BERICHT

des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2004

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen (§§ 29 Berliner Datenschutzgesetz, 18 Abs. 3 Berliner Informationsfreiheitsgesetz). Der vorliegende Bericht schließt an den ***am 30. März 2004*** *vorgelegten Jahresbericht 2003 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2004 ab.*

Wiederum werden die über Berlin hinaus bedeutsamen Dokumente in einem gesonderten Anlagenband („Dokumente zu Datenschutz und Informationsfreiheit 2004“) veröffentlicht, der gemeinsam mit dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg herausgegeben wird.

Dieser Jahresbericht ist über das Internet ***(http://www.datenschutz-berlin.de)*** *abrufbar; wir bemühen uns, dort alle im Bericht zitierten Fundstellen zugänglich zu machen.*

Impressum

Herausgeber: Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4 – 10, 10787 Berlin
Telefon: (0 30) + 1 38 89-0
Telefax: (0 30) 2 15 50 50
E-Mail: mailbox@datenschutz-berlin.de
Internet: http://www.datenschutz-berlin.de

Redaktion: Laima Nicolaus

Druck: Druckerei Conrad GmbH

Inhaltsverzeichnis

1. Entwicklung des Datenschutzrechts

1.1 Deutschland und Europa

Rechtsprechung

Sowohl in Deutschland als auch in Europa hat der Datenschutz im vergangenen Jahr seine größten Impulse von der Rechtsprechung erfahren.

Ohne Zweifel stellt das Urteil des *Bundesverfassungsgerichts* zur *akustischen Wohnraumüberwachung („Großer Lauschangriff")* vom 3. März 2004[1] neben dem Volkszählungsurteil den größten verfassungsrechtlichen Meilenstein in der Entwicklung der informationellen Selbstbestimmung dar. Über die Feststellung hinaus, dass wesentliche Regelungen der Strafprozessordnung hierzu verfassungswidrig sind, werden Grundsätze zum Kernbereich privater Lebensgestaltung festgelegt, die in ihrer Bestimmtheit nicht zu übertreffen sind. So formuliert das Gericht im zweiten Leitsatz:

> *„Zur Unantastbarkeit der Menschenwürde gemäß Art. 1 Abs. 1 GG gehört die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung. In diesen Bereich darf die akustische Überwachung von Wohnraum zu Zwecken der Strafverfolgung (Art. 13 Abs. 3 GG) nicht eingreifen. Eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes zwischen der Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und dem Strafverfolgungsinteresse findet insoweit nicht statt."*

Die Auswirkungen sind nicht auf die Regelungen zur akustischen Wohnraumüberwachung selbst beschränkt. Vielmehr werden auch alle anderen ähnlich tief in das informationelle Selbstbestimmungsrecht eingreifenden strafprozessualen und sicherheitsrechtlichen Maßnahmen zu überprüfen sein[2]. Aber auch in anderen Lebensbereichen muss der Schutz des Kernbereichs der Lebensgestaltung neu überdacht werden.

Auch die Regelungen des *Außenwirtschaftsgesetzes* zur Telefon- und Postüberwachung durch das Zollkriminalamt wurden am gleichen Tag vom Bundesverfassungsgericht für verfassungswidrig erklärt[3]. Hier rügte das Gericht vor allem den mangelnden Rechtsschutz für die Betroffenen und unzureichende Regelungen für die Verarbeitung der Daten.

Obwohl bereits im November 2003 entschieden, löste ein Urteil des *Europäischen Gerichtshofs* im vergangenen Jahr heftige Debatten über die Reichweite der Europäischen Datenschutzrichtlinie aus[4]. Eine schwedische Katechetin hatte personenbezogene Daten über Arbeitskollegen ohne deren Ein-

1 1 BvR 2378/98

2 vgl. 4.3.1

3 Beschluss vom 3. März 2004, 1 BvF 3/92

4 Urteil vom 6. November 2003, Rs C-101/01

willigung auf eine Website gestellt und daraufhin von einem Gericht eine Geldstrafe auferlegt bekommen. Das Gericht stellte klar, dass die Veröffentlichung personenbezogener Daten im *Internet* eine automatisierte Verarbeitung von Daten darstellt und damit Privilegien für andere Datenverarbeitungsformen nicht gelten. Allerdings liegt in der Einstellung personenbezogener Daten in das Internet keine Datenübermittlung in Drittstaaten, selbst wenn diese von dort abgerufen werden können. Und schließlich geht die Meinungsfreiheit dem Grundrecht auf informationelle Selbstbestimmung nicht vor (und umgekehrt auch nicht), beide Grundrechte sind miteinander in einen ausgewogenen Gleichklang zu bringen. Bereits früher im Jahr 2003 hatte der EuGH eine Entscheidung gefällt, nach der auch der Rechnungshof der Datenschutzrichtlinie (und damit den nationalen Datenschutzgesetzen) sowie dem Erforderlichkeitsprinzip unterliegt. Einzelne Bürgerinnen und Bürger in den Mitgliedstaaten könnten sich unmittelbar auf die Datenschutzrichtlinie stützen, wenn sie die Anwendung entgegenstehenden nationalen Rechts verhindern wollen[5]. Die Entscheidungen, denen demnächst weitere folgen werden, zeigen, dass sich der Europäische Gerichtshof intensiv um die Fortentwicklung des Datenschutzes in Europa müht.

Zu einer ungewöhnlichen Kontroverse zwischen dem Bundesverfassungsgericht und dem *Europäischen Gerichtshof für Menschenrechte* (EuGMR) kam es bei der Frage, wie weit die geschützten *Persönlichkeitsrechte von Prominenten* gegenüber der *Presse* reichen. Prinzessin Caroline von Hannover (vormals Monaco) hatte gegen einige Illustrierte auf Schadensersatz geklagt, die Bilder von ihr, ihren Partnern und ihren Kindern bei privaten Handlungen zeigten. Das Bundesverfassungsgericht hatte im Dezember 1999 zwar die Veröffentlichung der Bilder, auf denen die Kinder der Prinzessin zu sehen waren, untersagt, da Kinder schutzwürdiger seien als Erwachsene. Die Prinzessin selbst dagegen müsse die Veröffentlichung von Fotos hinnehmen, auch wenn sie ihr privates Alltagsleben betreffen, da sie eine „absolute Person der Zeitgeschichte“ sei[6]. Der EuGMR relativierte diese Entscheidung: Er stellte nicht kategorisch darauf ab, ob es sich um eine Person der Zeitgeschichte handele (was im übrigen ebenfalls bezweifelt wurde, da Prinzessin Caroline keine öffentlichen Ämter wahrnehme), sondern darauf, inwieweit die veröffentlichten Fotos zu einer Debatte beitragen, für die ein Allgemeininteresse geltend gemacht werden kann. Dies sei hier nicht der Fall gewesen, die Öffentlichkeit könne kein legitimes Interesse daran geltend machen zu erfahren, wo sich die Prinzessin aufhält und wie sie sich allgemein in ihrem Privatleben verhält. Jede Person, auch wenn es sich um eine Persönlichkeit des öffentlichen Lebens handele, dürfe die „legitime Erwartung“ hegen, dass ihr Privatleben geschützt und geachtet wird[7]. Die Entscheidung ist von der deutschen Presse heftig kritisiert worden, die Bundesregierung hat es jedoch abgelehnt, gegen die Entscheidung Rechtsmittel einzulegen.

