach hatte ich darauf aufmerksam gemacht, dass sich Krankenkassen sensible Gesundheitsdaten übermitteln lassen. Auf der Grundlage des § 13 Absatz 4 der Richtlinie des Gemeinsamen Bundesausschusses über Leistungen zur medizinischen Rehabilitation (Rehabilitationsrichtlinie) erhielten sie die Entlassungsberichte aus Rehabilitationseinrichtungen. Diese Berichte enthielten auch sehr persönliche Daten, so zum Beispiel eine sozialmedizinische Beurteilung im Hinblick auf die Selbstständigkeit der Leistungsempfänger, ihre Motivation zur Lebensstiländerung sowie ihre Leistungsfähigkeit im Erwerbsleben. Diese Angaben gingen deutlich über den Umfang der personenbezogenen Daten hinaus, die den gesetzlichen Krankenkassen auf Grundlage des § 301 Absatz 4 SGB V von den Rehabilitationseinrichtungen zu übermitteln sind. Nach Erörterung mit dem Gemeinsamen Bundesausschuss wird § 13 Absatz 4 der Rehabilitationsrichtlinie nun dahingehend abgeändert, dass Entlassungsberichte nach Beendigung medizinischer Rehabilitationsleistungen nicht mehr an die Krankenkassen übermittelt werden.

14. 20. TB Nr. 10.3.2; 21. TB Nr. 14.3 zu **EPOS 2.0:**

Wiederholt hatte ich über die Entwicklung und Einführung des neuen elektronischen Personal-, Organisations- und Stellenmanagementsystems EPOS 2.0 berichtet. In diesem Zusammenhang hatte ich mich auch für einen datenschutzgerechten Umgang mit Personal-/Personalaktendaten ausgeschiedener Beschäftigter eingesetzt, den das System bisher leider noch nicht realisiert. Im Berichtszeitraum konnte ich mit dem BMI nun endlich auch eine technische Lösung zur Löschung der nicht mehr erforderlichen Daten ehemaliger Mitarbeiter abstimmen. Mit deren Umsetzung gehe ich zukünftig von einem datenschutzkonformen Umgang auch mit diesen Personal-/Personalaktendaten in EPOS 2.0 aus.

15. 21. TB Nr. 14.2 zum **Dienstrechtsneuordnungsgesetz:**

Das Gesetz zur Neuordnung und Modernisierung des Bundesdienstrechts (kurz: Dienstrechtsneuordnungsgesetz) ist am 12. Februar 2009 in Kraft getreten (BGBl I 2009 S. 160). Ich konnte erreichen, dass datenschutzrechtliche Belange gebührend berücksichtigt worden sind, etwa zur Führung und Aufbewahrung von Personalakten. Zu begrüßen ist besonders, dass die Einführung elektronischer Personalakten nunmehr auf eine gesicherte gesetzliche Grundlage gestellt worden ist.

16. 21. TB Nr. 11.2 zum **Express- und Paketzustelldienst UPS**:

Von dem Verfahren des Express- und Paketzustelldienstes UPS, das Datenschutzniveau der Unternehmen der UPS-Gruppe an europäische Standards heranzuführen, habe ich berichtet. Ich hatte UPS im Jahr 2003 nach § 4c Absatz 2 BDSG eine Genehmigung zum Datenaustausch erteilt (vgl. 20. TB Nr. 14.1.2). Nunmehr hat UPS sich dafür entschieden, den gesamten Datentransfer auf die Grundlage der Standardvertragsklauseln II (2004/915/EG) zu stellen, so dass Einzelgenehmigungen insoweit künftig nicht mehr erforderlich sein werden.

17. 21. TB Nr. 12.6 zur **Übermittlung flugmedizinischer Daten an das Luftfahrt-Bundesamt (LBA):**

Anlässlich eines Besuchs beim Flugmedizinischen Dienst der Deutschen Gesellschaft für Luft- und Raumfahrt habe ich mir nun die praktische Anwendung der gesetzlich vorgeschriebenen Aufsicht des LBA über die flugmedizinischen Sachverständigen und Zentren (§ 24e Absatz 7 Luftverkehrszulassungsverordnung – LuftVZO) erläutern lassen. Dem LBA stehen zur Ausübung der Aufsicht zwei Möglichkeiten zur Verfügung: Entweder lässt sich das LBA stichprobenartig ausgewählte anonymisierte flugmedizinische Unterlagen zusenden oder kontrolliert die Sachverständigen vor Ort. Dabei müssen auch bei der Vor-Ort-Kontrolle die Unterlagen anonymisiert werden. Nur in Fällen, in denen ein konkreter Verdacht auf Ungereimtheiten besteht, z. B. dass einem offensichtlich untauglichen Bewerber ein Tauglichkeitszeugnis ausgestellt wurde, muss der flugmedizinische Sachverständige die Zuordnung zu der Person des Bewerbers ermöglichen. Leider gibt es zur Zeit keine eindeutigen Regelungen zur Durchführung von Vor-Ort-Kontrollen, so dass ich das LBA aufgefordert habe, hier tätig zu werden.

Nicht zuletzt vor dem Hintergrund eines Falles, in dem ein Fliegerarzt über 250 Piloten die Flugtauglichkeit bescheinigte, ohne diese Personen tatsächlich untersucht zu haben, verschließe ich mich nicht der Forderung, die Fachaufsicht des LBA zu stärken und angemessene Änderungen in der LuftVZO zu akzeptieren. Allerdings teilte mir das zuständige BMVBS mit, dass die Zuständigkeit für die Rechtsetzung im gesamten Bereich der Lizenzierung einschließlich des flugmedizinischen Untersuchungswesens zwischenzeitlich auf die europäische Ebene übergegangen und ein nationales Gesetzgebungsverfahren angesichts im Jahr 2010 zu erwartender europäischer Regelungen nicht angezeigt sei.

Ich werde die Entwicklung weiterhin aufmerksam verfolgen und mich dafür einsetzen, dass ein Gleichgewicht zwischen der notwendigen Fachaufsicht und dem schutzwürdigen Interesse des Einzelnen hergestellt wird.

18. 21. TB Nr. 12.2 ff. zu **Telematikverfahren für Kraftfahrzeuge:**

Zu den Telematikverfahren für Kraftfahrzeuge – E-Call, Event Data Recorder, Pay as You Drive – haben sich in der Zwischenzeit keine wesentlichen neuen Entwicklungen ergeben. Bezüglich des automatischen Notrufsystems E-Call geht die Europäische Kommission nach wie vor davon aus, dass es ab Septem-

ber 2010 in alle neu zugelassenen Fahrzeuge eingebaut werden kann. Zur Zeit wird versucht, die technischen Voraussetzungen hierfür zu schaffen, wie zum Beispiel ein europaweit einheitliches Datenprotokoll und die erforderliche Ausstattung der Notrufstellen mit Empfangsgeräten. Hinsichtlich der Nutzung von in die Kraftfahrzeuge eingebauten Fahrtdatenaufzeichnungsgeräten ist bisher, soweit ersichtlich, kein quantitativer Sprung eingetreten. Ein Einsatz als Unfalldatenschreiber oder im Rahmen besonderer Pay-as-You-Drive-KFZ-Versicherungstarife erfolgt bisher in Deutschland noch nicht in nennenswertem Umfang. Aus datenschutzrechtlicher Sicht ist daran festzuhalten, dass solche Geräte grundsätzlich nur auf freiwilliger Basis eingebaut werden sollten.

19. 21. TB Nr. 7.6 zu **Wissenschaftsservern:**

Ich hatte über die Arbeit der Forschungsdatenzentren des Statistischen Bundesamtes und der Statistischen Landesämter sowie über das vom Statistischen Bundesamt entwickelte Modell eines Wissenschaftsservers berichtet. Mit dessen Hilfe soll es möglich werden, den Wissenschaftlern das volle Analysepotential von statistischen Einzeldaten, das bisher nur am Gastwissenschaftlerarbeitsplatz bei den Ämtern selbst oder im Wege des kontrollierten Fernrechnens zugänglich ist, in datenschutzgerechter Form auch am normalen Arbeitsplatz (z. B. Universitätsinstitut) zur Verfügung zu stellen. Die zur Erprobung des Verfahrens begonnene Machbarkeitsstudie konnte bisher nach Auskunft des Statistischen Bundesamtes (aus Kostengründen) nicht zum Abschluss geführt werden. Ob und gegebenenfalls wann ein derartiges Verfahren eingeführt wird, ist derzeit nicht absehbar.

20. 21. TB Nr. 9.4 zu **SWIFT:**

Über die unzulässige Datenübermittlung an US-Behörden durch das internationale Bankennetzwerk SWIFT (Society for Worldwide Interbank Financial Telecommunication) hatte ich berichtet. Am 28. Juni 2007 haben die Regierungen der EU-Mitgliedstaaten eine Vereinbarung über den Zugriff der US-Sicherheitsbehörden auf europäische Bankdaten gebilligt. Dem zufolge hat sich das US-Finanzministerium schriftlich verpflichtet, die durch SWIFT übermittelten Daten ausschließlich zur Terrorismusbekämpfung und nicht für handels- oder industriepolitische Zwecke zu nutzen. Die vom US-Finanzministerium vorgeschlagene Regelung sieht zudem vor, dass die SWIFT-Daten nach maximal fünf Jahren gelöscht werden müssen, insbesondere diejenigen, die nicht zur Terrorismusbekämpfung benötigt werden. Mindestens einmal jährlich muss eine Prüfung vorgenommen werden, welche von SWIFT erhaltenen Daten gelöscht werden können. Ein EU-Beauftragter, der von der Europäischen Kommission, vom Ministerrat und vom Parlament bestimmt wird, soll jährlich darüber Bericht erstatten, ob die USA ihre Zusagen einhalten. SWIFT hat darüber hinaus Ende letzten Jahres eine Änderung ihrer IT-Infrastruktur angekündigt. Demzufolge soll bis Ende 2009 ein weiteres europäisches Rechenzentrum in der Schweiz errichtet werden, nach dessen Errichtung eine Spiegelung der Transaktionsdaten mit rein europäischem Hintergrund in den USA entfallen wird. Erfreulich ist ferner, dass die deutschen Banken ihrer Informationspflicht gegenüber ihren Kunden nachgekommen sind und auf die mögliche Datenübermittlung an das in den USA ansässige SWIFT-Rechenzentrum im Falle von grenzüberschreitenden Zahlungsaufträgen hinweisen.

21. 21. TB Nr. 5.2.4.1 zur **Verarbeitung erkennungsdienstlicher Unterlagen im Bundeskriminalamt:**

Ich begrüße es, dass das BKA nunmehr das Verfahren insofern geändert hat, als dort künftig alle Datensätze einer Aussonderungsprüfung unterzogen werden, deren E-Gruppe nach Löschung in den Ländern systemtechnisch in den „endgültigen Besitz“ des BKA übergegangen ist, ohne dass es auf den Ablauf einer durch das BKA vergebenen Aussonderungsprüffrist ankommt. Durch die im August 2008 erfolgte Verfahrensumstellung sind ca. 300 000 Datensätze vom BKA zu überprüfen.

22. 21. TB Nr. 5.2.7 zur **Geldwäsche:**

Das Gesetz zur Ergänzung der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung ist am 21. August 2008 in Kraft getreten (BGBl. I 2008 S. 1690). Dieses Gesetz dient im Wesentlichen der Umsetzung der Dritten EG-Geldwäscherichtlinie (ABl. L 309 vom 25. November 2005, 15) und der ergänzenden Richtlinie 2006/70/EG. Das novellierte Geldwäschegesetz wird voraussichtlich zu einer Zunahme der anzeigepflichtigen Geldwäscheverdachtsfälle führen. Zum einen sollen die anzeigepflichtigen Transaktionen ausgeweitet werden. Ferner soll das zur Geldwäschebekämpfung entwickelte Instrumentarium auch für die Bekämpfung der Terrorismusfinanzierung eingesetzt werden. Es ist also zu erwarten, dass die problematische Speicherung von standardisierten „Verdachtsanzeigen“, die nicht zur Anklage wegen einer Straftat nach § 261 StGB (Geldwäsche) führen, ansteigen wird. Gleichwohl werden personenbezogene Daten bis zu zehn Jahren gespeichert, um sie gegebenenfalls für die Bekämpfung sonstiger Katalogdelikte, die in § 261 StGB aufgelistet sind, zu verwenden. Dies ist mit dem Zweckbindungsprinzip kaum vereinbar.

23. 21. TB Nr. 5.4.1 zum **Zollfahndungsdienstegesetz:**

Die nach dem Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 zur präventiven Telekommunikationsüberwachung erforderlich gewordenen Anpassungen des Zollfahndungsdienstgesetzes sind mit dem Gesetz zur Änderung des Zollfahndungsdienstgesetzes (ZfDG) vom 22. Juni 2007 (BGBl. I 2007 S. 1037) umgesetzt worden.

Den verfassungsrechtlichen Vorgaben zur Gewährleistung des Kernbereichs privater Lebensgestaltung wurde dabei allerdings nicht in vollem Umfang

Rechnung getragen. Quasi als Vorbild für die spätere BKA-Gesetzesnovelle (Nr. 4.3.1) wird der Kernbereichsschutz auch in diesem Gesetz insofern unzulässig verkürzt, als eine präventiv-polizeiliche Telekommunikationsüberwachung nur unzulässig ist, wenn aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass allein kernbereichsrelevante Kommunikationsinhalte erfasst werden. Zudem fehlen kernbereichsschützende Regelungen in Zusammenhang mit den in §§ 18 ff. ZfDG normierten verdeckten Datenerhebungsbefugnissen völlig.