5 Urteil vom 20. Mai 2003, Rs C-145/00

6 1 BvR 653/96

7 Urteil vom 24. Juni 2004, Beschwerde Nr. 59320/00

Bundesrecht

Die Umsetzung des Vierten Gesetzes für moderne Dienstleistungen am Arbeitsmarkt vom 24. Dezember 2003 (*„Hartz IV“*) – ein wahres Weihnachtsgeschenk – stand im Laufe des Jahres im Mittelpunkt unserer Aktivitäten. Um die Umstellung dieses erheblichen Teils des Sozialsystems zum 1. Januar 2005 zu ermöglichen, wurden hektische Aktivitäten entfaltet, die vielfach die gebotene Rücksicht auf Belange des Datenschutzes vermissen ließen[8].

Nach der Behebung der technischen Mängel stand zum 1. Januar 2005 auch die Umsetzung des Gesetzes über die Erhebung von streckenbezogenen Gebühren für die Benutzung von Bundesautobahnen mit schweren Nutzfahrzeugen (*Autobahnmautgesetz* – ABMG) an. Trotz gesetzlicher Zweckentfremdungsverbote entstand hier eine Informationsinfrastruktur, die für die informationelle Selbstbestimmung vielerlei Risiken birgt[9].

Ein weiteres wichtiges Gesetzgebungsvorhaben des Bundes war die Neufassung des *Telekommunikationsgesetzes*, die unter anderem wegen der Europäischen Kommunikationsrichtlinie von 2002 erforderlich war[10]. Die bisher in einer eigenen Verordnung enthaltenen Datenschutzbestimmungen wurden nunmehr in das Gesetz selbst integriert[11]. Wesentliche zukunftsweisende Regelungen betreffen die Verarbeitung von Standortdaten beim Mobiltelefon, die künftig die Basis für vielerlei Mehrwertdienste sein werden. Verhindert werden konnte eine Verpflichtung der Telekommunikationsunternehmen, Verkehrsdaten über eine bestimmte Zeit auch dann für die Strafverfolgung zu speichern, wenn sie für Telekommunikationszwecke nicht oder nicht mehr benötigt werden.

In Kraft getreten ist auch eine Bestimmung im Gesetz gegen den unlauteren Wettbewerb, nach dem das unaufgeforderte *elektronische Zusenden von Werbung* grundsätzlich verboten ist[12].

Vor dem zunehmenden Missbrauch von *Kameratelefonen* durch heimliche Aufnahmen häufig indiskreten Charakters wurde in das Strafgesetzbuch eine Bestimmung eingefügt, nach der sich strafbar macht, wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt (§ 201 a). Auch diese Bestimmung ist von der Presse heftig kritisiert worden, da man zu Unrecht eine Beschränkung des investigativen Journalismus befürchtete[13].

8 vgl. 3.1

9 vgl. 4.2.2

10 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der Kommunikation, ABl. EG L 201/37

11 vgl. 5.1

12 vgl. 4.6.4, 5.1

13 vgl. 5.1

Das Bundesdatenschutzgesetz (BDSG) vom 18. Mai 2001[14] ist auch hinsichtlich der Altverfahren am 23. Mai 2004 in vollem Umfang in Kraft getreten. Dieses Datum hat eine Reihe hektischer Reaktionen ausgelöst, insbesondere was die Verpflichtung zur Bestellung betrieblicher Datenschutzbeauftragter betrifft – obwohl diese Verpflichtung nicht nur seit 2001, sondern von Beginn der Datenschutzgesetzgebung im Bund an besteht.

Die beiden in Zusammenhang mit dem BDSG 2001 diskutierten Projekte eines *Auditgesetzes* (vgl. § 9 a BDSG) sowie einer grundsätzlichen Modernisierung des Datenschutzes durch ein *BDSG „zweiter Stufe"*[15] sind im vergangenen Jahr nicht vorangekommen, obwohl sie Bestandteil der Koalitionsvereinbarungen sind. Bewegung hat es dagegen bei dem Entwurf eines Informationsfreiheitsgesetzes des Bundes gegeben. Gegen den Widerstand der Ministerialbürokratie haben die Regierungsfraktionen Ende 2004 einen Entwurf in den Bundestag eingebracht, der Anfang 2005 beraten und beschlossen werden soll[16].

Europäische Entwicklung

Der Entwurf einer *Verfassung für Europa*, der am 29. Oktober 2004 in Rom von den Staats- und Regierungschefs feierlich unterzeichnet wurde, ist auch ein Meilenstein in der Geschichte des europäischen Datenschutzes. Als einziges Grundrecht wird es sowohl im Teil I, der eigentlichen Verfassung (Art. I-51), als auch in Teil II, der Charta der Grundrechte der Union (Art. II-68), verankert. Neu ist die Befugnis, durch Europäisches Gesetz oder Rahmengesetz den Datenschutz sowohl für die Gemeinschaftsorgane als auch für die Mitgliedstaaten zu regeln (Art. I-51 Abs. 2). Die Überwachung durch unabhängige Behörden wird gewährleistet.

Die europäischen Gremien haben wiederum eine Vielzahl von Aktivitäten auf dem Gebiet des Datenschutzes entfaltet.

Sehr umstritten ist die Kommissionsentscheidung vom 14. Mai 2004 zur Übermittlung von *Flugpassagierdaten* in die USA, die die dortigen Grenz- und Sicherheitsbehörden aufgrund der Gesetzgebung nach dem 11. September 2001 von den europäischen Fluggesellschaften verlangen. Sie schafft zusammen mit einem Ratsbeschluss über ein bilaterales Abkommen mit den USA aus der Sicht der Kommission eine hinreichende Rechtsgrundlage; ebenso soll sie die Angemessenheit des Schutzes der Passagierdaten in den USA sichern. Das Europäische Parlament, das wie die Datenschutzbeauftragten diese Auffassung nicht teilt, hat gegen die Kommissionsentscheidung den Europäischen Gerichtshof angerufen[17].

14 nunmehr in der Fassung der Bekanntmachung vom 14. Januar 2003, BGBl. I, S. 66

15 Roßnagel, Alexander; Pfitzmann, Andreas; Garstka, Hansjürgen: Modernisierung des Datenschutzrechts. Berlin: Bundesministerium des Innern, 2001

16 vgl. 4.9.1

17 vgl. 4.7.1

Eine andere Entscheidung der Kommission betrifft *Standardvertragsklauseln* zur Gewährleistung hinreichender Datenschutzgarantien in Drittländern. Zu den bereits bestehenden Standardklauseln hatten Wirtschaftsverbände wie die Internationale Handelskammer Alternativvorschläge entwickelt, da sie die bisherigen Regelungen für zu starr empfanden. Mit Entscheidung vom 15. Juni 2004 wurden diese alternativen Standardklauseln als gleichberechtigt anerkannt[18].

Ein erhebliches Arbeitspensum hat erneut die Arbeitsgruppe zum Schutz personenbezogener Daten nach Art. 29 der Datenschutzrichtlinie, die aus den nunmehr 25 Datenschutzbehörden der Mitgliedstaaten, dem Europäischen Datenschutzbeauftragten und der Kommission besteht, hinter sich gebracht. Im Jahr 2004 wurden fast 20 Arbeitspapiere zu den verschiedensten Themenbereichen verabschiedet.

Weitere Fortschritte hat die Zusammenarbeit der Datenschutzbehörden bei der Anerkennung *verbindlicher Unternehmensregelungen* gemacht. Die bis dahin nur von wenigen Behörden diskutierten Verfahrensregelungen wurden nunmehr auch in der Art. 29-Gruppe erörtert mit dem Ziel, ein abgestimmtes Verfahren der Prüfung einschließlich einer von allen zugrunde zu legenden Checklist zu entwickeln[19].

1.2 Berlin

Nachdem das erste Gesetz über den Datenschutz in der Berliner Verwaltung (Berliner Datenschutzgesetz – BlnDSG) am 22. Juli 1978 in Kraft getreten war, dauerte es weit über ein Jahr, bis der erste Berliner Datenschutzbeauftragte Dr. Hans-Joachim Kerkau am 1. November 1979 sein Amt antrat. Somit war im November vergangenen Jahres das 25-jährige Bestehen unserer Dienststelle zu feiern. Dies nahmen wir zum Anlass für eine Reihe von Aktivitäten, die den hohen Stellenwert belegten, den der Datenschutz im Land Berlin besitzt.

Die Datenschutzgesetzgebung in Berlin konzentrierte sich auf einzelne spezialrechtliche Regelungen.

Aufgrund kritischer Stellungnahmen, die wir in den vergangenen Jahren vorgelegt hatten, sowie parlamentarischer Initiativen wurde das Allgemeine Sicherheits- und Ordnungsgesetz (*ASOG*) in zwei datenschutzrechtlich relevanten Punkten geändert: Die *Schleierfahndung*, die sich als untaugliches Fahndungsmittel erwiesen hat und auf deren Bedenklichkeit die Datenschutzbeauftragten seit jeher hingewiesen hatten, wurde wieder abgeschafft. Die Vorschriften zur *Rasterfahndung*, die sich im Vorjahr ebenfalls als verbesserungsbedürftig erwiesen hatten, wurden in einigen Punkten präzisiert,

18 vgl. 4.7.1

19 vgl. 4.7.1

wenn auch unserer Forderung nach frühester Information unserer Dienststelle über eine bevorstehende Rasterfahndung nicht entsprochen wurde[20].

Das im November 2003 beschlossene Gesetz über die Einrichtung eines Zentralen *Personalüberhangmanagements* ist am 1. Januar 2004 in Kraft getreten und regelt den Übergang der Personalüberhangkräfte der Berliner Verwaltung zum Zentralen Personalüberhangmanagement (ZeP) durch Einzelversetzungen. Wir hatten in letzter Minute deutliche datenschutzrechtliche Verbesserungen erreichen können. Seit Frühjahr 2004 werden die Bediensteten in den Stellenpool versetzt, um von dort aus anderen Verwendungen zugeführt zu werden.

Ein aufwändiges Pseudonymisierungkonzept wird die mit dem Gesetz über die Statistik der Personalstruktur und der Personalkosten im unmittelbaren Landesdienst (*Personalstrukturstatistikgesetz* – PSSG) vom 2. Dezember 2004 einzurichtende landesübergreifende Personalstatistik kennzeichnen. In jahrelangen intensiven Gesprächen konnte eine datenschutzgerechte Ausgestaltung dieses ehrgeizigen Projekts erreicht werden, die bundesweit ihresgleichen sucht[21].

In Zusammenhang mit der Umsetzung des Professorenbesoldungsreformgesetzes ebenfalls mit Gesetz vom 2. Dezember 2004 wurden die Bestimmungen über die Verarbeitung personenbezogener Daten in der *Hochschule* neu gefasst. Sie enthalten nun eine Vollregelung, die es den Hochschulangehörigen gestattet, alle einschlägigen Vorschriften an einer einzigen Stelle im Hochschulgesetz zu finden[22].

Auch das neue *Schulgesetz* vom 26. Januar 2004 enthält eine Vielzahl von Regelungen zum Datenschutz in der Schule, die allerdings durch Rechtsverordnungen und Ausführungsvorschriften noch umgesetzt werden müssen. Dieser Prozess ist noch im Gange[23].

Mit dem *Hundegesetz* vom 23. September 2004 ging eine jahrelange Debatte über einen angemessenen gesetzlichen Schutz vor gefährlichen Hunden vorläufig zu Ende. Bereits zu früheren Entwürfen hatten wir eine Reihe von Vorschriften zum Schutz personenbezogener Daten der Hundehalter gemacht. Sie sind nunmehr in das Gesetz eingeflossen. Neu ist die Verpflichtung, künftig in jeden Hund einen Chip zu implantieren, der der Identifizierung des Tieres dient. Trotz Verabschiedung des Gesetzes ist weiterer Regelungsbedarf zum Umgang mit den Chipdaten allseits anerkannt[24].

20 vgl. 4.1.1
21 vgl. 4.5.2
22 vgl. 4.5.1
23 vgl. 4.5.3
24 vgl. 4.4.2

2. Technische Rahmenbedingungen

2.1 Entwicklung der Informationstechnik

Entwicklungstrends

Wie immer wollen wir an dieser Stelle darüber berichten, welche auffälligen Entwicklungstrends in der Informations- und Kommunikationstechnik im Berichtsjahr zu beobachten waren. Natürlich ist es nicht so, dass es zu dem Thema in jedem Jahr neue Überraschungen gibt. Die Trends halten über lange Jahre an, viele folgen offenkundigen Gesetzmäßigkeiten.

Das Gesetz des Intel-Mitbegründers Gordon Moore aus dem Jahr 1965 besagt, dass sich die Leistungsfähigkeit von Mikroprozessoren alle 18 Monate verdoppelt, wobei die Kosten sich im Wesentlichen nicht verändern. Das Gesetz lässt sich ebenfalls anwenden auf die Speichertechnologien und auf die Übertragungsgeschwindigkeiten in Computernetzen. Das Gesetz hat sich seit mindestens 30 Jahren als gültig erwiesen und man geht davon aus, dass es so lange weiter gilt, bis in etwa 20 Jahren die Größe der Schaltkreise auf Atom- bzw. Molekülgröße geschrumpft ist. Erst dann könnten neue Technologieformen wie z. B. die Quantentechnologie neue Wachstumsformeln nötig machen.

Mikroprozessoren werden kontinuierlich schneller, kleiner und billiger. Die darauf aufbauenden Systeme wie z. B. Computer und Handys machen diese Entwicklung mit. Die Vielfalt der Systeme profitiert von der Reduzierung des Energieverbrauchs, von der Erfindung neuer Materialien, die das Siliziummonopol bei der Entwicklung neuer Prozessorformen und Speichertechnologien aufbrechen könnten[25].

Die immer reichhaltiger werdenden Anwendungsformen der Informations- und Kommunikationstechnik profitieren von der steigenden Fähigkeit zur Kommunikation untereinander, insbesondere davon, dass die Verfahren zur drahtlosen Kommunikation permanent fortentwickelt werden.

Mikroprozessoren und Systeme, die auf ihnen aufbauen, durchdringen zunehmend den Alltag. Selbst wenn man den kommerziellen Sektor nicht mitrechnet, dürften längst auf jeden Einwohner eines entwickelten Landes Dutzende von Mikroprozessoren entfallen: Der PC zu Hause, der moderne Festanschluss für das Telefon, das Handy für unterwegs, die Chipkarten in unserer Brieftasche, die elektronisch gesteuerten Haushaltsgeräte, die elektronischen Steuerungssysteme in modernen Kraftfahrzeugen, die Unterhaltungselektronik und digitale Fotoapparate enthalten Mikroprozessoren und Speichermedien der vielfältigsten Art.

25 z. B. die Polymerelektronik, die bis Ende 2004 ein Förderschwerpunkt des Bundesministeriums für Bildung und Wissenschaft war

Diese Systeme beginnen miteinander zu kommunizieren, ohne dass dies vom Menschen unmittelbar veranlasst wird. So sollen z. B. die Kommunikationsmöglichkeiten in modernen *Kraftfahrzeugen* besonders gefördert werden: Sechs große europäische Autohersteller arbeiten in einem Projekt mit zwei großen Elektronikherstellern und dem Berliner Fraunhofer-Institut für offene Kommunikationssysteme an einem gemeinsamen Programm zur Kommunikation zwischen Fahrzeugen über Ad-hoc-Netze. Dieses Projekt wird vom Bundesministerium für Bildung und Wissenschaft gefördert. Fahrzeuge könnten dann automatisch andere Fahrzeuge und deren Fahrer vor Gefahrenstellen wie Glatteis, Unfällen oder Staus warnen.