Ich hatte auf diese Defizite im Rahmen des Gesetzgebungsverfahrens und einer Anhörung des Rechtsausschusses des Deutschen Bundestages hingewiesen. Die Regelungen haben seinerzeit weit weniger Diskussionen ausgelöst als die vergleichbaren Regelungen der BKA-Gesetzesnovelle.

24. 21. TB Nr. 6.2 zur **akustischen Wohnraumüberwachung:**

Ich habe bereits über die am 1. Juli 2005 in Kraft getretene Neuregelung der akustischen Wohnraumüberwachung in der StPO berichtet. Inzwischen hat das BVerfG die neuen Vorschriften in § 100c StPO zum Schutz des Kernbereichs privater Lebensgestaltung für verfassungsgemäß erklärt (Beschluss vom 11. Mai 2007, 2 BvR 543/06).

Die von der Bundesregierung vorgelegten Statistiken zur akustischen Wohnraumüberwachung für die Jahre 2006 und 2007 (Bundestagsdrucksache 16/6363 und 16/10300) zeigen, dass sich im Jahr 2006 der Rückgang der Anwendungszahlen seit dem Urteil des BVerfG zum „Großen Lauschangriff“ weiter fortsetzte und im repressiven Bereich nur noch drei Überwachungsmaßnahmen (gegenüber sieben im Jahr 2005) durchgeführt wurden. Dagegen ist die Anwendungshäufigkeit im Jahr 2007 auf zehn Maßnahmen gestiegen. Damit gab es aber auch 2007 deutlich weniger Maßnahmen als in den Jahren vor dem Urteil des BVerfG. Der Trend, dass bestimmte, nach wie vor im Anlasstatenkatalog des § 100c StPO enthaltene Delikte (wie z. B. Geldfälschung oder qualifizierte Formen der Hehlerei) für die akustische Wohnraumüberwachung in der Praxis keine Rolle spielen, setzte sich fort. Daher halte ich eine kritische Überprüfung des Straftatenkatalogs unter dem Aspekt des tatsächlichen Bedarfs weiterhin für geboten.

25. 21. TB Nr. 10.3 zur **unterdrückten Rufnummer:**

Wie bereits berichtet, nutzen einzelne Versandhäuser einen Service, mit dem auch der mit unterdrückter Rufnummer anrufende Kunde schneller persönlich begrüßt werden kann. Voraussetzung ist die ausdrückliche Einwilligung des Kunden in eine Nutzung der Rufnummer, auch wenn diese unterdrückt ist. Aufgrund der vorangegangenen Beratung war ich davon ausgegangen, dass die Einwilligungen korrekt eingeholt werden.

Die Eingabe einer Kundin eines der Versandhäuser veranlasste mich zu einer erneuten Rückfrage bei dem betreffenden Telekommunikationsanbieter zur Praxis bei diesem Versandhaus. Hier konnte ich zunächst überraschend wenig Verständnis für die seinerzeit vereinbarten Vorgaben erkennen. Letztendlich hat das Versandhaus bis auf weiteres auf die Nutzung des Leistungsmerkmals verzichtet, wahrscheinlich da es seinen Kunden eine umfangreiche Information über die Aufhebung der Rufnummernunterdrückung nicht geben wollte.

Anlagen

Anlage 1

Hinweise für die Ausschüsse des Deutschen Bundestages

Nachfolgend habe ich dargestellt, welche Beiträge dieses Berichtes für welchen Ausschuss von *besonderem Interesse* sein könnten:

Auswärtiger Ausschuss	13.1; 13.5 ff.; 13.6; 13.8; 13.9; 14.2
Innenausschuss	2.1 bis 2.9; 3.1; 3.2.1 bis 3.2.5; 3.4.4 bis 3.4.7; 4.1.; 4.2.1; 4.8.3; 5.2 bis 5.5; 6; 6.3; 6.3.1 f.; 6.5; 6.8; 6.9; 7.1 bis 7.3; 7.6; 7.10; 7.11; 11.2; 11.3; 13.3.1 bis 13.3.2; 13.3.6; 13.5.3; 13.6; 16.1 bis 16.4
Sportausschuss	5.9
Rechtsausschuss	2.1 bis 2.6; 2.8 bis 2.10; 3.1; 3.2.1 bis 3.2.5; 3.4.4 bis 3.4.7; 4.1; 4.5; 5.1; 6.3.1 f.; 6.9; 7.1 bis 7.4; 7.6; 7.10; 7.11; 8; 13.2; 13.3.1; 13.5 ff.; 13.6; 16.8; 16.12
Finanzausschuss	6.4; 9.1 bis 9.5; 16.5
Ausschuss für Wirtschaft und Technologie	2.2 bis 2.6; 2.8; 3.1; 3.2.1 bis 3.2.5; 3.4.1; 3.4.4 bis 3.4.7; 6; 6.2; 6.9; 7.1 bis 7.2; 7.9; 7.11; 8; 13.2.3
Ausschuss für Ernährung, Landwirtschaft und Verbraucherschutz	2.2 bis 2.6; 2.8; 3.1; 3.4.4 bis 3.4.5; 3.4.7; 6; 6.8; 8.5
Ausschuss für Arbeit und Soziales	7.6; 10.4; 10.5.1 bis 10.5.4; 11.1; 11.3; 11.4; 16.6 f.
Verteidigungsausschuss	14.1; 16.10 f.
Ausschuss für Familie, Senioren, Frauen und Jugend	2.9; 7.3
Ausschuss für Gesundheit	6.1; 6.1.2; 6.2; 10.1 bis 10.4; 16.13
Ausschuss für Verkehr, Bau und Stadtentwicklung	12.1
Ausschuss für Bildung, Forschung und Technikfolgenabschätzung	6; 6.3; 6.8; 8; 8.1 bis 8.5
Ausschuss für die Angelegenheiten der Europäischen Union	6; 8; 13.1 bis 13.2; 13.2.1; 13.5 ff.; 13.8
Ausschuss für Kultur und Medien	3.2.1 bis 3.2.2; 5.5; 5.7; 7.1 bis 7.3; 7.6
Ausschuss für Kultur und Medien – Unterausschuss „Neue Medien“ –	6; 6.3; 6.8; 7.1 bis 7.3; 8; 8.1 bis 8.5;

Anlage 2

Übersicht über die durchgeführten Kontrollen, Beratungen und Informationsbesuche

Auswärtiges Amt

– Botschaft

Bundeskanzleramt (einschließlich Beauftragter für Kultur und Medien)

– Bundesnachrichtendienst

– Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (Zentrale und zwei Außenstellen)

Bundesministerium des Innern

– Ministerium

– Bundesverwaltungsamt

– Statistisches Bundesamt

– Technisches Hilfswerk

– Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

– Bundesinstitut für Sportwissenschaft

– Bundeskriminalamt (Wiesbaden, Meckenheim und Berlin)

– Bundespolizeidirektion

– Bundespolizeiamt Halle/S

– Bundespolizeiamt Flughafen Frankfurt/Main

– Bundesamt für Verfassungsschutz

Bundesministerium der Justiz

– Bundesamt für Justiz

– Bundesnotarkammer

– Generalbundesanwalt

Bundesministerium der Finanzen

– Bundeszentralamt für Steuern/Informationszentrale für steuerliche Auslandsbeziehungen

– Bundesanstalt für Finanzdienstleistungsaufsicht

– Deutsche Bundesbank

Bundesministerium für Arbeit und Soziales

– Ministerium

– Deutsche Rentenversicherung Bund

– Bundesagentur für Arbeit

– Agentur für Arbeit (Jobbörse)

Bundesministerium der Verteidigung

– Ministerium

– Militärischer Abschirmdienst

Bundesministerium für Familie, Senioren, Frauen und Jugend

– Bundesamt für den Zivildienst

Bundesministerium für Gesundheit

– Bundesversicherungsamt

– Robert-Koch-Institut

Bundesministerium für Verkehr, Bau und Stadtentwicklung

– Ministerium

– Luftfahrt-Bundesamt

– Kraftfahrt-Bundesamt

– Maritimes Sicherheitszentrum

Bundesministerium für Wirtschaft und Technologie

– Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung

– Ministerium

Deutsche Post AG

– Zentrale

– Briefzentrum Köln

– DHL Zentrale

– Tochterunternehmen Deutsche Post Adress GmbH und Deutsche Post Direkt GmbH

Neue Postdienstunternehmen

– Hermes Logistik Service, Außenstelle Aachen

– TNT Express und TNT Post (Thomas Nationwide Transport)

– PIN Mail AG, Berlin

Telekommunikationsunternehmen

– Deutsche Telekom AG

noch Anlage 2

- Kabel Deutschland GmbH
- Mobilcom Communicationstechnik GmbH
- O2 (Germany) GmbH & Co. OHG
- O2 (Germany) Service GmbH
- Betamax GmbH & Co. KG
- Arcor AG & Co. KG

Sonstige

- Innungskrankenkasse Hamburg
- Innungskrankenkasse Weser-Ems
- BARMER Ersatzkasse
- Wirtschaftsunternehmen wegen Verfahren zur Sicherheitsüberprüfung

Anlage 3

Übersicht über Beanstandungen nach § 25 BDSG

Auswärtiges Amt

- Verstoß einer Auslandsvertretung gegen § 4f Absatz 2 Satz 1 BDSG wegen Bestellung des Kanzlers der Botschaft (u. a. Zuständigkeit für Personalangelegenheiten) zum behördlichen Datenschutzbeauftragten (s. Nr. 14.2)
- Verstoß einer Auslandsvertretung gegen § 18 Absatz 2 Satz 1 BDSG wegen mangelnder Führung des Verzeichnisses der Datenverarbeitungsanlagen (s. Nr. 14.2)
- Verstoß einer Auslandsvertretung gegen § 18 Absatz 2 Satz 2 i. V. m. § 4e BDSG wegen fehlender schriftlicher Angaben zur Zweckbestimmung der Datenerhebung und -verwendung sowie der Rechtsgrundlage der Datenerhebung (s. Nr. 14.2)

Bundesministerium des Verteidigung

- Verstoß des Militärischen Abschirmdienstes gegen § 24 Absatz 4 BDSG wegen fehlender Mitwirkung (s. Nr. 4.7.2)

Bundesministerium für Wirtschaft und Technologie

- Verstoß der PIN Group AG gegen die Mitwirkungspflicht nach § 24 Absatz 4 BDSG (s. Nr. 3.3.2)

Gesetzliche Krankenkassen

Drei Beanstandungen wegen:

- Verstoß gegen das in § 35 SGB I normierte Sozialgeheimnis
- Verstoß gegen § 284 Absatz 3 SGB V
- Verstoß gegen die Vorschriften des § 78a SGB X und der Anlage zu § 78a SGB X (s. Nr. 10.2.4)

Zwei Beanstandungen wegen:

- Verstoß gegen das in § 35 SGB I normierte Sozialgeheimnis
- Verstoß gegen die Vorschriften des § 78a SGB X und der Anlage zu § 78a SGB X (s. Nr. 10.2.4)

Sonstige

- Verstoß gegen Sicherheitsüberprüfungen außerhalb des SÜG wegen fehlender Rechtsgrundlage für eine Zuverlässigkeitsüberprüfung (s. Nr. 4.8.3.2)

Anlage 4

Deutscher Bundestag **Drucksache 16/4882**

16. Wahlperiode 28. 03. 2007

Beschlussempfehlung und Bericht

des Innenausschusses (4. Ausschuss)

zu der Unterrichtung durch den Bundesbeauftragten für den Datenschutz – Drucksache 15/5252 –

Tätigkeitsbericht 2003 und 2004 des Bundesbeauftragten für den Datenschutz – 20. Tätigkeitsbericht –

A. Problem

Der 20. Tätigkeitsbericht gibt einen Überblick über die Schwerpunkte der Arbeit des Bundesbeauftragten für den Datenschutz in den Jahren 2003 und 2004 sowie einen Ausblick auf anstehende wichtige Fragen.

Umfassend wird die Weiterentwicklung und Modernisierung des Datenschutzrechts begründet. Die Gefahren für das informationelle Selbstbestimmungsrecht durch die immer weiter voranschreitenden technologischen Innovationen werden verdeutlicht. Ebenso werden die zunehmende Bedeutung europäischer Rechtsinstrumente und ihre Auswirkungen auf den Datenschutz aufgezeigt.

Zudem enthält die Unterrichtung wesentliche Feststellungen zur datenschutzrechtlichen Kontrolle von öffentlichen Stellen des Bundes.