Die Welt der kabellosen Helfer – das Internet der Dinge

Wem ist es nicht schon passiert: Die Ware wurde an der Kaufhauskasse bezahlt, sorgfältig eingepackt, unten in der Tasche verstaut und beim Verlassen des Kaufhauses ertönen schrille Signale, die anderen Kunden blicken sich um. Der Fehler ist schnell aufgeklärt, aber die Peinlichkeit besteht doch. Es kann ja nicht jeder wissen, dass die Ware bezahlt ist und nur die Diebstahlsicherung nicht entfernt oder deaktiviert wurde. Die Diebstahlsicherung besteht aus einem Etikett („tag“), das mit Radiofrequenzen animiert wurde, seine Existenz anzuzeigen (*Radio Frequency Identification – RFID*). Diese Technik kennen wir schon seit vielen Jahren. Inzwischen ist sie leistungsfähiger geworden und vermag viel mehr, als nur ihre Existenz anzuzeigen. Sie beginnt die Warenwirtschaft und die Logistik zu revolutionieren – leider nicht ohne Risiken für die informationelle Selbstbestimmung der Kunden. Wir gehen auf diese Technik später in einem Schwerpunktthema ein[26].

RFID-Tags dienen der Identifizierung von Waren, Objekten, Tieren, aber auch Personen[27]. Sie senden Identitätsmerkmale an einen Empfänger und zeigen an, was oder wer sich im Empfangsbereich dieser Geräte befindet.

Die Identifizierung ist aber längst nicht alles, was miniaturisierte Mikroelektronik zu leisten vermag. Viele Szenarien, die sich mit allgegenwärtiger (*ubiquitous*) oder um sich greifender (*pervasive*) Informationstechnologie befassen, beziehen auch die Gewinnung von Messwerten mit ein. Im Kühlschrank der modernen Küche reicht es nicht aus, dass das Gerät von der Existenz einer Getränkeflasche weiß, wichtig ist auch der Füllstand der Flasche, wenn der Besitzer rechtzeitig an den Nachkauf erinnert werden oder der Ersatz gar automatisch bestellt werden soll. *Sensoren* sind Voraussetzung dafür, dass Mikrosysteme Gewichte, Temperaturen und Druckverhältnisse messen können, aber auch, dass in den Körper implantierte Systeme Körpertemperatur, Blutdruck und andere Werte ermitteln und bei Bedarf aussenden können.

[26] vgl. 3.4

[27] vgl. 4.4.2

Eine spezielle Form der Sensoren stellen Mikrosysteme dar, die feststellen können, wo sie sich befinden (*Lokalisatoren*), indem sie z. B. GPS-Empfänger enthalten oder nutzen können. Wenn sie die Ergebnisse ihrer Standortermittlungen mittels Funktechnik weiterleiten können, können sie den aktuellen Verbleib von Fahrzeugen, transportierten Gegenständen, aber auch von Kindern oder orientierungslosen Personen melden.

Drahtlos sendende Identifikatoren, Sensoren und Lokalisatoren werden kleiner, billiger und genügsamer, was ihren Stromverbrauch und die Anforderungen an Umgebungsbedingungen angeht. Sie können überall angebracht, eingebaut oder implantiert werden. Sie senden ihre Informationen an Informationssysteme, die sie den jeweiligen Anwendungen entsprechend verarbeiten. In dieser informatisierten Welt kann jedes Objekt, gleichgültig, ob Sache oder Lebewesen, jederzeit identifiziert, auf seinen Zustand oder Status untersucht und lokalisiert werden. Solche Visionen sind keine ferne Utopie mehr; bedeutende Wissenschaftler, die sich mit solchen Technologien beschäftigen, reflektieren diese Aspekte der Zukunft auch unter gesellschaftspolitischem Hintergrund[28].

Friedemann Mattern, Leiter des Instituts für Pervasive Computing an der Eidgenössischen Technischen Hochschule Zürich, leitet aus diesen Entwicklungen diverse Szenarien ab[29].

Unter *„Embedded Computing“* wird die Integration von Mikroprozessoren in alltägliche Gegenstände verstanden. Diese können so befähigt werden, Informationen aufzunehmen, zu verarbeiten und weiterzuleiten, so dass sie sich mit anderen Alltagsgegenständen zu Netzen zusammenschließen können, ja sogar kooperieren können. Mattern beschreibt das Beispiel einer Rasenbewässerung, die in Abhängigkeit von der durch Sensoren festgestellten Bodenfeuchtigkeit und der Wettervorhersage aus dem Internet arbeitet.

Verlorene Gegenstände, die sich lokalisieren und ihren Standort weitermelden können, können so wiedergefunden werden. Ein solches Szenario ist selbst unter heutigen technischen und ökonomischen Rahmenbedingungen für große, wertvolle und mobile Gegenstände, z. B. Mietautos oder Lastwagen, realistisch. Mit weiterer Miniaturisierung, Verbilligung und Reduzierung des Energiebedarfs sind solche Techniken auch für einfachere Gegenstände einsetzbar.

Die Fahrgewohnheiten von Kraftfahrern können durch die Identifizierung des Kraftfahrers durch das benutzte Fahrzeug, durch seine Lokalisierung mittels GPS, durch Aufzeichnung der Fahrgeschwindigkeit, der positiven und negativen Beschleunigungen präzise ermittelt und an Kfz-Versicherun-

[28] vgl. z. B. Mattern, Friedemann (Hrsg.): Total vernetzt – Szenarien einer informatisierten Welt. Berlin: Springer, 2003; Weiser, Mark: The Computer for the 21st Century, Scientific American 265(3), 66–75

[29] Mattern, Friedemann: Ubiquitous Computing: Eine Einführung mit Anmerkungen zu den sozialen und rechtlichen Folgen. In: Taeger, Jürgen, Wiebe, Andreas (Hrsg.): Mobilität, Telematik, Recht (DGRI-Jahrestagung 2004). Köln: Verlag Dr. Otto Schmidt, 2005

gen weitergeleitet werden, die damit ihre Tarife dynamisch an die Risiken anpassen können, die der Autofahrer eingeht.

Werden Mikroprozessoren in die Kleidung und in Gegenstände, die man regelmäßig am Körper trägt (Armbanduhren, Schmuck, Schuhe), integriert, so spricht man von *„Wearable Computing“*. Bereits 1998 beschrieben wir ein Szenario mit in der Kleidung integrierten Sensoren, die die Signale eines implantierten RFID-Chips aufnehmen und zur Rettung eines Joggers beitragen, der beim Sport einen Herzanfall erleidet[30].

Die dritte Vision betrifft *„Sensornetze“*. Eine Vielzahl miniaturisierter Sensoren wird in die Umwelt eingebracht; sie können ihre jeweilige Umgebung beobachten und untereinander Ergebnisse austauschen. Handelt es sich z. B. um Sensoren, die Temperaturen messen können, so können sie etwa durch Vergleich der gemessenen Temperaturen plötzliche Temperatursteigerungen und Ausbreitungsgeschwindigkeit sowie -richtung von Bränden feststellen und entsprechende Alarmmeldungen abgeben. Eine ganz aktuelle Anwendung sind Drucksensoren, die im Meer ausgebracht werden und bei Tsunami-Warnsystemen Verwendung finden.

Die Vision der Sensornetze macht anschaulich, was sich beispielsweise unter den Begriff *„Smart Dust“* (Intelligenter Staub) zusammenfassen lässt: Hochgradig miniaturisierte – geradezu staubartige – miteinander und mit Hintergrundsystemen kommunizierende – spezialisierte Mikroprozessoren, für deren Anwendungsbereiche und -zwecke der Fantasie keine Grenzen gesetzt werden können.

Und was ist mit dem Datenschutz?

Die Datenschutzgesetze des Bundes und der Länder wurden in den letzten Jahren aus Anlass der Umsetzung der Europäischen Datenschutzrichtlinie von 1995 novelliert. Gleichzeitig erfolgte eine teilweise zaghafte Anpassung an die aktuellen informationstechnischen Rahmenbedingungen, die es erlauben, die mit dem Trend zur Vernetzung einhergehenden Konsequenzen für die informationelle Selbstbestimmung und für die Sicherheit der Datenverarbeitung mit der Terminologie des Datenschutzes zu erfassen. Nach wie vor ist umstritten, wieweit die vielfältigen Beeinträchtigungen der Privatsphäre oder Beeinträchtigungen des eigenen Selbstbestimmungsrechts, die das Internet mit sich bringt, durch den Datenschutz erfasst, bewertet und vielleicht auch unterbunden werden können. Die anarchische Entwicklung des E-Mail-Dienstes im Internet mit seinen extremen Risiken für die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der E-Mails, mit der extensiven Verbreitung von Schadsoftware, der Vermüllung der elektronischen Postfächer mit Spam sei hier als Beispiel genannt.

[30] JB 1998, 2.1

Es ist längst erkannt, dass die umfassende Modernisierung des Datenschutzrechts unumgänglich ist, wolle man sich nicht den mit der zunehmenden Informatisierung verbundenen Gefahren für die Persönlichkeitsrechte widerstandslos ausliefern[31]. Welchen Regelungsbedarf bewirkt aber „Smart Dust“ und seine Vorläufer?

War die elektronische Beobachtbarkeit der Menschen bisher beschränkt auf die Erkenntnisse, die sich aus der Nutzung elektronischer Kommunikationsmedien wie Internet, Telefon und Handy ergaben, so fallen diese Beschränkungen mit der Ausweitung des Ubiquitous Computing zum „Internet der Dinge“. Der vollständigen Erfassbarkeit der mit dem Kommunikationsverhalten verbundenen Lebensäußerungen steht jetzt die vollständige Erfassbarkeit alles persönlichen Verhaltens entgegen, Persönlichkeitsprofile könnten lückenlos erstellt werden.

Was wird aus dem Gerüst des Datenschutzes im Zeitalter der allgegenwärtigen Systeme, in dem permanent Daten erhoben, verarbeitet und kommuniziert werden? Was wird aus den Prinzipien des Datenschutzes wie das Gebot der Zweckbindung bei der Datenverarbeitung, der Erforderlichkeit der Datenverarbeitung als Voraussetzung für ihre Zulässigkeit, was wird aus dem Auskunftsrecht, was aus dem Gebot, dass prinzipiell jeder wissen soll, wer wann zu welchen Zwecken und in welcher Weise Daten über ihn verarbeitet (Transparenz)? Wie kann noch eine Einwilligung in die Datenverarbeitung sinnvoll und wirksam gegeben werden?

Diese Prinzipien können kaum mehr eingehalten werden[32]. Die permanente Erhebung personenbezogener Daten durch allgegenwärtige Sensoren, Identifikatoren und Lokalisatoren würde zur permanenten Vorratsspeicherung von Daten führen, die keinem konkreten Zweck dienen und daher auch nicht aktuell erforderlich sind. Sie werden gesammelt, um sie bei passender Gelegenheit zu nutzen. Die Kenntnisnahme permanenter Erhebungen oder gar das Erfordernis rechtlich wirksamer Einwilligungen scheitert schon an der schieren Masse. Und wie und bei wem sollte man Auskunftsrechte wahrnehmen können?

Der Datenschutz steht also angesichts der technischen Entwicklung vor neuen Herausforderungen.

2.2 Datenverarbeitung in der Berliner Verwaltung

Angesichts der Haushaltslage des Landes sind die Bemühungen weiter verstärkt worden, mit der Automatisierung von Verwaltungsprozessen personelle Einsparungen zu erreichen und gleichzeitig die Bürgerfreundlichkeit

[31] Roßnagel, Alexander; Pfitzmann, Andreas; Garstka, Hansjürgen: Modernisierung des Datenschutzrechts. Berlin: Bundesministerium des Inneren, 2001

[32] Roßnagel, Alexander; Müller, Jürgen: Ubiqitous Computing – neue Herausforderungen für den Datenschutz. In: Computer und Recht 8/2004

zu verbessern. Waren es im vorigen Jahr vor allem IT-Projekte, die sich direkt am Verwaltungsreformprozess orientierten (Querschnittscontrolling, Stellenpool), so sind im Berichtsjahr vor allem Projekte zu erwähnen, die die Ablösung lange veralteter Verfahren im Bereich der Ordnungs- und Strafverfolgungsbehörden betreffen. Die Ablösung des ehrwürdigen Uralt-Verfahrens ISVB der Polizei durch das neue Verfahren *POLIKS* steht kurz bevor, die Ablösung des kaum weniger ehrwürdigen Verfahrens Einwohnerwesen (*EWW*) ist ebenfalls vorangetrieben worden. Auch das *Ausländerwesen* steht vor einem informationstechnologischen Umbruch. Erfreulicherweise werden für die genannten neuen IT-Verfahren ausführliche Sicherheitskonzepte mit fachlicher Unterstützung erfahrener Unternehmen erarbeitet. Zu erwarten ist auch, dass es zu einer Umsetzung dieser Konzepte kommt. Demgegenüber kommt die Erarbeitung von behördlichen Sicherheitskonzepten, die die Sicherheit der lokalen IT-Infrastruktur gewährleisten sollen, kaum voran. Nach wie vor werden die knappen Mittel als Begründung herangezogen, ohne zu bedenken, dass dies nur bedeutet, dass bei der Verteilung der Mittel der IT-Sicherheit nur eine beklagenswert geringe Priorität eingeräumt wird. Möge dieses nicht eines Tages teuer werden!

IT-Politik in der Berliner Landesverwaltung

Zum wiederholten Male in der Geschichte der Datenverarbeitung in der Berliner Landesverwaltung sind im Berichtsjahr grundlegende gesetzgeberische und verwaltungsorganisatorische Änderungen der Entscheidungsfindung und der Organisation der Datenverarbeitung erfolgt. Wie immer ging es darum, Entscheidungsprozesse zu straffen, Kompetenzen zu bündeln, damit Synergieeffekte zu erzielen und die Effizienz des IT-Einsatzes in Berlin zu steigern. Insbesondere soll die Vereinheitlichung der IT-Welten in der Berliner Verwaltung wieder gefördert werden, nachdem zuvor die zentrale Steuerung eher unverbindlichen Charakter hatte und die verschiedenen Behörden weitgehend eigenständig ihre IT-Infrastrukturen gestaltet hatten.

Wie bereits im letzten Jahresbericht[33] angedeutet, ist das IT-Regelwerk grundlegend erneuert worden. Mit dem Gesetz über die Anstalt öffentlichen Rechts *IT-Dienstleistungszentrum Berlin*[34] (IDZ) hat der Landesbetrieb für Informationstechnik einen neuen Namen und eine neue Rechtsform erhalten. Mit der Erlangung der Rechtsfähigkeit soll dem IDZ mehr Flexibilität und Unabhängigkeit bei seinen Entscheidungen zugebilligt werden, damit es sich auch auf dem Markt behaupten kann.