B. Lösung

Kenntnisnahme der Unterrichtung und einstimmige Annahme der Entschließung

C. Alternativen

Keine

D. Kosten

Keine

noch Anlage 4

Beschlussempfehlung

Der Bundestag wolle beschließen, in Kenntnis der Unterrichtung auf Drucksache 15/5252 folgende Entschließung anzunehmen:

1. Der Deutsche Bundestag unterstreicht seine Forderung aus den Entschließungen zum 18. und 19. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz nach einer zügigen Modernisierung und Weiterentwicklung des Datenschutzrechts. Für einen modernen und innovativen Datenschutz ist es in Anbetracht neuer technologischer Entwicklungen mit ständig wachsenden Datenbeständen und deren zunehmender Vernetzung dringend erforderlich, die Reform nunmehr zügig voranzutreiben. Ein modernes, leicht verständliches und übersichtliches Datenschutzrecht ist auch ein wirtschaftlicher Standortvorteil (20. TB Nr. 2.1).	**Nicht** erledigt s. 22. TB Nr. 2.2 f.
2. Der Deutsche Bundestag hält an seiner bereits in der Entschließung zum 19. Tätigkeitsbericht aufgestellten Forderung nach einem Datenschutzauditgesetz gemäß § 9a BDSG fest. Ein solches Gesetz muss den Unternehmen die Möglichkeit eines Audits auf freiwilliger Basis bieten und unbürokratisch ausgestaltet sein. So könnte es ein wichtiges Element eines modernen Datenschutzes werden. Der Deutsche Bundestag fordert die Bundesregierung auf, einen entsprechenden Gesetzentwurf vorzulegen (20. TB Nr. 2.2).	**Noch nicht** erledigt, aber aufgegriffen im Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften (Bundesratsdrucksache 4/09) s. 22. TB Nr. 2.4
3. Der Deutsche Bundestag erwartet von der Bundesregierung, dass sie seine mehrfach erhobene Forderung aufgreift, den Arbeitnehmerdatenschutz gesetzlich zu regeln, und unverzüglich einen entsprechenden Gesetzentwurf vorlegt (20. TB, Nr. 2.5 und 10.1).	**Nicht** erledigt s. 22. TB Nr. 11.1
4. Der Deutsche Bundestag unterstützt die Bemühungen zur Schaffung eines europäischen Raums der Freiheit, der Sicherheit und des Rechts. Hierzu zählt auch die Schaffung eines hohen und harmonisierten Datenschutzstandards in der dritten Säule der EU. Ein gemeinsamer europaweiter Datenschutzstandard würde auch das Verfahren der grenzüberschreitenden Datenübermittlung vereinheitlichen und damit den Informationsaustausch zwischen den Polizei- und Sicherheitsbehörden erleichtern. Die Bundesregierung wird deshalb aufgefordert, sich auf der Basis des Rahmenbeschlusses über den Datenschutz in der dritten Säule der EU für eine zügige Verabschiedung entsprechender datenschutzrechtlicher Regelungen auf diesem Gebiet innerhalb der deutschen Ratspräsidentschaft einzusetzen (20. TB Nr. 3.3.4).	Erledigt Der „Rahmenbeschluss über den Schutz personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen“ wurde durch den Rat der Innen- und Justizminister der EU-Mitgliedstaaten am 27. November 2008 beschlossen. s. 22. TB Nr. 13.3.1
5. Der Deutsche Bundestag kritisiert, dass eine Vielzahl von personenbezogenen Daten über den internationalen Zahlungsverkehr durch die Society for Worldwide Interbank Financial Telecommunication (SWIFT) an US-amerikanische Behörden übermittelt wurden, ohne zu klären, ob dafür eine Rechtsgrundlage vorhanden ist. Die Bundesregierung wird aufgefordert, sich für eine Lösung einzusetzen, die sicherstellt, dass bei der Datenübermittlung an ausländische Behörden zur Terrorbekämpfung die Grundsätze des Datenschutzes der EU sowie das Bankgeheimnis und das informationelle Selbstbestimmungsrecht der Bankkunden gewährleistet sind.	Erledigt Die Regierungen der EU-Mitgliedsstaaten haben am 28. Juni 2007 eine Vereinbarung über den Zugriff der US-Sicherheitsbehörden auf europäische Bankdaten gebilligt, die seitens der US-Regierung vorgeschlagen wurde. s. 22. TB Nr. 16.21

noch Anlage 4

6. Der Deutsche Bundestag unterstützt die Bundesregierung in dem Ziel, bei den anstehenden Verhandlungen zwischen der EU und den USA für ein längerfristiges Abkommen zur Übermittlung von Fluggastdaten ein angemessenes Datenschutzniveau zu gewährleisten, insbesondere bei der Begrenzung der Datenübermittlung und der Zweckbindung. Vordringlich ist die Umstellung vom sog. Pull-Verfahren (Abrufzugriff) auf das sog. Push-Verfahren (Übermittlung durch die Fluggesellschaften) (20. TB Nr. 22.2).	Erledigt Ein neues EU-Abkommen mit den USA zur Übermittlung von PNR-Daten wurde im Jahre 2007 geschlossen. s. 22. TB Nr. 13.5.2
7. Der Deutsche Bundestag hat bereits in seiner Entschließung zum 19. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (Bundestagsdrucksache 15/4597) die Bedeutung von Entwicklung und Einsatz datenschutzfreundlicher Technologien hervorgehoben (Nr. 5). Er fordert die Bundesregierung auf, sich für die Gewährleistung des Daten- und Verbraucherschutzes bei der Nutzung der RFID-Technologie einzusetzen. Insbesondere muss dafür Sorge getragen werden, dass die Betroffenen umfassend über den Einsatz, Verwendungszweck und den Inhalt von RFID-Tags informiert werden. Es muss die Möglichkeit bestehen, die im Handel verwendeten RFID-Tags dauerhaft zu deaktivieren bzw. die darauf enthaltenen Daten zu löschen, wenn Daten nicht mehr erforderlich sind. Ferner muss gewährleistet werden, dass Daten von RFID-Tags aus verschiedenen Produkten nur so verarbeitet werden, dass keine heimlichen personenbezogenen Verhaltens-, Nutzungs- und Bewegungsprofile erstellt werden können. Die Bundesregierung wird aufgefordert, dem Deutschen Bundestag noch in diesem Jahr über ihre Aktivitäten und Planungen und einen möglichen gesetzgeberischen Handlungsbedarf zu berichten (20. TB Nr. 4.2.1).	**Noch nicht** in allen Punkten erledigt Die Bundesregierung (BMWi, BMELV) hat hierzu – auch im Rahmen der EU-Präsidentschaft – mehrere Aktionen durchgeführt. Insbesondere wurde mit Vertretern der Wirtschaft über daten- und verbraucherschutzfreundliche Lösungen diskutiert s. 22. TB Nr. 6.7
8. In der Entschließung zum 19. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz war die Bundesregierung vom Bundestag aufgefordert worden, zu prüfen, ob und wie, etwa durch Regelungen zur Beschränkung der Profilbildung, zur Begrenzung der zentralen Auskunfteien auf branchenspezifische Auskunftssysteme und zur Stärkung der Rechtsposition der Betroffenen gegenüber zentralen Auskunfteien und ihren Vertragspartnern, ein wirksamer Schutz der Betroffenen und ihres Restitutionsinteresses insbesondere bei Verarbeitung unrichtiger Daten erreicht werden kann. Der Deutsche Bundestag wird den nunmehr vorliegenden Bericht der Bundesregierung insbesondere im Hinblick auf eventuell bestehenden Gesetzgebungsbedarf prüfen.	**Noch nicht** erledigt, aber aufgegriffen durch den Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes (Bundestagsdrucksache 16/10529) s. 22. TB Nr. 2.3, 3.2.5, 3.4.4
9. Der Einsatz von Genomanalysen ist in den letzten Jahren aufgrund des wissenschaftlichen Fortschritts immer weiter ausgedehnt worden und beschränkt sich nicht mehr auf die Verbrechensbekämpfung und die Überführung von Straftätern. Aber nur für diesen Bereich gibt es spezialgesetzliche Regelungen, während ansonsten auf das allgemeine Datenschutzrecht zurückgegriffen werden muss. Dieses reicht vielfach nicht aus, um den Kernbereich der Persönlichkeit eines jeden Menschen gegen Missbrauch wirkungsvoll zu schützen. Der Deutsche Bundestag hält eine gesetzliche Regelung für den Bereich der Humangenetik für erforderlich. Er erwartet deshalb von der Bundesregierung, noch in dieser Legislaturperiode eine gesetzliche Regelung über genetische Untersuchungen bei Menschen vorzulegen, in der die Bereiche geregelt werden sollen, die angesichts der Erkenntnismöglichkeiten der Humangenetik einen besonderen Schutzstandard erfordern, um die Persönlichkeitsrechte der Bürgerinnen und Bürger zu schützen (20. TB Nr. 2.6).	**Noch nicht** erledigt Die Bundesregierung hat einen Gesetzentwurf vorgelegt, der sich im parlamentarischen Abstimmungsverfahren befindet (Bundestagsdrucksache 16/10532). s. 22. TB Nr. 10.1

noch Anlage 4

10. Der Bundestag erinnert an die Zusage des Bundesministeriums der Finanzen, den Betroffenen auch gegenüber der Steuerverwaltung einen Anspruch auf Auskunft zu den über sie gespeicherten Daten einzuräumen. Der Stellungnahme der Bundesregierung ist zu entnehmen, dass dieser Auskunftsanspruch deswegen noch nicht in ein Gesetzgebungsverfahren eingebracht worden ist, weil „zuvor die personellen, organisatorischen und haushalterischen Auswirkungen“ geprüft werden müssten. Der Deutsche Bundestag fordert die Bundesregierung auf, diese Prüfungen nunmehr zeitnah abzuschließen und die gesetzliche Regelung eines Auskunftsanspruchs in der AO in die Wege zu leiten (20. TB Nr. 8.1).	**Noch nicht** erledigt, da sich das BMF trotz BVerfG-Beschlusses und der BT-Entschließung zum 20. TB weiterhin weigert, Auskunftsrechte der Betroffenen anzuerkennen s. 22. TB Nr. 9.5
11. Durch das Gesetz zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003 wurde mit Wirkung vom 1. April 2005 Finanz- und anderen Behörden die Möglichkeit eingeräumt, bei Kreditinstituten Informationen über Stammdaten von Konto- und Depotverbindungen einzuholen, damit – wie von der Rechtsprechung des Bundesverfassungsgerichts gefordert – strukturelle Erhebungsdefizite vermieden werden. Der Deutsche Bundestag sieht Änderungen des geltenden Rechts hinsichtlich der Ausgestaltung des Kontenabrufverfahrens wie die Informationsverpflichtungen der Behörden, Dokumentation der Abrufe und die Benennung der Leistungen, die zur Kontenabfrage berechtigen, als erforderlich an. Darüber hinaus sollte in geeigneter Form ein Zeichnungsvorbehalt durch den Behördenleiter oder einer von ihm speziell beauftragten Führungskraft vorgesehen werden, um Routineabfragen und Missbrauchsmöglichkeiten vorzubeugen.	Erledigt § 93 Abs. 8 AO alte Fassung wurde durch § 93 Abs. 8 - 10 AO neue Fassung ersetzt. Aus § 93 Abs. 8 AO ergeben sich mittelbar die Behörden, die zum Kontenabruf berechtigt sind, die Abrufvoraussetzungen und die Zweckbestimmungen. s. 22. TB Nr. 9.4
12. Der Deutsche Bundestag begleitet die Vorbereitungen für die elektronische Gesundheitskarte mit großem Interesse. Er unterstreicht noch einmal seine Forderung, die verschiedenen technischen Lösungsansätze ohne Vorfestlegung auf ein bestimmtes Verfahren umfassend und sorgfältig zu prüfen, um ein Maximum an Datenschutz zu gewährleisten. Nur wenn die Bedenken und Ängste der betroffenen Menschen überzeugend ausgeräumt sind, kann die flächendeckende Einführung der Gesundheitskarte erfolgreich gelingen.	Erledigt Die Bundesregierung achtet darauf, dass eine sorgfältige und technikoffene Testphase zur Einführung der elektronischen Gesundheitskarte möglich ist. s. 22. TB Nr. 6.1
13. Der Deutsche Bundestag ist weiterhin der Überzeugung, dass sinnvolle E-Government-Angebote zu Entbürokratisierung und Bürgernähe beitragen können. Hierbei muss aber dem Datenschutz ein hoher Stellenwert eingeräumt werden, da nur so die Akzeptanz bei den Betroffenen erreicht werden kann, die für eine erfolgreiche Umsetzung des Programms erforderlich ist.	**Noch nicht** in allen Punkten erledigt s. 22. TB Nr. 2.7, 6.6

In der Plenarsitzung des Deutschen Bundestages vom 29. März 2007 einstimmig angenommen.

Anlage 5

Deutscher Bundestag **Drucksache 16/12271**

16. Wahlperiode 17. 03. 2009

Beschlussempfehlung und Bericht
des Innenausschusses (4. Ausschuss)

zu der Unterrichtung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
– Drucksache 16/4950 –

Tätigkeitsbericht 2005 und 2006 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
– 21. Tätigkeitsbericht –

A. Problem

Der 21. Tätigkeitsbericht stellt die Arbeitsschwerpunkte des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in den Jahren 2005 und 2006 überblickartig dar und geht dabei insbesondere auf die zunehmende technologisch bedingten Kontroll- und Überwachungsrisiken sowohl im Verhältnis Staat-Bürger als auch beim Umgang der Wirtschaft mit personenbezogenen Daten ein. Schwerpunkte setzt der Bericht unter anderem bei der Darstellung und Beurteilung europäischer Rechtsentwicklungen, beim technologischen Datenschutz und bei datenschutzrechtlichen Fragen der inneren Sicherheit. Dabei werden auch wichtige Feststellungen zur datenschutzrechtlichen Kontrolle von öffentlichen Stellen des Bundes getroffen. Zentrale Bedeutung für die weitere Entwicklung zur Informationsgesellschaft misst der Bericht der Frage zu, wie der Gesetzgeber zukünftig von seinen Gestaltungsoptionen Gebrauch mache, ob er die Grundrechtspositionen stärke oder neue Grundrechtseinschränkungen legitimiere.