Wegen der Auswirkungen auf die Entscheidungsprozesse bei der Datenverarbeitung in der Landesverwaltung haben die neuen Verwaltungsvorschriften für die Steuerung des IT-Einsatzes in der Berliner Verwaltung (*VV IT-Steuerung*)[35] vermutlich eine größere Bedeutung für das Verwaltungshandeln in diesem Sektor. Die zentralen Steuerungsaufgaben werden von einem IT-Kompetenzzentrum der Senatsverwaltung für Inneres unter der Leitung eines IT-Staatssekretärs wahrgenommen. Sie umfassen die Konzeption des IT-Einsatzes im Lande, die Festlegung einheitlicher Verfahrensweisen und Standards für die Planung, Realisierung und Fortschreibung von IT-Maßnahmen, die IT-Sicherheit, das IT-Controlling, die einheitlichen Verfahrensweisen und Standards bei der Beschaffung von Produkten und Dienstleistungen, die Aushandlung von Landesvereinbarungen mit IT-Dienstleistern und das E-Government. Zentrales Beratungsgremium ist der neue *Landesausschuss für den IT-Einsatz*. Ihm gehören neben dem IT-Staatssekretär drei weitere Staatssekretäre und drei vom Rat der Bürgermeister benannte Bezirksamtsmitglieder an. Die fachliche Vorabstimmung leistet ein IT-Koordinierungsgremium.

Damit löst eine politische Entscheidungsstruktur die bisher eher fachlich geprägte Struktur ab. Der bisherige IT-Koordinierungs- und Beratungsausschuss (*IT-KAB*), der unter der Leitung der Senatsverwaltung für Inneres die Geschicke der Informationstechnik im Lande entscheidend bestimmte, wird – so er die Rolle des IT-Koordinierungsgremiums in möglicherweise geänderter Zusammensetzung übernimmt – nur noch fachlich beratende Funktion haben. Abzuwarten ist, ob, und wenn ja, wo der Berliner Beauftragte für Datenschutz und Informationsfreiheit seine beratende Stimme einbringen kann. Wir versprechen uns mit der Politisierung der Entscheidungsfindung in Hinblick auf die IT-Sicherheit Vorteile. Zwar hat der IT-KAB, auch mit seinen Arbeitsgruppen „IT-Sicherheit“ und „Modellsicherheitskonzept“, das Thema IT-Sicherheit immer mit der angemessenen Bedeutung behandelt, nur an der Umsetzung der dort erarbeiteten Regelwerke wie z. B. die IT-Sicherheitsrichtlinie des Landes[36] haperte es gewaltig, in erster Linie, weil die politische Entscheidungsebene in den Behörden vielfach andere Prioritäten für den Einsatz ihrer Finanzmittel sah. Mit der neuen Struktur reicht es nicht, den guten Willen der eigenen IT-Fachleute zu bremsen, jetzt muss man sich in den Entscheidungsgremien dazu bekennen, ob die Datenverarbeitung mit der nötigen Sicherheit funktionieren soll oder nicht.

IT-Sicherheit in Berlin

Das Berliner Datenschutzgesetz verlangt in § 5 Abs. 2, dass bei der Verarbeitung personenbezogener Daten die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität gewährleistet werden müssen und dass diese revisionsfähig und transparent stattfinden muss. Mit den ersten vier Begriffen wird weltweit IT-Sicherheit beschrieben. Die Gewährleistung dieser Sicherheitsziele kann nicht mit einer zufälligen Auswahl aus irgendwelchen Maßnahmenkatalogen oder per Wunschzettel aus den Angeboten der IT-Sicherheitsindustrie erreicht werden. Vielmehr bedarf es systematischer, auf anerkannten Methoden basierender, aber auf den konkreten Einzelfall ausgerich-

33 JB 2003, 2.2

34 GVBl. 2004, S. 459 ff.

35 DBl. I 2004, S.10 ff.

36 DBl. I 1999, S. 5 ff.

teter *Risikoanalysen* als Voraussetzung dafür, dass die technischen und organisatorischen Maßnahmen auf die Reduzierung der vorhandenen nicht tragbaren Risiken gerichtet werden und somit ein Sicherheitskonzept bilden. Aus diesem Grunde wird auch in § 5 Abs. 3 BlnDSG die Durchführung einer Risikoanalyse und die Erarbeitung eines Sicherheitskonzepts verlangt. Die Sicherheitsrichtlinie wird derzeit im Rahmen der neuen Regelungen zur IT-Steuerung zu IT-Sicherheitsgrundsätzen fortgeschrieben. Die wesentlichen Inhalte bleiben aber unangetastet.

Es bleibt auch dabei, dass jährlich bis zum März des laufenden Jahres ein *IT-Sicherheitsbericht* erstellt wird. Allerdings wird bei der zuständigen Senatsverwaltung darüber nachgedacht, die Informationsbasis für diese Berichte vertrauenswürdiger zu gestalten. Bisher basierten diese Berichte vorwiegend auf Umfragen bei den Berliner Behörden. Die dabei entstandenen Ergebnisse hatten mit unseren Kontrollerfahrungen nicht viel zu tun.

Der letzte Bericht, der sich mit dem Jahr 2003 befasst, fußt auf dem Rücklauf von 53 Behörden. Die Frage nach der Existenz und dem Umsetzungsgrad von behördlichen und verfahrensspezifischen Sicherheitskonzepten haben 42 davon beantwortet. Ein knappes Drittel (13) davon bejahte die Existenz eines schriftlich festgelegten behördlichen Sicherheitskonzepts, gut die Hälfte (22) bekundete, dass für Teilbereiche ein solches Sicherheitskonzept vorläge, die übrigen 7 gaben zu, dass schriftliche Sicherheitskonzepte fehlten. Diese sieben Behörden waren offenbar zum Teil der Meinung, dass es mündliche Sicherheitskonzepte geben könnte, denn immerhin haben nur zwei von den 42 Behörden angegeben, dass bei ihnen das Sicherheitskonzept zumindest in einzelnen Maßnahmen umgesetzt worden sei. Zu den verfahrensspezifischen Sicherheitskonzepten macht der Bericht keine quantitativen Aussagen. Für beide Arten von Sicherheitskonzepten wurden qualitative Aspekte (Aktualität, Vollständigkeit, Existenz einer Risikoanalyse, Zeitrahmen für die Umsetzung, Revisionsfähigkeit) nicht einmal erfragt.

Die übrigen Aussagen des IT-Sicherheitsberichts ergaben zumindest, dass eine Vielzahl von Einzelmaßnahmen (Virenschutz, Firewalls, Verschlüsselung usw.) von einem mehr oder weniger großen Teil der Behörden getroffen worden ist, um augenfällige Risiken abzuwehren. Gleiches gilt für die Nutzung von zentralen Angeboten an Sicherheitstechnik im Berliner Landesnetz. 35 der 53 Behörden führen eine dezentrale Virenprüfung durch, d. h., ein Drittel der Behörden verzichtet darauf und vertraut ausschließlich auf die zentrale Virenschutzprüfung im Landesbetrieb für Informationstechnik (Grenznetz zwischen Internet und Landesnetz)[37]. Dieses ist grob leichtfertig, denn Viren in passwortgeschützten oder verschlüsselten Dateien werden zentral nicht oder nicht zuverlässig abgefangen.