B. Lösung

Kenntnisnahme der Unterrichtung und einstimmige Annahme einer Entschließung

C. Alternativen

Keine

D. Kosten

Keine

noch Anlage 5

Beschlussempfehlung

Der Bundestag wolle beschließen, in Kenntnis der Unterrichtung auf Drucksache 16/4950 folgende Entschließung anzunehmen:

1. Der Deutsche Bundestag begrüßt, dass die Bundesregierung seine Forderung aus den Entschließungen zum 19. und 20. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach Vorlage eines Datenschutzauditgesetzes gemäß § 9a BDSG aufgegriffen hat und an einem entsprechenden Gesetzentwurf arbeitet. Ein solches Gesetz muss den Unternehmen die Möglichkeit eines Audits auf freiwilliger Basis bieten und unbürokratisch ausgestaltet sein.

   Dieses Projekt muss jetzt zügig vorangebracht werden, damit ein Datenschutzauditgesetz noch in dieser Legislaturperiode verabschiedet werden kann (21. TB, Nr. 2.4).

2. Der Abstand zwischen den geltenden datenschutzrechtlichen Bestimmungen und der rasanten technologischen Entwicklung mit ihren Folgen in allen Lebensbereichen wird immer größer. Das vom Deutschen Bundestag geforderte moderne, leicht verständliche und übersichtliche Datenschutzrecht wäre nicht nur ein wirtschaftlicher Standortvorteil, sondern könnte auch einen wertvollen Beitrag zur Entbürokratisierung leisten (21. TB, Nr. 2.1).

3. Der Deutsche Bundestag beobachtet sorgfältig die Entwicklung von Informations- und Kommunikationstechnologien, die neben Vorteilen für das tägliche Leben auch neue Risiken wie z. B. Identitätsdiebstahl, diskriminierende Profilerstellung oder Betrugsdelikte mit sich bringen.

   Die Bundesregierung wird aufgefordert, dafür Sorge zu tragen, dass datenschutzfreundliche Technologien weiter entwickelt, verbreitet und verwendet werden, um den Schutz der Privatsphäre und den Datenschutz zu verbessern.

4. Nachdem auf europäischer Ebene eine Initiative zum Arbeitnehmerdatenschutz nicht mehr zu erwarten ist, weist der Deutsche Bundestag die Bundesregierung noch einmal nachdrücklich auf seine mehrfach erhobene Forderung hin, schnellstmöglich einen Gesetzentwurf zum Arbeitnehmerdatenschutz vorzulegen (21. TB, Nr. 2.7).

5. Der Deutsche Bundestag hat zuletzt in seiner Entschließung zum 20. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die Bundesregierung an ihre Zusage erinnert, den Betroffenen auch gegenüber der Steuerverwaltung einen Anspruch auf Auskunft zu den über sie gespeicherten Daten einzuräumen. Gleichzeitig hatte er die Bundesregierung aufgefordert, ihre Prüfungen über die personellen, organisatorischen und haushalterischen Auswirkungen eines solchen Auskunftsanspruchs zeitnah abzuschließen.

   Dieser Aufforderung ist die Bundesregierung noch immer nicht nachgekommen. Der Deutsche Bundestag fordert die Bundesregierung deshalb erneut auf, den Auskunftsanspruch des Betroffen auch in der Steuerverwaltung sicherzustellen.

6. Der Deutsche Bundestag fordert die Bundesregierung auf, die Bürgerinnen und Bürger besser vor den Gefahren des Missbrauchs biometrischer Systeme zu schützen. Bei der Entwicklung von Biometrieanwendungen muss ein hoher Datenschutzstandard gewährleistet sein, so dass der Datenschutz der Bürgerinnen und Bürger sichergestellt ist und Missbrauchsmöglichkeiten ausgeschlossen sind.

7. Der Deutsche Bundestag teilt die Auffassung der Bundesregierung, dass das Bundesdatenschutzgesetz auch für Rechtsanwälte gilt. Er begrüßt, dass die Bundesregierung prüft, welche gesetzlichen Regelungen sich im Zusammenhang mit der Verarbeitung mandatsbezogener Daten durch Rechtsanwälte empfehlen, um eine wirksame Datenschutzkontrolle zu gewährleisten, ohne dass das besonders geschützte Vertrauensverhältnis zwischen Rechtsanwalt und Mandant in unzulässiger Weise beeinträchtigt wird.

In der Plenarsitzung des Deutschen Bundestages vom 19. März 2009 einstimmig angenommen.

Anlage 6 (zu Nr. 13.9)

29. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre
Montreal (Kanada), 26. bis 28. September 2007

Resolution über den dringenden Bedarf an globalen Standards zum Schutz von Passagierdaten, die von Regierungsstellen zu Justizvollzugs- und Grenzschutzzwecken herangezogen werden

Antragsteller: Der Bundesbeauftragte für den Datenschutz und Informationsfreiheit (Deutschland)

Unterstützt von: Österreichische Datenschutzkommission (Österreich)

Office of the Privacy Commissioner of Canada (Kanada)

Office of the Information and Privacy Commissioner of British Columbia

Office of the Information and Privacy Commissioner of Ontario

European Data Protection Supervisor (Europäische Gemeinschaft)

La Commission Nationale de l'Informatique et des Libertés (Frankreich)

Landesbeauftragte für Datenschutz und die Informationsfreiheit Nordrhein-Westfalen (Deutschland – Regional)

Garante per la protezione dei dati personali (Italien)

College Bescherming Persoonsgegevens (Niederlande)

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Rumänien)

Agencia de Protección de Datos (Spanien)

Information Commissioner (Vereinigte Königreich)

Die Konferenz beruft sich auf

– das 2002 auf der 24. Internationalen Konferenz in Cardiff angenommene Kommuniqué;

– die 2003 auf der 25. Internationalen Konferenz in Sydney angenommene Resolution über die Übertragung von Passagierdaten;

– die 2005 auf der 27. Internationalen Konferenz in Montreux verabschiedete Deklaration zum Datenschutz und zum Schutz der Privatsphäre in einer globalisierten Welt; in denen zum Ausdruck kommt, dass es gilt, zwischen dem legitimen Kampf gegen den Terrorismus und gegen die internationale Kriminalität einerseits und dem Datenschutz und dem Schutz der Privatsphäre andererseits ein Gleichgewicht herzustellen.

Die Konferenz vermerkt, dass

– Regierungsstellen zunehmend den Zugriff zu Passagierdaten suchen, die im Kampf gegen den Terrorismus, gegen illegale Einwanderung und andere Verbrechen verwendet werden sollen, ohne dass genügend Rücksicht auf Persönlichkeitsschutz und die Menschenrechte der Passagiere genommen wird;

– manche Passagierdaten dazu benutzt werden können, Folgerungen über Religionszugehörigkeit, Ethnie und andere äußerst heikle Zusammenhänge zu ziehen,

– weltweit viele Regierungen ständig mehr Daten von Verkehrsträgern verlangen,

– Verkehrsträger die Passagierdaten aus kommerziellen Gründen erfassen und dann aufgefordert werden, sie für Justizvollzugszwecke zur Verfügung zu stellen,

– Verkehrsträger zunehmend viele verschiedene Forderungen zur Übergabe von Daten erfüllen müssen und sich an viele verschiedene Datenübertragungssysteme halten müssen, wodurch unter den Verkehrsträgern wie auch unter den Passagieren Ungewissheit über ihre Rechte und Pflichten entsteht, wodurch die Passagiere nur schwer verstehen, wie ihre Daten genutzt werden, und wodurch auch das Risiko entsteht, dass die Verkehrsträger die Daten unsachgemäß übertragen,

– diese vielen verschiedenen Forderungen und Systeme sowohl für die Verkehrsträger als auch für die Passagiere mit Kosten verbunden sind,

– juristische und technische Übereinstimmung erforderlich ist, damit die Verkehrsträger diese Forderungen erfüllen können,

– manche Verkehrsträger immer noch nicht ihrer Pflicht nachkommen, Passagiere über die Verwendung und Offenlegung ihrer Daten zu unterrichten,

– andere globale Abmachungen zur Erleichterung des internationalen Flugverkehrs getroffen worden sind, und dass dringender Bedarf besteht, globale Lösungen zu treffen, die den internationalen Reiseverkehr erleichtern und dabei das Recht der Passagiere auf Persönlichkeitsschutz respektieren.

Die Konferenz bestätigt erneut, dass

– Datenschutz und Schutz der Privatsphäre – wie in Artikel 12 der Allgemeinen Deklaration der Menschenrechte und in anderen Rechtsinstrumenten verankert – Privatpersonen und ihre persönlichen Daten schützen und zusammen mit anderen Rechten in allen Ersuchen zur Übertragung und Nutzung von Passagierdaten für Justizvollzugszwecke berücksichtigt werden müssen,

noch Anlage 6

- die Verarbeitung von Passagierdaten in einem Rahmen stattfinden sollte, der die anerkannten Datenschutzgrundsätze und -standards berücksichtigt,
- in allen Ersuchen staatlicher Behörden für die Nutzung von Passagierdaten Folgendes nachgewiesen werden sollte:
  - sie sind nachweisbar notwendig, um ein spezifisches Problem anzusprechen,
  - sie sind nachweisbar mit Wahrscheinlichkeit geeignet, das Problem anzusprechen,
  - sie entsprechen proportional ihrem Sicherheitswert, und sie greifen nachweisbar weniger in die Privatsphäre ein als alternative Optionen, sowie dass all solche Ersuche regelmäßig zu überprüfen sind, um festzustellen, ob die Maßnahmen noch erforderlich sind,
- die Notwendigkeit, unter allen Umständen die Privatsphäre zu schützen, nicht nur für globale Datenschutzkreise, sondern auch für alle eine grundsätzliche Aufgabe bleibt, die um die Wahrung der fundamentalen Rechte und Freiheiten besorgt sind, und
- wenn Regierungsstellen sich nicht bemühen, die Datenschutzbelange richtig zu wägen, die echte Gefahr besteht, dass diese Stellen beginnen könnten, die fundamentalen Rechte und Freiheiten selbst, die sie schließlich schützen wollen, zu unterminieren.

Im Bestreben nach globalen Standards zum Schutz von Passagierdaten, die von Regierungsstellen zu Justizvollzugs- und Grenzschutzzwecken herangezogen werden, ruft die Konferenz dazu auf,

- dass internationale Organisationen (wie z. B. IATA und ICAO), Regierungsstellen und Verkehrsträger mit den Beauftragten für den Datenschutz und für die Privatsphäre zusammenarbeiten, um verbindliche globale Lösungen mit angemessenen Datenschutzsicherheiten einzuführen,
- dass Regierungsstellen gewährleisten, dass alle Ersuche für die Nutzung von Passagierdaten
  - nachweisbar notwendig sind, um ein spezifisches Problem anzusprechen,
  - nachweisbar mit Wahrscheinlichkeit geeignet sind, das Problem anzusprechen;
  - ihrem Sicherheitswert proportional entsprechen, und
  - nachweisbar weniger in die Privatsphäre eingreifen als alternative Optionen, sowie dass all solche Ersuche regelmäßig überprüft werden sollten, um festzustellen, ob die Maßnahmen noch erforderlich sind,
- dass alle Passagierdaten nutzenden staatlichen Programme für Datenminimalisierung sowie für die ausdrückliche Beschränkung der Nutzung, Offenlegung und Einbehaltung der Daten auf die entsprechenden Programmzwecke sowie für die Richtigkeit der Daten, für das Recht auf Zugriff zu den Daten, für die Korrigierung der Daten und für eine unabhängige Überprüfung sorgen sollten,
- dass alle Lösungen die juristischen, technischen, finanziellen und wirtschaftlichen Belange der Verkehrsträger und der Behörden berücksichtigen müssen,
- dass Regierungsstellen offen und transparent die Zwecke, zu denen die Daten gesammelt und genutzt werden, angeben, und sicher stellen, dass alle Passagiere – ungeachtet ihrer Nationalität oder ihres Herkunftslandes – Zugang zu ihren persönlichen Informationen sowie zu einem angemessenen Rechtshilfemechanismus haben,
- dass Verkehrsträger ihre Passagiere über die Nutzung und Offenlegung ihrer Daten durch Regierungsstellen und Justizvollzugsbehörden, über Flugverbotslisten und ähnliche Überwachungslisten sowie über die Verfügbarkeit von Rechtshilfemaßnahmen im Zusammenhang mit Passagierdaten und damit zusammenhängenden persönlichen Informationen ausreichend unterrichten, und
- dass die Beauftragten für den Datenschutz und den Schutz der Privatsphäre weiterhin zusammenarbeiten, um sachgemäße Datenschutzmaßnahmen zu gewährleisten und auf verbindliche globale Lösungen zu dringen.

Erläuternder Hinweis

Die Regierungen verschiedener Länder haben zunehmend versucht, Passagierdaten als Waffe im Kampf gegen Terrorismus, transnationale Kriminalität und andere Verbrechen zu nutzen. Dadurch sind in Bezug auf die geforderten Datenelemente, die Verwendung der Daten und die Stufe der Sicherheitsmaßnahmen Differenzen aufgetreten.

Das Wesen des internationalen Reiseverkehrs fordert einen globalen Ansatz, und es ist eine globale Lösung dringend erforderlich, um eine angemessene Sicherheitsstufe zu erlangen und das Vertrauen der Passagiere zu gewinnen, während proportionale Maßnahmen unternommen werden, die den notwendigen Datenschutz und den Schutz der Privatsphäre beinhalten. Während Bedenken über den Datenschutz und den Schutz der Privatsphäre die vorrangigen Themen darstellen, die bei jeder globalen Lösung zu berücksichtigen sind, bietet sich auch Gelegenheit, andere juristische, technische, finanzielle und wirtschaftliche Fragen von Fluggesellschaften und Passagieren in Betracht zu ziehen.

Globale Standards können die Fairness, Übereinstimmung, juristische Gewissheit und Sicherheit für Passagiere und Verkehrsträger gewährleisten. Es ist klar, dass Verkehrsträger, Justizvollzugsbehörden, internationale Orga-

noch Anlage 6

nisationen, zivilgesellschaftliche Gruppen und Datenschutzexperten an der globalen Lösung beteiligt sein müssen. Das Engagement der Datenschutzbeauftragten ist unentbehrlich, wenn Fortschritte erzielt werden sollen. Sie müssen die Führung übernehmen und auf einer solchen Lösung bestehen.

Anlage 7 (zu Nr. 13.9)

30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre
Straßburg, 15. bis 17. Oktober 2008

Entschließung zum Datenschutz in Sozialen Netzwerkdiensten

Antragsteller: Berliner Beauftragter für Datenschutz und Informationsfreiheit, Deutschland

Unterstützt durch:

Commission Nationale de l'Informatique et des Libertés (CNIL), Frankreich;

Bundesbeauftragter für Datenschutz und Informationsfreiheit, Deutschland;

Garante per la protezione dei dati personali, Italien;

College Bescherming Persoonsgegevens, Niederlande;

Privacy Commissioner, Neuseeland;

Eidgenössischer Datenschutz und Öffentlichkeitsbeauftragter (EDÖB), Schweiz

Entschließung

Soziale Netzwerkdienste[1] haben in den letzten Jahren große Beliebtheit erworben. Diese Dienste bieten ihren Teilnehmern Interaktionsmöglichkeiten auf der Basis von selbst generierten persönlichen Profilen, die in einem noch nie da gewesenen Ausmaß die Veröffentlichung persönlicher Informationen zu den betreffenden Personen (und auch anderen Personen) mit sich bringen. Die sozialen Netzwerkdienste bieten zwar ein neues Spektrum von Möglichkeiten für Kommunikation und den Echtzeit-Austausch von Informationen jeder Art, die Nutzung dieser Dienste kann jedoch auch eine Gefährdung der Privatsphäre ihrer Nutzer – und Anderer – mit sich bringen, denn personenbezogene Daten einzelner Personen werden in bisher unbekannter Weise und Menge öffentlich (und global) zugänglich, einschließlich großer Mengen digitaler Fotos und Videos. Der Einzelne läuft Gefahr, die Kontrolle über die Nutzung der Daten durch Andere zu verlieren, wenn sie erst einmal im Netzwerk publiziert sind: Während der Community-Bezug sozialer Netzwerke die Vorstellung erweckt, die Veröffentlichung der eigenen persönlichen Daten laufe in etwa auf das Gleiche hinaus, wie früher das Mitteilen von Information unter Freunden von Angesicht zu Angesicht, können Profildaten tatsächlich für alle Teilnehmer einer Community (deren Zahl in die Millionen gehen kann) verfügbar sein. Derzeit gibt es wenig Schutz dagegen, dass personenbezogene Daten jeder Art aus Profilen kopiert werden – durch andere Mitglieder des Netzwerks oder durch unbefugte netzwerkfremde Dritte – und zum Aufbau von Persönlichkeitsprofilen verwendet werden oder dass die Daten anderweitig wieder veröffentlicht werden. Es kann sehr schwierig – und manchmal unmöglich – sein zu erreichen, dass Daten, wenn sie einmal publiziert sind, wieder vollständig aus dem Internet entfernt werden. Selbst nach ihrer Löschung auf der ursprünglichen Website (z. B. dem sozialen Netzwerk) können Kopien bei Dritten oder bei den Anbietern der sozialen Netzwerkdienste verbleiben. Personenbezogene Daten aus Nutzerprofilen können auch außerhalb des Netzwerks bekannt werden, wenn sie von Suchmaschinen indexiert werden. Hinzu kommt, dass manche Anbieter sozialer Netzwerkdienste über Applikationsprogrammierschnittstellen Drittanbietern Nutzerdaten zur Verfügung stellen, die dann unter der Kontrolle dieser Dritten stehen. Ein Beispiel von Wiederverwendungen, das großes öffentliches Aufsehen erregt hat, ist die Praxis von Personalverantwortlichen, Nutzerprofile von Stellenbewerbern oder Angestellten zu durchsuchen. Presseberichten zufolge gibt bereits heute ein Drittel der Personalverantwortlichen an, bei ihrer Arbeit Daten aus sozialen Netzwerkdiensten zu nutzen, z. B. um die einzelnen Angaben von Bewerbern zu überprüfen und/oder zu ergänzen. Profilinformationen und Verkehrsdaten werden von Anbietern sozialer Netzwerkdienste auch zur Weiterleitung zielgerichteter Werbung an ihre Nutzer verwendet. Sehr wahrscheinlich werden in Zukunft noch weitere unerwartete Verwendungen von Informationen in Nutzerprofilen auftreten. Zu weiteren, bereits jetzt identifizierten spezifischen Risiken für Datenschutz und Datensicherheit zählen erhöhte Risiken durch Identitätsbetrug, der durch die umfangreiche Verfügbarkeit personenbezogener Daten in Nutzerprofilen begünstigt wird, und durch eine mögliche Übernahme von Profilen durch unbefugte Dritte. Die 30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre erinnert daran, dass diese Risiken bereits in dem Dokument „Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten" („Rom-Memorandum")[2] der 43. Tagung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation (3. bis 4. März 2008) und in dem ENISA Positionspapier Nr. 1 „Security Issues and Recommendations for Online Social Networks"[3] (Oktober 2007) analysiert wurden. Die in der In-

[1] „Ein sozialer Netzwerkdienst stellt ab auf den Aufbau […] sozialer Online-Netzwerke für Gruppen von Menschen, die gemeinsame Interessen und Aktivitäten teilen oder daran interessiert sind, die Interessen und Aktivitäten Anderer zu erkunden […]. Die meisten Dienste sind hauptsächlich webbasiert und bieten Nutzern eine Reihe verschiedener Interaktionsmöglichkeiten […]". Zitat aus Wikipedia: http://en.wikipedia.org/wiki/Social_network_service.

[2] http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491

[3] http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

ternationalen Konferenz versammelten Datenschutzbeauftragten sind von der Notwendigkeit überzeugt, dass als Erstes eine intensive Informationskampagne unter Beteiligung aller öffentlichen und privaten Interessengruppen – von Regierungsstellen bis zu Bildungseinrichtungen wie Schulen, von Anbietern sozialer Netzwerkdienste bis zu Verbraucher- und Nutzerverbänden, einschließlich der Datenschutzbeauftragten selbst – durchgeführt werden muss, um den vielfältigen mit der Nutzung sozialer Netzwerkdienste verbundenen Gefahren vorzubeugen.

Empfehlungen

In Anbetracht der besonderen Natur der Dienste und der kurz- und langfristigen Gefahren für die Privatsphäre des Einzelnen richtet die Konferenz folgende Empfehlungen an Nutzer und Anbieter sozialer Netzwerkdienste:

Nutzer sozialer Netzwerkdienste

Organisationen, denen am Wohl der Nutzer sozialer Netzwerke gelegen ist – einschließlich Diensteanbieter, Regierungen und Datenschutzbehörden – sollten mithelfen, die Nutzer über den Schutz ihrer personenbezogenen Daten aufzuklären und die folgende Botschaften zu vermitteln.

1. Veröffentlichung von Daten

Nutzer sozialer Netzwerkdienste sollten sich sorgfältig überlegen, welche persönlichen Daten sie – wenn überhaupt – in einem sozialen Netzwerkprofil publizieren. Sie sollten bedenken, dass sie zu einem späteren Zeitpunkt mit einer Information oder mit Bildern konfrontiert werden könnten, z. B. wenn sie sich um eine Arbeitsstelle bewerben.

Insbesondere sollten Minderjährige vermeiden, ihre Privatanschrift oder ihre Telefonnummer mitzuteilen. Privatpersonen sollten sich überlegen, ob es nicht ratsam wäre, in einem Profil anstelle ihres wirklichen Namens ein Pseudonym zu verwenden. Dabei sollten sie jedoch nicht vergessen, dass auch die Benutzung von Pseudonymen nur einen begrenzten Schutz gewährt, da Dritte in der Lage sein können, ein solches Pseudonym aufzudecken.

2. Die Privatsphäre Anderer

Nutzer sollten auch die Privatsphäre Anderer achten. Sie sollten besonders vorsichtig sein bei der Veröffentlichung personenbezogener Daten Anderer (einschließlich Bildern, oder sogar mit Zusatzinformationen versehenen Bildern) ohne die Einwilligung der betreffenden Personen.

Anbieter sozialer Netzwerkdienste

Anbieter sozialer Netzwerkdienste tragen eine besondere Verantwortung dafür, die Belange von Personen, die soziale Netzwerke nutzen, zu beachten und zu wahren. Sie sollten nicht nur die Regelungen des Datenschutzrechts einhalten, sondern auch die folgenden Empfehlungen umsetzen.

1. Datenschutzvorschriften und -standards

Anbieter, die in verschiedenen Ländern oder sogar weltweit tätig sind, sollten die Datenschutzstandards der Länder einhalten, in denen sie ihre Dienste betreiben. Zu diesem Zweck sollten die Anbieter Datenschutzbehörden konsultieren, wenn und soweit dies notwendig ist.

2. Aufklärung der Nutzer

Anbieter sozialer Netzwerkdienste sollten ihre Nutzer über die Verarbeitung ihrer personenbezogenen Daten transparent und offen informieren. Es sollte auch aufrichtig und verständlich über mögliche Folgen einer Veröffentlichung persönlicher Daten in einem Profil und über verbleibende Sicherheitsrisiken sowie über gesetzliche Zugriffsrechte Dritter (einschließlich z. B. von Strafverfolgungsbehörden) aufgeklärt werden. Eine solche Aufklärung sollte auch Hinweise dazu enthalten, wie Nutzer mit personenbezogenen Daten von Dritten umgehen sollten, die in ihren Profilen enthalten sind.

3. Nutzerkontrolle

Anbieter sollten die Kontrolle der Nutzer über die Verwendung ihrer Profildaten durch andere Community-Mitglieder weiter verbessern. Sie sollten die Einschränkung der Sichtbarkeit ganzer Profile sowie von in Profilen enthaltenen Daten, und in Community-Suchfunktionen ermöglichen. Die Anbieter sollten auch eine Kontrolle der Nutzer über die Nutzung von Profil- und Verkehrsdaten, z. B. für zielgerichtete Werbung, ermöglichen. Als ein Minimum sollten eine Opt-out-Möglichkeit für allgemeine Profildaten und eine Opt-in-Möglichkeit für sensible Profildaten (z. B. politische Überzeugungen, sexuelle Orientierung) und Verkehrsdaten geboten werden.

4. Datenschutzfreundliche Standardeinstellungen

Darüber hinaus sollten Anbieter datenschutzfreundliche Standardeinstellungen für Nutzerprofilinformationen anbieten. Standardeinstellungen spielen eine Schlüsselrolle beim Schutz des Privatsphäre der Nutzer: Es ist bekannt, dass lediglich eine Minderheit von Nutzern, die sich bei einem Dienst anmelden, irgendwelche Änderungen daran vornimmt.

Diese Einstellungen müssen bei einem sozialen Netzwerkdienst, der sich an Minderjährige wendet, besonders restriktiv sein.

5. Sicherheit

Anbieter sollten die Sicherheit ihrer Informationssysteme weiter verbessern und aufrechterhalten und die Nutzer ge-

noch Anlage 7

gen betrügerische Zugriffe auf ihre Profile schützen, indem sie für die Konzeption, die Entwicklung und den Betrieb ihrer Anwendungen anerkannte Methoden einschließlich unabhängigem Auditing und unabhängiger Zertifizierung verwenden.

6. Auskunftsrechte

Anbieter sollten Personen (gleichgültig ob Mitglieder des sozialen Netzwerkdienstes oder nicht) ein Recht auf Auskunft zu ihren personenbezogenen Daten gewähren und erforderlichenfalls diese Daten berichtigen.

7. Löschung von Nutzerprofilen

Anbieter sollten den Nutzern die Möglichkeit geben, ihre Mitgliedschaft auf einfache Weise zu beenden und ihre Profile sowie alle Inhalte oder Informationen, die sie in dem sozialen Netzwerk publiziert haben, zu löschen.

8. Pseudonyme Nutzung des Dienstes

Anbieter sollten als Option die Möglichkeit der Einrichtung und Verwendung pseudonymer Profile anbieten und zur Nutzung dieser Option ermutigen.

9. Zugriff durch Drittpersonen

Anbieter sollten wirksame Maßnahmen ergreifen, um das Durchsuchen und/oder massenweise Herunterladen (oder „bulk harvesting“) von Profildaten durch Dritte zu verhindern.

10. Indexierbarkeit der Nutzerprofile

Die Anbieter sollten sicherstellten, dass Nutzerdaten von externen Suchmaschinen nur durchsucht werden können, wenn der Nutzer dazu seine ausdrückliche, vorherige und informierte Einwilligung erteilt hat. Die Nichtindexierbarkeit von Profilen durch Suchmaschinen sollte als Standard eingestellt sein.