Basiert der IT-Sicherheitsbericht im Wesentlichen auf dem Glauben an die Ehrlichkeit und Kompetenz der antwortenden Behörden, so sehen die Ergebnisse ganz anders aus, wenn die Existenz und Qualität von Sicherheitskonzepten einer Kontrolle unterzogen wird. So befasst sich der *Rechnungshof von Berlin* (trotz der immer wieder behaupteten Kostenträchtigkeit der IT-Sicherheit) ebenfalls intensiv mit der Durchsetzung von IT-Sicherheit im Lande. 2003 hat er beinahe flächendeckend IT-Sicherheitskonzepte der Behörden angefordert und auf Aktualität, Fortschreibungsstatus, Vollständigkeit, funktionales Sicherheitsniveau, Stand der Umsetzung und Revisionsfähigkeit überprüft. Seine Ergebnisse decken sich in keiner Weise mit dem Sicherheitsbericht. Von 113 in die Prüfung einbezogenen Behörden haben nur zwei ein vollständiges, schriftliches und umgesetztes Sicherheitskonzept vorweisen können, in mehr als hundert Fällen lag kein schriftliches Konzept im Sinne der IT-Sicherheitsrichtlinie vor.

Hoffnung auf die Verbesserung der Situation haben wir im Zusammenhang mit der Entwicklung eines *Modellsicherheitskonzepts* durch eine Arbeitsgruppe des IT-KAB unter der Federführung der Senatsverwaltung für Inneres. Das Modellsicherheitskonzept basiert auf dem Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[38] und vereinfacht dessen Anwendung durch die Vorabeinbeziehung relevanter Rahmenbedingungen in der Berliner Verwaltung. Das Modellsicherheitskonzept wird sukzessiv aufgebaut und ist somit in den bereits fertig gestellten Teilbereichen sofort anwendbar.

Aktuelle IT-Projekte des Landes

Erneut sind wir über eine Vielzahl neuer IT-Projekte in öffentlichen Stellen Berlins unterrichtet worden. Nach der Abschaffung des *Dateienregisters* mit der Novellierung des Berliner Datenschutzgesetzes im Jahre 2001 ist die Pflicht zu unserer Unterrichtung über neue Automationsvorhaben (§ 24 Abs. 3 Satz 3 BlnDSG) die einzige direkt verfügbare Quelle, aus der wir erfahren, welche IT-Verfahren künftig unserer Kontrolle unterliegen. Die zitierte Vorschrift sagt nichts darüber aus, wann eine solche Unterrichtung zu erfolgen hat. Wenn die öffentlichen Stellen erwarten, dass wir zu einem Verfahren aus rechtlicher und technisch-organisatorischer Sicht Stellung beziehen, dann muss die Unterrichtung so früh erfolgen, dass eine Prüfung der in der Regel sehr umfänglichen Unterlagen so rechtzeitig Ergebnisse erbringt, dass diese im Bedarfsfall noch zu Modifikationen im IT-Projekt führen können. Wenn die Verfahren dagegen in den Echtbetrieb gegangen sind oder dies kurz bevorsteht, können eventuell festgestellte datenschutzrechtliche Mängel nur auf der Grundlage von § 26 BlnDSG beanstandet oder im unerheblichen Fall bemängelt werden. Die notwendigen Modifikationen müssten in diesem Falle nachträglich durchgeführt werden.

Im Bereich der Sicherheit und Strafverfolgung stand das neue Verfahren *POLIKS* (Polizeiliches Informations- und Kommunikationssystem) im

[37] vgl. auch 4.8.3

[38] BSI (Hrsg.): IT-Grundschutzhandbuch. Köln: Bundesanzeiger-Verlag, 2003 (Druckfassung)

Vordergrund, mit dem im Frühjahr 2005 endlich das alte ISVB abgelöst werden soll. Das moderne Verfahren integriert auch die Fahndungsaufgaben, die Dokumentation polizeilichen Handelns und die Sachbearbeitung einschließlich der Funktionen der Formularerfassung, die zuvor im Verfahren BMO-Office die Arbeit der Schutzpolizei im Rahmen des Berliner Modells unterstützten. Anders als das alte Verfahren ISVB, welches auf neue Anforderungen, auch solche, die aus datenschutzrechtlich Sicht umzusetzen gewesen wären, nicht angepasst werden konnte, ist POLIKS sehr flexibel, z. B. was die Vergabe von Zugriffsberechtigungen und die Auswahl der Protokollierungen betrifft. Allerdings stellt das neue Verfahren erweiterte Ansprüche an die Benutzer, so dass von besonderem Schulungsbedarf ausgegangen werden muss, wenn die Ordnungsmäßigkeit der Datenverarbeitung sichergestellt bleiben soll. Für POLIKS ist ein detailliertes Sicherheitskonzept erstellt worden, welches auch aus unserer Sicht die Sicherheitsansprüche, die an ein solches Verfahren zu stellen sind, hinreichend erfüllt. Für die Umsetzung und für die notwendigen Fortschreibungen und Anpassungen soll ein IT-Management sorgen.

In der Ordnungsverwaltung wird weiterhin an der Erneuerung des automatisierten *Meldewesens* gearbeitet. Es soll eine erprobte Standardsoftware eingesetzt werden, die zurzeit auf Berliner Ansprüche angepasst wird.

Die Ablösung des Fachverfahrens AUSREG durch das Nachfolgeverfahren AUSREG2 in der Abteilung *Ausländerangelegenheiten* im Landeseinwohneramt Berlin wurde vorangetrieben. Kurz vor Ende des Berichtsjahrs erfolgte die Zusendung der Ergebnisse einer dritten Voruntersuchungsphase. Zu den ersten beiden Phasen hatten wir bereits erste vorsorgliche Hinweise gegeben. Wegen der intensiven und vielfältigen Kommunikationsbeziehungen im Bereich des Ausländerwesens betrafen sie die rechtlichen Voraussetzungen für automatisierte Abrufverfahren, ferner die beabsichtigte Verarbeitung von besonders schutzbedürftigen Daten nach § 6 a BlnDSG, für die besondere Absicherungen notwendig sind.

Ebenfalls im Bereich der Ordnungsaufgaben berieten wir ein Projekt für ein *Sprachdialogsystem* SDS-Info im Landesbetrieb für Informationstechnik. Hier soll den Bürgern ermöglicht werden, telefonisch den Stand der Bearbeitung von Anträgen zur Ausstellung von Reisepässen und anderen Personaldokumenten zu erfragen. Dazu bedarf das System einer Online-Schnittstelle zur Bundesdruckerei, die diese Dokumente herstellt.

Bei den bezirklichen *Einbürgerungsstellen* soll ein neues IT-Verfahren EvASta (Einbürgerung von Ausländern) eingeführt werden. Dabei handelt es sich um eine Standardsoftware, die auch in anderen Kommunen eingesetzt wird und an Berliner Anforderungen angepasst werden muss. An diesem Projekt zeigte sich, dass eine zurückhaltende Informationspolitik uns gegenüber zu unerwarteten Verzögerungen führt. Zunächst war nur die Notwendigkeit gesehen worden, den behördlichen Datenschutzbeauftragten des Pilotbezirks zu informieren (Pflicht nach § 19 a Abs. 3 Satz 3 BlnDSG). Als

dieser zu Recht erkannte, dass wegen der Verarbeitung besonderer Daten nach § 6 a BlnDSG (Volkszugehörigkeit = ethnische Herkunft) eine Voruntersuchung nach § 19 a Abs. 1 Satz 3 Nr. 1 BlnDSG notwendig war, wandte er sich an uns mit der Bitte um Unterstützung (§ 19 a Abs. 4 BlnDSG). Die dann erfolgte Erinnerung an die ebenfalls gesetzliche Verpflichtung, uns über das Verfahren zu unterrichten, führte zu einer Entrüstung, die bei Befassung mit den datenschutzrechtlichen Beteiligungspflichten vermeidbar gewesen wäre. Ansonsten ergab sich eine noch nicht ausgestandene Kontroverse zu der Frage, wie lange die Daten im System und in Akten vorgehalten werden dürfen, wenn es dazu keine rechtlichen Bestimmungen gibt.