Anlage 8 (zu Nr. 13.9)

30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre
Straßburg, 17. Oktober 2008

Entschließung zum Schutz der Privatsphäre von Kindern im Internet

Antragstellerin: Die Datenschutzbeauftragte von Kanada

Unterstützt durchs : Datenschutzbeauftragter, Neuseeland

La Commission Nationale de l'Informatique et des Libertés (Frankreich)

Datenschutzbeauftragter, Irland

Beauftragter für den Datenschutz und Informationsfreiheit, Berlin

Überall in der Welt gehen die Jugendlichen von zu Hause und von der Schule aus sowie über ihre kabellosen Geräte ins Internet. Sie nutzen das Internet zur sozialen Interaktion – sie tauschen Geschichten, Ideen, Fotos und Videos aus, sie bleiben den Tag über durch SMS-Mitteilungen in Kontakt mit ihren Freunden und sie beteiligen sich an Online-Spielen gemeinsam mit anderen Personen am anderen Ende der Welt.

Dabei werden die Jugendlichen auch mit den Schwierigkeiten und Herausforderungen bezüglich des Schutzes ihrer persönlichen Daten im Internet konfrontiert. Das Fehlen einer Regelung bei zahlreichen Internet-Diensten macht die Sache schwierig. Viele der bei Jugendlichen beliebtesten Websites sammeln große Mengen personenbezogener Daten für Verkaufs- und Marketingzwecke.

Mit steigender Anzahl der im Internet angebotenen Anwendungen und Technologien wird die Menge der gesammelten und aufbewahrten personenbezogenen Daten immer größer. Heute sind sich die Jugendlichen oft nicht darüber bewusst, dass ihre Auskünfte, ihre Gewohnheiten und ihre Verhaltensweisen im Internet überwacht werden. Untersuchungen zeigen, dass die Jugendlichen (wie auch zahlreiche Erwachsene) nur selten die Geheimhaltungserklärungen der von ihnen besuchten Websites lesen, was nicht überrascht, denn die Vertraulichkeitserklärungen zahlreicher Websites sind in einer technischen oder juristischen Fachsprache abgefasst, die für die meisten Leser schwer verständlich ist.

Wenn auch manche Jugendliche die mit ihren Online-Aktivitäten verbundenen Gefahren erkennen, so verfügen sie doch nicht über die Erfahrung, die technischen Kenntnisse oder die nötigen Instrumente, um diese Gefahren zu mindern. Oft kennen sie ihre gesetzlichen Rechte nicht.

Vor fast 20 Jahren hat die Generalversammlung der Vereinten Nationen 1989 ein Übereinkommen über die Rechte des Kindes verabschiedet. In diesem heißt es, dass die Staaten die Rechte des Kindes achten und schützen müssen, einschließlich ihres Rechtes auf den Schutz ihrer Privatsphäre.

Seit dieser Zeit bereiteten den Datenschutzbeauftragten die Verletzungen der Privatsphäre von Kindern im Internet immer mehr Sorgen.

In der am 20. Februar 2008 vom Ministerrat des Europarats angenommenen Erklärung zum Schutz der Würde, Sicherheit und der Privatsphäre von Kindern im Internet zeigt sich dieser von der Notwendigkeit überzeugt, Kinder über die lange Speicherdauer und über die Risiken der von ihnen ins Internet eingestellten Inhalte aufzuklären. Er erklärte darüber hinaus, dass, anders als bei der Strafverfolgung, keine fortbestehenden oder dauerhaft zugänglichen Aufzeichnungen über die von Kindern ins Internet eingestellten Inhalte existieren sollten, die deren Würde, Sicherheit und Privatsphäre angreifen oder ihnen auf andere Art und Weise jetzt oder zu einem späteren Zeitpunkt ihres Lebens schaden können.

Die Datenschutzbeauftragten haben zugleich erkannt, dass ein auf Erziehung ausgerichteter Ansatz, verbunden mit einer Regelung des Datenschutzes, eine der wirksamsten Methoden zur Bewältigung dieses Problems darstellt. So haben mehrere Länder innovative, auf Erziehung angelegte Konzepte umgesetzt, um der Herausforderung zu begegnen, die der Schutz der Privatsphäre von Kindern im Internet darstellt.

Kinder und Jugendliche haben ein Recht darauf, sich online sicher bewegen und positive Erfahrungen machen zu können, bei denen sie die Absichten der Personen, mit denen sie interagieren, kennen und verstehen.

Die auf der 30. internationalen Konferenz versammelten Beauftragten für den Datenschutz und für die Privatsphäre haben beschlossen:

– die Erarbeitung von Ansätzen zu fördern, die auf Erziehung angelegt sind, um die Lage in Bezug auf den Schutz der Privatsphäre im Internet auf nationaler wie auf internationaler Ebene zu verbessern;

– bemüht zu sein, dafür zu sorgen, dass Kinder und Jugendliche in der ganzen Welt Zugang zu einem sicheren Online-Umfeld haben, das ihre Privatsphäre respektiert;

– mit Partnern und Akteuren im eigenen Land und im Ausland zusammenzuarbeiten, in der Erkenntnis, dass die Zusammenarbeit mit den Fachleuten, die das tägliche Leben der Kinder beeinflussen, von entscheidender Bedeutung ist;

– miteinander zu arbeiten, um beispielhafte Praktiken auszutauschen und Aktivitäten zur Erziehung der Öffentlichkeit durchzuführen, um Kinder und Jugendli-

noch Anlage 8

che stärker zu sensibilisieren hinsichtlich der Gefahren in Bezug auf den Schutz ihrer Privatsphäre, die mit ihren Online-Aktivitäten verbunden sind, und bezüglich der sich ihnen bietenden Möglichkeiten einer aufgeklärten Wahl, um ihre persönlichen Informationen zu kontrollieren;

– bei Erziehenden die Einsicht zu fördern, dass die Sensibilisierung für den Schutz der Privatsphäre einen wesentlichen Aspekt der Kindererziehung darstellt und in ihr Unterrichtsprogramm aufgenommen werden muss;

– zu fordern, dass die Behörden Gesetze erlassen, die die Sammlung, Verwendung und Mitteilung personenbezogener Daten von Kindern einschränken, einschließlich geeigneter Bestimmungen für den Fall von Verstößen;

– bei Online-Werbung für Kinder oder verhaltensbezogener Werbung geeignete Einschränkungen bei der Sammlung, Verwendung und Mitteilung personenbezogener Daten von Kindern zu fordern;

– die Betreiber von Websites für Kinder anzuhalten, ihr soziales Bewusstsein unter Beweis zu stellen, indem sie Vertraulichkeitserklärungen und Nutzungsvereinbarungen einführen, die klar, einfach und verständlich sind und indem sie die Nutzer über die Gefahren für den Schutz der Privatsphäre und die Sicherheit sowie über die ihnen auf der Website gebotenen Wahlmöglichkeiten aufklären.

Anlage 9 (zu Nr. 13.8)

Erklärung der Europäischen Datenschutzkonferenz von Zypern, angenommen am 11. Mai 2007

Im Rat der Europäischen Union ist ein Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten bei der Verarbeitung im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen Gegenstand von Beratungen.

Die Schaffung eines harmonisierten und hohen Standards für den Datenschutz bei polizeilichen und justiziellen Maßnahmen in der Union ist in der Tat ein entscheidender Bestandteil der Achtung und des Schutzes von Grundrechten, wie des Rechts auf den Schutz personenbezogener Daten, bei der Schaffung eines Raums der Freiheit, der Sicherheit und des Rechts.

Die Initiativen in der Europäischen Union zur Verbesserung der Bekämpfung von schweren Straftaten und Terrorismus haben das Ziel gemeinsam, nationale Grenzen innerhalb der Union zunehmend unwichtiger werden zu lassen, wenn es um die Bedingungen für den Austausch von Daten zwischen zuständigen Behörden geht. Daten für die Strafverfolgung sollen auf verschiedenen Wegen zugänglich gemacht werden, inklusive der Möglichkeit des direkten Zugriffs auf nationale Datenbestände.

Diese Initiativen zeigen deutlich, dass die Verpflichtung der Union zur Hilfe beim Kampf gegen schwere Straftaten und Terrorismus nicht auf die Schaffung der Bedingungen für den Informationsaustausch zwischen den Mitgliedstaaten beschränkt ist; klar erkennbar haben die Initiativen auch Auswirkungen auf die Datenverarbeitung auf nationaler Ebene, die jedem möglichen Austausch vorangeht. Es ist klar, dass jede Entwicklung auf diesem Gebiet abgewogen werden muss mit angemessenen und harmonisierten Datenschutzrechten und -verpflichtungen, wobei das gegenseitige Vertrauen in diese ein entscheidender Bestandteil ist.

Innerhalb der Europäischen Union unterscheidet sich die Datenschutz-Gesetzgebung für Maßnahmen der Strafverfolgung sowohl der Natur als auch der Sache nach. Sie gewährleistet somit sicherlich keinen harmonisierten Ansatz zum Datenschutz für Strafverfolgungs-Informationen, für die Rechte des Betroffenen sowie für eine effektive unabhängige Kontrolle.

Im Hinblick auf den zunehmenden Rückgriff auf die Verfügbarkeit („availability“) von Informationen als Konzept zur Verbesserung des Kampfes gegen schwere Straftaten, sowohl auf nationaler Ebene wie zwischen den Mitgliedstaaten, führt das Fehlen eines harmonisierten und hohen Standards für den Datenschutz in der Union zu einer Situation, in der das Grundrecht auf den Schutz personenbezogener Daten nicht mehr ausreichend gewährleistet wird.

Mit Bezugnahme auf ihr Positionspapier zu Strafverfolgung und Informationsaustausch in der EU (April 2005) und an ihre Erklärungen von Krakau (2005), Budapest (2006) und London (2006) erinnernd, ruft die gesamte Europäische Datenschutzkonferenz daher die im Rat der Europäischen Union und im Europäischen Parlament vertretenen Mitgliedstaaten dazu auf, einen solchen harmonisierten und hohen Standard des Datenschutzes in der Europäischen Union zu schaffen.

Die Europäische Datenschutzkonferenz ist sich über die Grundsatz-Diskussion im Rat über den Anwendungsbereich des vorgeschlagenen Rahmenbeschlusses bewusst: sollte er nur auf Daten anwendbar sein, die zwischen Mitgliedstaaten ausgetauscht werden oder auf jegliche Verarbeitung durch Polizei- und Justizbehörden?

Die Europäische Datenschutzkonferenz weist wiederholt darauf hin, dass Initiativen der Union Auswirkungen auf nationaler Ebene haben und darauf, dass eine Begrenzung des Anwendungsbereiches auf Daten, die zwischen den Mitgliedstaaten ausgetauscht werden oder werden könnten, das Risiko besonderer Unsicherheiten und Unwägbarkeiten über den Anwendungsbereich des vorgeschlagenen Rahmenbeschlusses mit sich bringen würde. Sie **betont, dass nur ein umfassender Anwendungsbereich unter Einschluss aller Arten der Verarbeitung personenbezogener Daten den notwendigen Schutz der Individuen gewährleisten kann.**

Die Europäische Datenschutzkonferenz **betont weiter, dass die von der deutschen Ratspräsidentschaft am 13. März 2007 vorgelegte Fassung des Entwurfs des Rahmenbeschlusses auch bezüglich anderer Datenschutz-Grundsätze keine verlässliche und strenge Datenschutzordnung enthält** und dass sie weder die Stellungnahme der Europäischen Datenschutzkonferenz vom 24. Januar 2006 noch die Stellungnahme des EP vom 18. Mai 2006 einbezogen hat.

Während der Entwurf einige Verbesserungen im Hinblick auf die Erreichung eines harmonisierten Rahmens für die Verarbeitung gebracht hat, ist er bislang unbefriedigend bei den Vorkehrungen zur Gewährleistung des Schutzes der Privatsphäre der Bürger. Dies muss besonders gelten, wenn man die bereits bestehende europäische Gesetzgebung zum Datenschutz berücksichtigt, insbesondere den rechtlichen Rahmen, der von den nationalen Gesetzgebern bei der Umsetzung der Richtlinie 95/46/EG geschaffen wurde und der ebenfalls auf die Verarbeitung personenbezogener Daten in dem fraglichen Bereich anwendbar ist. Darüber hinaus wiederholt die Europäische Datenschutzkonferenz, dass es notwendig ist, die auf nationaler Ebene bestehenden Schutzvorkehrungen zum Datenschutz zu erhalten, indem ein bindendes europäisches Instrumentarium verabschiedet wird.

Mit dem Ziel einer tatsächlichen Verbesserung beim Datenschutz in der dritten Säule unterstreicht die Europäische Datenschutzkonferenz die folgenden Grundsätze,

noch Anlage 9

die bei dem wichtigen Gesetzgebungsakt Rahmenbeschluss zu beachten sind:

- Zweckbegrenzung: die Notwendigkeit, die gesetzlichen Zwecke genau zu definieren, zu denen die Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen erlaubt ist, ohne irgendwelche Generalklauseln, die die weitere Verarbeitung „für jegliche andere Zwecke“ erlaubt. Das Prinzip der Zweckbegrenzung ist ein Grundsatz in der EU-Richtlinie und in der Konvention 108.

- Datenkategorien: die Verarbeitung besonderer Kategorien von Daten ist verboten, es sei denn besondere Bedingungen werden erfüllt und besondere Garantien werden in der nationalen Gesetzgebung gegeben (Artikel 8 EU-Richtlinie, Artikel 6 Konvention 108). Darüber hinaus sollen angemessene Sicherheitsvorkehrungen für die Verarbeitung biometrischer und genetischer Daten gewährleistet werden.

- Kategorien von Betroffenen: Es ist ein Erfordernis des Verhältnismäßigkeitsgrundsatzes, Unterscheidungen zwischen den verschiedenen Kategorien von Personen wieder einzuführen, die von der Verarbeitung für Polizei und Strafverfolgung betroffen sind.

- Regelung der Weitergabe von Daten an Drittstaaten: Es ist ein Erfordernis des Zweckmäßigkeits-Grundsatzes, dass gemeinsame Kriterien definiert und ein Verfahren geschaffen wird, um den Datenschutz-Standard in einem Drittland oder einer internationalen Einrichtung einschätzen zu können, bevor personenbezogene Daten übertragen werden. Dies soll nicht allein dem Ermessen der Mitgliedstaaten überlassen werden. Die Festlegung eines EU-Standards für ein solches Verfahren ist erforderlich, um Harmonisierung in Europa zu erreichen, und das Prinzip der Feststellung eines angemessenen Datenschutzniveaus entspricht der Regelung durch das Europarats-Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981.

- Benachrichtigung des Betroffenen: Benachrichtigung des Betroffenen soll umfassend sein, einschließlich der Identität der für die Verarbeitung verantwortlichen Stelle, der möglichen Empfänger und der Rechtsgrundlage für die Verarbeitung. Jede Beschränkung soll präzise gefasst und begrenzt sein.

- Auskunftsrecht: Die Regelung zum Auskunftsrecht muss im Einklang mit den Anforderungen der Europäischen Menschenrechtskonvention und der Rechtsprechung stehen. Durch den Ausschluss eines wirksamen Beschwerderechts in einigen Fällen befindet sich der derzeitige Vorschlag nicht im Einklang mit diesen Anforderungen. Darüber hinaus soll die Kontrollinstanz oder das Beschwerdegericht das Recht haben, dem Betroffenen Informationen zu übermitteln, wenn ihm diese ungerechtfertigterweise vorenthalten wurden. Es sollte weniger Ausnahmen vom Auskunftsrecht geben.

- Anzeige und Vorabkontrolle: Anzeige gegenüber und Vorabkontrolle durch die Kontrollinstanz sollten, soweit angemessen, eine Vorbedingung für die Verarbeitung sein. Die Vorabkontrolle soll von den nationalen Datenschutzkontrollinstanzen vorgenommen werden. Die Möglichkeit von Ausnahmen bei der Veröffentlichung der Anzeige sollte je nach Art der Verarbeitung erwogen werden.

- Kontrollinstanzen: Eine Gemeinsame Kontrollbehörde (JSA) soll als unabhängige Kontrollinstanz konzipiert sein. Der Rahmenbeschluss soll Aussagen über deren Zusammensetzung, Aufgaben und Zuständigkeiten enthalten. Sie soll insbesondere mit der Befugnis zu Beratung, Nachforschung und zum Einschreiten ausgestattet sein.

Die Europäische Datenschutzkonferenz anerkennt auch die Wichtigkeit einer möglichst schnellen Verabschiedung des Rahmenbeschlusses. Jedoch wird der derzeit diskutierte Vorschlag keinen ausreichend harmonisierten und hohen Standard des Datenschutzes gewährleisten. Die grundlegende Bedeutung des Rahmenbeschlusses nicht nur für den Schutz der Rechte der Bürger der Europäischen Union, sondern auch für die Strafverfolgung, rechtfertigt eine Diskussion, die nicht durch einen engen Zeitrahmen gefährdet wird.

Die Europäische Datenschutzkonferenz ruft den Rat daher dazu auf, sich mehr Zeit für die Verhandlungen zur Entwicklung eines Rahmenbeschlusses zu nehmen, der einen hohen Datenschutz-Standard bietet.

Die Europäische Datenschutzkonferenz ist bereit, weiter zum Verfahren der Verabschiedung eines solchen Rahmenbeschlusses beizutragen und schlägt eine Anhörung der Arbeitsgruppe des Rates vor, um ihre Standpunkte darzulegen.

Anlage 10 (zu Nr. 13.8)

Erklärung der Europäischen Datenschutzkonferenz vom 16. bis 18. April 2008 in Rom

Die Europäische Union wird in Kürze über verschiedene neue Initiativen zur verbesserten Kontrolle von Reisenden in die Europäische Union und aus der Europäischen Union, diskutieren. Drei von der Kommission vor kurzem verabschiedete Mitteilungen[4] haben zum Ziel, eine solche Diskussion über die nächsten Schritte zum Border Management, sowie über die Schaffung eines Europäischen Grenzüberwachungssystems und über die Bewertung von Frontex in Gang zu bringen.

Zusammen mit den Maßnahmen, die bereits eingeführt wurden oder bald eingeführt werden sollen, und die auf eine verbesserte Überwachung von Reisenden für Grenzkontrollen, Visum-Politik und Strafverfolgungsmaßnahmen abzielen, lassen die aktuellen Mitteilungen deutlich eine Entwicklung in Richtung einer vollständigen Kontrolle und Überwachung von Personen – unabhängig von ihrer Nationalität – die in das Schengen-Gebiet einreisen oder ausreisen, erkennen.

Obwohl ein effizientes Border Management für den Schutz der Union gegen mögliche Bedrohungen notwendig ist, so darf dies niemals in unverhältnismäßiger Weise die Rechte und Freiheiten der Reisenden, und vor allem nicht deren Recht auf Privatsphäre verletzen. Die Überwachung der Reisenden muss wohlbegründet sein und darf nur in Ausnahmefällen gestattet werden, und dies auch nur für berechtigte und besondere Zwecke. Jede allgemeine Überwachung stellt nicht hinnehmbare Risiken für die Freiheit der Einzelnen dar.

Ein anderes Thema, das überdacht werden muss, ist das zu Grunde liegende Konzept, Reisenden zu misstrauen, in dem man ausgewählte „vertrauenswürdige“ Reisende von allen anderen Reisenden isoliert, und die letzteren sogar als potentielle Straftäter erachtet. Das wird eine Durchleuchtung vor und am Eingang beinhalten, so wie die Kontrolle der Grenzüberschreitungen und die automatische Verarbeitung spezieller Daten der Reisenden. Dieses Konzept trägt nicht gerade viel dazu bei, den „symbolischen Effekt, die EU als weltoffen darzustellen“[5], zu verwirklichen, so wie es die Mitteilung der Kommission erwähnt, und es ist sogar fraglich, ob dies mit den Werten der Europäischen Union im Einklang steht.

Die Konferenz hat bereits die Mitglieder der Europäischen Union und die Kommission, den Rat und das Europäische Parlament dazu aufgerufen, zuerst einmal eine Evaluierung zu fertigen, ob die bereits bestehenden rechtlichen Maßnahmen effektiv umgesetzt und durchgeführt werden.[6] Ein neuer Vorschlag sollte nur dann eingebracht werden und wenn klare Hinweise vorliegen, die solche Maßnahmen unterstützen.

Allerdings fand bis jetzt keine solche Bewertung über die Effektivität der Umsetzung der bestehenden rechtlichen Maßnahmen statt. Auch wurden keine verlässlichen Hinweise vorgelegt, die die Notwendigkeit neuer Systeme untermauern. Ebenso wenig wurden Beweise erbracht, die es erforderlich erscheinen lassen, die aktuellen Initiativen auf diesem Gebiet zu ergänzen.

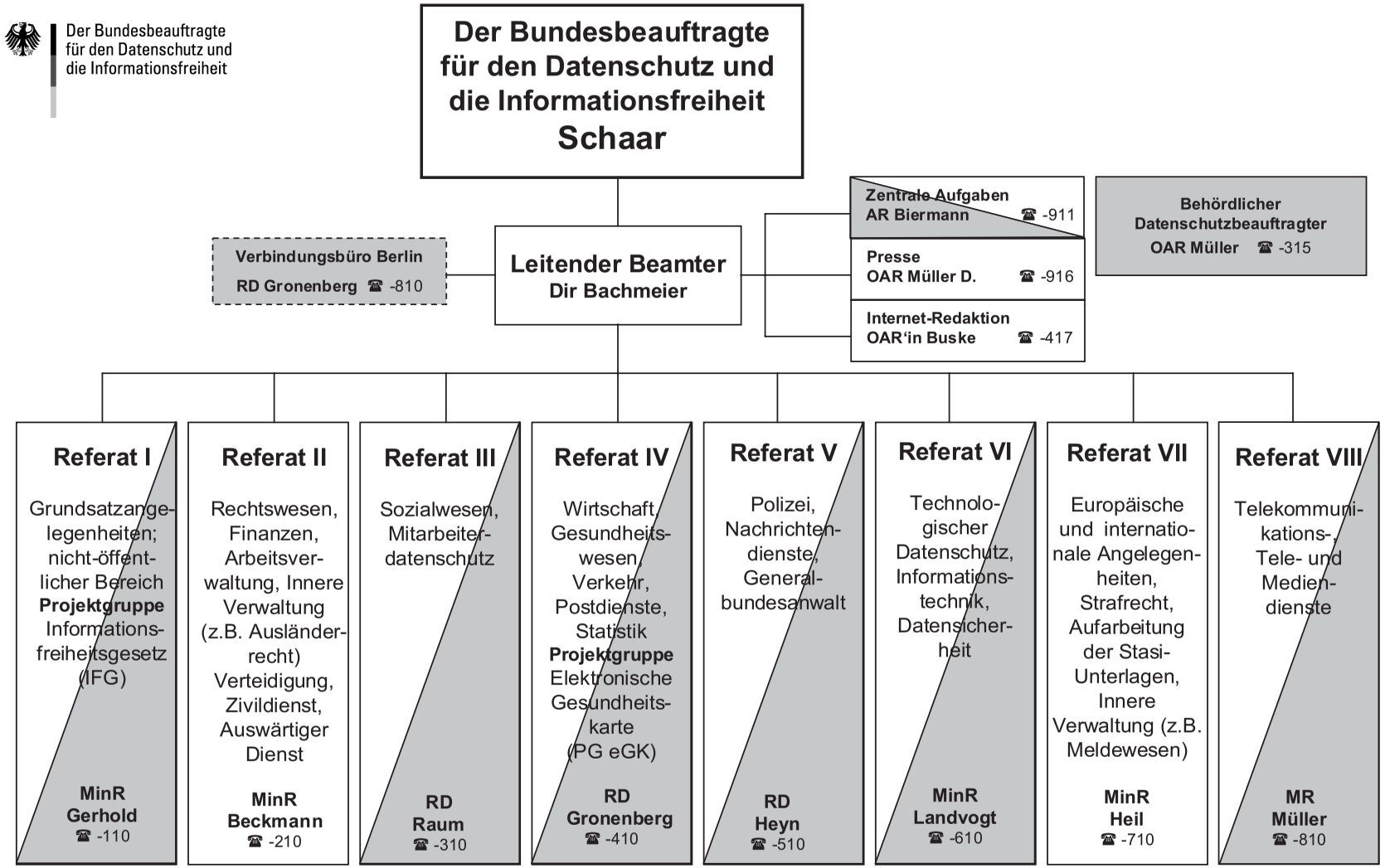
Die von der Kommission vorgelegten Informationen über die geplanten Systeme liefern keinen klaren Beweis für ihre Effektivität. In Bezug auf die direkten und indirekten Kosten im Hinblick auf die Freiheiten und die Bürgerrechte – ganz abgesehen von den finanziellen Aspekten – für die Schaffung neuer Systeme wie zum Beispiel das Einreise-Ausreise-System, sollten auch aussagekräftige Beweise vorliegen, dass dieses System die beste Antwort auf das Problem ist, das es in Angriff nehmen soll.

Da dies anscheinend nicht der Fall ist, ruft die Konferenz die Europäische Union auf, die Notwendigkeit und Verhältnismäßigkeit weiterer Maßnahmen im Lichte der oben erwähnten Kommentare sorgfältig zu überdenken, und zwar vor allem in Bezug auf die in den Mitteilungen der Kommission vorgesehenen Vorschläge.

[4] KOM (2008) 69 endg.
KOM (2008) 68 endg.
KOM (2008) 67 endg.

[5] KOM (2008) 69 endg. Seite 6.

[6] Erklärung von Larnaka über die Verfügbarkeit, Mai 2007


Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Schaar
Verbindungsbüro Berlin
RD Gronenberg ☎ -810
Leitender Beamter
Dir Bachmeier
Zentrale Aufgaben
AR Biermann ☎ -911
Presse
OAR Müller D. ☎ -916
Internet-Redaktion
OAR'in Buske ☎ -417
Behördlicher Datenschutzbeauftragter
OAR Müller ☎ -315
Referat I
Grundsatzangelegenheiten; nicht-öffentlicher Bereich
Projektgruppe Informationsfreiheitsgesetz (IFG)
MinR Gerhold ☎ -110
Referat II
Rechtswesen, Finanzen, Arbeitsverwaltung, Innere Verwaltung (z.B. Ausländerrecht) Verteidigung, Zivildienst, Auswärtiger Dienst
MinR Beckmann ☎ -210
Referat III
Sozialwesen, Mitarbeiterdatenschutz
RD Raum ☎ -310
Referat IV
Wirtschaft, Gesundheitswesen, Verkehr, Postdienste, Statistik
Projektgruppe Elektronische Gesundheitskarte (PG eGK)
RD Gronenberg ☎ -410
Referat V
Polizei, Nachrichtendienste, Generalbundesanwalt
RD Heyn ☎ -510
Referat VI
Technologischer Datenschutz, Informationstechnik, Datensicherheit
MinR Landvogt ☎ -610
Referat VII
Europäische und internationale Angelegenheiten, Strafrecht, Aufarbeitung der Stasi-Unterlagen, Innere Verwaltung (z.B. Meldewesen)
MinR Heil ☎ -710
Referat VIII
Telekommunikations-, Tele- und Mediendienste
MR Müller ☎ -810
Anschriften:
Bonn: Husarenstr. 30, 53117 Bonn
Berlin: Friedrichstr. 50, 10117 Berlin
Telefon: 0228 / 997799-0
Fax: 0228 / 997799-550
E-Mail: poststelle@bfdi.bund.de
Internet: www.bfdi.bund.de
Legende:
Aufgaben werden in Bonn wahrgenommen
Aufgaben werden in Berlin wahrgenommen
Stand: April 2009

Sachregister

Als Fundstelle ist die Nummer des Abschnitts oder des Beitrages angegeben, in dem der Begriff verwendet wird.

Abkürzungsverzeichnis/Begriffe

AA	Auswärtiges Amt
a. a. O	am angegebenen Orte
ABl.	Amtsblatt der Europäischen Gemeinschaften
ABMG	Autobahnmautgesetz
Abs.	Absatz
AFIS	Automatisches Fingerabdruck-Identifizierungssystem
AG	Aktiengesellschaft, aber auch: Arbeitsgruppe
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
ALG II	Arbeitslosengeld II
Alt.	Alternative
AO	Abgabenordnung
API	Advance passenger information
ARGE	Arbeitsgemeinschaften nach dem Sozialgesetzbuch II
Art.	Artikel
ATDG	Antiterrordateigesetz
AufenthG	Aufenthaltsgesetz
AufenthV	Aufenthaltsverordnung
AuslG	Ausländergesetz
AVV	Allgemeine Verwaltungsvorschrift
AWG	Außenwirtschaftsgesetz
Az.	Aktenzeichen
AZR	Ausländerzentralregister
AZRG	Gesetz über das Ausländerzentralregister
BA	Bundesagentur für Arbeit
BAC	Basic Access Control
BaFin	Bundesanstalt für Finanzdienstleistungen
BAföG	Bundesausbildungsförderungsgesetz
BAG	Bundesamt für Güterverkehr
BAköV	Bundesakademie für öffentliche Verwaltung
BAMF	Bundesamt für Migration und Flüchtlinge
BAN	Bundespolizeiaktennachweis
BArchG	Bundesarchivgesetz
BAZ	Bundesamt für den Zivildienst
BBG	Bundesbeamtengesetz
BCR	Binding Corporate Rules; verbindliche unternehmensinterne Datenschutzregelungen
bDSB	behördlicher Datenschutzbeauftragter
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

BfD/BA	Beauftragter für den Datenschutz der Bundesanstalt für Arbeit
BfJ	Bundesamt für Justiz
BfV	Bundesamt für Verfassungsschutz
BGBl.	Bundesgesetzblatt
BKA	Bundeskriminalamt
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
Bluetooth	Standard für die drahtlose Übermitlung von Sprache und Daten im Nahbereich
BMAS	Bundesministerium für Arbeit und Soziales
BMF	Bundesministerium der Finanzen
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BMVBW	Bundesministerium für Verkehr, Bau- und Wohnungswesen
BMVg	Bundesministerium der Verteidigung
BMWi	Bundesministerium für Wirtschaft und Technologie
BND	Bundesnachrichtendienst
BNDG	Gesetz über den Bundesnachrichtendienst
BPol	Bundespolizei
BPolG	Bundespolizeigesetz
BR	Bundesrat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStU	Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BT	Bundestag
BVA	Bundesverwaltungsamt, aber auch: Bundesversicherungsamt
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfSchG	Bundesverfassungsschutzgesetz
BVerwG	Bundesverwaltungsgericht
BVV	Bundesvermögensverwaltung
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
BZSt	Bundeszentralamt für Steuern
bzw.	beziehungsweise
ca.	circa
CC	Common Criteria
CD/CD-ROM	Compact Disc - Read Only Memory
DB	Deutsche Bahn
d. h.	das heißt

DDR	Deutsche Demokratische Republik
DMP	Disease-Management-Programme
DNA	Desoxyribonoclein acid (acid=Säure)
Dok.	Dokument
DRM	Digital Rights Management (Digitales Rechte Management)
Drs.	Drucksache
Düsseldorfer Kreis	Koordinierungsgremium der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich
DV/dv	Datenverarbeitung
EAC	Extended Access Controll
e. V.	eingetragener Verein
E-Commerce	Elektronic Commerce/Elektronischer Handel
ED	Erkennungsdienst
EDPS	Europäischer Datenschutzbeauftragter
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft(en)
EG-ZIS	Europäisches Zollinformationssystem
EHUG	Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister
EJG	Eurojust-Gesetz
ELENA	Elektronischer Einkommensnachweis (JobCardverfahren)
ELSTER	Elektronische Steuererklärung
E-Mail	Electronic Mail
EP	Europäisches Parlament
E-PA	Elektronischer Personalausweis
EPOS	Elektronisches Personal-, Organisations- und Stellenmanagement-System
EstG	Einkommensteuergesetz
ETB	Elektronisches Tagebuch
etc.	ecetera
eTIN	Lohnsteuerliches Ordnungsmerkmal
EU	Europäische Union
EuGH	Europäischer Gerichtshof
Eurodac	Europäisches daktyloskopisches Fingerabdrucksystem zur Identifizierung von Asylbewerbern
EUROPOL	Europäisches Polizeiamt
EVN	Einzelverbindungsnachweis
EWG	Europäische Wirtschaftsgemeinschaft
EWR	Europäischer Wirtschaftsraum
f.	folgend
FDZ	Forschungsdatenzentrum
ff.	folgende
FH Bund	Fachhochschule des Bundes für öffentliche Verwaltung

FIDE	automatisiertes Aktennachweissystem im Zollbereich
FIFA	Fédération Internationale de Football Association
FIU	Financial Intelligence Unit
FKS	Finanzkontrolle Schwarzarbeit
FVG	Finanzverwaltungsgesetz
G.10	Artikel 10 Gesetz
GBA	Generalbundesanwalt beim Bundesgerichtshof
gem.	gemäß
GFG	Gemeinsame Finanzermittlungsgruppe
GG	Grundgesetz
ggf.	gegebenenfalls
GGO	Gemeinsame Geschäftsordnung der Bundesministerien
GK	Gemeinsame Kontrollinstanz von Europol
GKI	Gemeinsame Kontrollinstanz von Schengen
GKV	Gesetzliche Krankenversicherung
GKV-WSG	Gesetz zur Stärkung des Wettbewerbs in der Gesetzlichen Krankenversicherung
GmbH	Gesellschaft mit beschränkter Haftung
GMBl	Gemeinsames Ministerialblatt
GMG	Gesetz zur Modernisierung der gesetzlichen Krankenversicherung
GTAZ	Gemeinsames Terrorismusabwehrzentrum
GwG	Geldwäschegesetz
HKP	häusliche Krankenpflege
HPC	Health Professional Card
html	Hypertext Markup Language-Standardisierte Seitenbeschreibungssprache für Seiten im Internet/Intranet
HVBG	Hauptverband der gewerblichen Berufsgenossenschaften
IATA	International Air Transport Association
i. d. F.	in der Fassung
i. S. d.	im Sinne des (der)
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
ICAO	International Civil Aviation Organization
ICHEIC	International Commission on Holocaust Era Insurance Claims
IFG	Informationsfreiheitsgesetz
IFOS-Bund	Interaktives Fortbildungssystem für die Bundesverwaltung
IHK	Industrie- und Handelskammer
IKPO	Internationale Kriminalpolizeiliche Organisation
ILO	International Labour Organization
IMK	Ständige Konferenz der Innenminister und -senatoren der Länder

IMSI	International Mobile Subscriber Identity
InGe	Integrationsdatei
INPOL	Informationssystem der Polizei
InsO	Insolvenzordnung
INZOLL	Informationssystem der Zollverwaltung
IP	Internet Protocol
IPR	Internationales Privatrecht
IPSec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
IT	Informationstechnik
IVBB	Informationsverbund Berlin-Bonn
JI-Rat	Rat der Innen- und Justizminister der Europäischen Union
KBA	Kraftfahrt-Bundesamt
KFU	Krebsfrüherkennungsrichtlinien
Kfz	Kraftfahrzeug
KOM	Europäische Kommission
KWG	Kreditwesengesetz
LAN	Local Area Network
LfD	Landesbeauftragter für den Datenschutz
lit.	litera (=Buchstabe)
LKA/LKÄ	Landeskriminalamt/Landeskriminalämter
LuftSiG	Gesetz zur Neuregelung von Luftsicherheitsaufgaben (Luftsicherheitsgesetz)
m. E.	meines Erachtens
MAD	Militärischer Abschirmdienst
MADG	Gesetz über den MAD
MDK	Medizinischer Dienst der Krankenversicherung
MRRG	Melderechtsrahmengesetz
MZG	Mikrozensusgesetz
NADIS	Nachrichtendienstliches Informationssystem
Nr.	Nummer
o. a.	oben aufgeführt
o. g.	oben genannt
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OFD	Oberfinanzdirektion
OK	Organisierte Kriminalität, aber auch: Organisationskomitee

OLAF	Europäisches Amt für Betrugsbekämpfung
PassG	Passgesetz
PAVOS	Polizeiliches Auskunfts- und Vorgangsbearbeitungssystem (beim BGS)
PC	Personalcomputer
PersauswG	Personalausweisgesetz
PKGr	Parlamentarisches Kontrollgremium
PNR	Passenger Name Record
Protection Profile	Schutzprofil
Ratsdok.	Ratskokument (EU)
Rdn.	Randnummer
Reha	Rehabilitation
RFID	Radio Frequency Identification – Transpondertechnik für die berührungslose Erkennung von Objekten
RFID-Chip	Radio Frequency Identification-Chip (Funkchip)
RSAV	Risikostrukturausgleichsverordnung
RVOrgG	Organisationsreform in der gesetzlichen Rentenversicherung
S.	Seite
s.	siehe
s. o.	siehe oben
s. u.	siehe unten
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
SchwarzArbG	Schwarzarbeitsbekämpfungsgesetz
SDÜ	Schengener Durchführungsübereinkommen
SG	Soldatengesetz
SGB	Sozialgesetzbuch
SGB I	Sozialgesetzbuch Erstes Buch (Allgemeiner Teil)
SGB II	Sozialgesetzbuch Zweites Buch (Grundsicherung für Arbeitssuchende)
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 VIII	Sozialgesetzbuch Achtes Buch (Kinder- und Jugendhilfe)
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)
SGB XII	Sozialgesetzbuch Zwölftes Buch (Sozialhilfe)
SigG	Signaturgesetz
SIS	Schengener Informationssystem

SMS	Short Message Service
sog.	so genannt
Stasi	Staatssicherheitsdienst der ehemaligen DDR
StDAV	Steuerdaten-Abruf-Verordnung
StDÜV	Steuerdatenübermittlungsverordnung
Steuer-ID	Identifikationsnummer für steuerliche Zwecke (steuerliches Identifikationsmerkmal/-nummer)
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StUG	Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz)
StVBG	Steuerverkürzungsbekämpfungsgesetz
StVergAbG	Steuervergünstigungsabbaugesetz
StVollzG	Strafvollzugsgesetz
SDDSG	Suchdienstedatenschutzgesetz
SÜFV	Sicherheitsüberprüfungsfeststellungsverordnung
SÜG	Sicherheitsüberprüfungsgesetz
TB	Tätigkeitsbericht
TBG	Terrorismusbekämpfungsgesetz
TC	Trusted Computing
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TOP	Tagesordnungspunkt
TPM	Trusted Platform Module
u. a.	unter anderem
u. ä.	und ähnliches
u. U.	unter Umständen
UIG	Umweltinformationsgesetz
UMTS	Universal Mobile Telecommunications System
UrhG	Urheberrechtsgesetz
US	United States
USB	Universal Serial Bus – eine Schnittstelle am PC
UStG	Umsatzsteuergesetz
usw.	und so weiter
VAM	Virtueller Arbeitsmarkt
VBM	vorläufiges Bearbeitungsmerkmal
VdAK	Verband der Angestellten-Krankenkassen
VDR	Verband Deutscher Rentenversicherungsträger
VG	Verwaltungsgericht
vgl.	vergleiche

VS	Verschlusssache
VIS	Visa-Informationssystem
vpS	Vorbeugender personeller Sabotageschutz
WiMax	Wordwide Interoperability for Microwave Access Standard gemäß IEEE 802.16a für lokale Funknetze
WM	Weltmeisterschaft
WP	Working Paperd/Arbeitspapier
www	World wide web
XML	Extensible Markup Language
z. B.	zum Beispiel
z. T.	zum Teil
ZAG	Zentren für Arbeit und Grundsicherung
ZDG	Zivildienstgesetz
ZIS	Zollinformationssystem
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister

Tätigkeitsbericht	Berichtszeitraum	Bundestagsdrucksachennummer
1.	1978	8/2460
2.	1979	8/3570
3.	1980	9/93
4.	1981	9/1243
5.	1982	9/2386
6.	1983	10/877
7.	1984	10/2777
8.	1985	10/4690
9.	1986	10/6816
10.	1987	11/1693
11.	1988	11/3932
12.	1989	11/6458
13.	1990	12/553
14.	1991 – 1992	12/4805
15.	1993 – 1994	13/1150
16.	1995 – 1996	13/7500
17.	1997 – 1998	14/850
18.	1999 – 2000	14/5555
19.	2001 – 2002	15/888
20.	2003 – 2004	15/5252
21.	2005 – 2006	16/4950