In der Verkehrsverwaltung wird ein Pilotprojekt „*Mobile Parking*“ initiiert, bei dem Autofahrer über das Handy Parkberechtigungen buchen können. Dabei können die Versuchsteilnehmer eine bestimmte Nummer wählen. Dort wird der Anruf der Person zugeordnet und die Zeit des Parkbeginns registriert. Gleiches geschieht bei Parkende. Die Gebühren werden per Einzugsermächtigung auf der Grundlage eines individuellen Parkkontos eingezogen. Dabei können Vorauszahlungen geleistet werden. Die Anmeldung zum Versuch erfolgt über das Internet bei einem österreichischen Auftragnehmer. Die Teilnehmer am Versuch erhalten eine Vignette mit einem zweidimensionalen Barcode, der von Kontrolleuren gelesen und zur Prüfung herangezogen werden kann, ob eine aktuelle Parkberechtigung gebucht worden ist. Die Datenverarbeitung basiert auf der Grundlage der Einwilligung des Betroffenen und ist als datenschutzfreundlich zu bewerten, da bei der Kontrolle nicht mehr personenbezogene Daten erfasst werden müssen als im üblichen Verfahren auch. Unsere Beratung bezog sich vorwiegend auf die Regelungen der Auftragsdatenverarbeitung in einem anderen EU-Land.

3. Schwerpunkte im Berichtsjahr

3.1 Hartz IV und der Datenschutz

Mit dem Sozialgesetzbuch (SGB) Zweites Buch (II) – Grundsicherung für Arbeitssuchende – erfolgt ab 1. Januar 2005 eine Zusammenführung von Arbeitslosenhilfe und Sozialhilfe. Ehemalige erwerbsfähige Sozialhilfeempfänger und Arbeitslosenhilfeempfänger erhalten ab diesem Zeitpunkt die gleichen Leistungen. Grundlage hierfür ist das Vierte Gesetz für moderne Dienstleistungen am Arbeitsmarkt vom 24. Dezember 2003[39], das in seinem Artikel 1 das neue SGB II einführt und Änderungen in zahlreichen weiteren Rechtsvorschriften vorsieht (allgemein *„Hartz IV“* genannt).

Das Gesetzgebungsvorhaben wurde in großer Eile durchgeführt. Die praktische Umsetzung erfolgte in noch größerer Eile. Leider führte dies zu erheblichen datenschutzrechtlichen Mängeln, die noch vermeidbar gewesen wären, wenn die Bundesagentur für Arbeit die Datenschutzbeauftragten von vornherein einbezogen hätte[40].

Die *Bundesagentur für Arbeit* begann ab Juli 2004 mit der Versendung der Vordrucke für die Beantragung des *Arbeitslosengeldes II* an 2,2 Millionen Empfänger von Arbeitslosenhilfe. In diesen Antragsformularen wurden zahlreiche Angaben verlangt, die für die Antragsbearbeitung nicht erforderlich waren und deren Erhebung damit datenschutzrechtlich unzulässig war. Nachdem die Datenschutzbeauftragten noch im August auf die datenschutzrechtlichen Mängel hingewiesen hatten, entwickelte die Bundesagentur für Arbeit im September 2004 in Zusammenarbeit mit dem Bundesbeauftragten für den Datenschutz Ausfüllhinweise, die zumindest die wesentlichen datenschutzrechtlichen Bedenken aufgreifen und den Betroffenen eine Hilfestellung zum datenschutzgerechten Ausfüllen des Antragsformulars an die Hand geben. Eine Überarbeitung der Antragsformulare selbst ließ sich leider kurzfristig nicht ermöglichen. Die Bundesagentur für Arbeit hat aber angekündigt, die Antragsvordrucke in der nächsten Druckauflage zu korrigieren. Dies soll im Frühjahr 2005 der Fall sein. Wir hoffen, dass die Bundesagentur für Arbeit ihre Zusage, den Bundesbeauftragten für den Datenschutz im Interesse der Betroffenen frühzeitig einzubeziehen, einhalten wird.

Neben den weitreichenden sozialen Folgen für die Betroffenen zieht die Zusammenlegung von Arbeitslosen- und Sozialhilfe organisationsrechtliche Folgen für die Sozialverwaltung nach sich. Während bisher die Kommunen für die Sozialhilfe und die Bundesagentur für Arbeit für die Arbeitslosen-

39 BGBl. I, S. 2954

40 Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. Oktober 2004 „Gravierende Datenschutzmängel bei Hartz IV“, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2004“, S. 16

hilfe verantwortlich waren, wurde die Trägerschaft für die Grundsicherung für Arbeitssuchende den Kommunen sowie der Bundesagentur für Arbeit gemeinsam übertragen. Zur einheitlichen Wahrnehmung der Aufgaben im Rahmen der Grundsicherung für Arbeitssuchende wurden so genannte Arbeitsgemeinschaften (ArGen) gegründet. Sie führen den Namen JobCenter und nehmen die Aufgaben der Grundsicherung für Arbeitssuchende für die jeweilige Arbeitsagentur und das Bezirksamt wahr. Grundlage hierfür sind in Berlin Errichtungsverträge über insgesamt zwölf ArGen, die von den Berliner Bezirksämtern mit den örtlichen Arbeitsagenturen abgeschlossen wurden.

Auch für die Datenschutzbeauftragten des Bundes und der Länder ist mit der Gründung der ArGen zum 1. Januar 2005 eine Änderung der Zuständigkeiten verbunden. Während bisher eine Trennung der Kontrollzuständigkeit des Bundesbeauftragten für den Datenschutz und der Landesbeauftragten für den Datenschutz bestand, wird diese Trennung mit der Gründung der Arbeitsgemeinschaften für die Grundsicherung für Arbeitssuchende teilweise aufgegeben. Die Tätigkeit der Arbeitsagenturen fällt nicht mehr wie bisher ausschließlich in den Zuständigkeitsbereich des Bundesbeauftragten für den Datenschutz, sondern hinsichtlich der Tätigkeit der ArGen nunmehr auch in die des jeweiligen Landesbeauftragten für den Datenschutz. Da wir bislang lediglich die Prüfkompetenz für die Datenverarbeitung der Sozialämter, nicht jedoch der Arbeitsagenturen hatten, betreten wir im Zuge von Hartz IV ebenfalls Neuland.

Die Vielzahl von Anfragen Betroffener nimmt mittlerweile einen bedeutenden Anteil unserer Arbeit ein. Verunsichert durch Presseberichte sowie eigene Erfahrungen bei der Beantragung des Arbeitslosengeldes II wandten sich zahlreiche Bürgerinnen und Bürger an uns und baten um Beratung und Hilfe im konkreten Einzelfall. Wir machten anfangs die Erfahrung, dass die von der Bundesagentur für Arbeit in ihrem Internetangebot zur Verfügung gestellten Ausfüllhinweise den Antragstellern in den Bezirksämtern offenbar nicht bereitgestellt wurden. Die Hinweise konnten den Betroffenen, die in der Mehrzahl nicht über einen Internetanschluss verfügen, insofern nicht bekannt sein. Wir nahmen die Eingaben zum Anlass, die Berliner Bezirksämter aufzufordern, die Ausfüllhinweise für die Antragsteller bereitzustellen.

Oft werden wir gefragt, was mit den überflüssig erhobenen Daten in den Antragsformularen geschieht. Sorge bereitet es den Bürgerinnen und Bürgern, ob die nicht erforderlichen Daten trotz datenschutzrechtlich unzulässiger Erhebung in das im Auftrag der Bundesagentur für Arbeit eigens für die Bearbeitung des Arbeitslosengeldes II entwickelte IT-Verfahren *A2LL*, das leider noch immer wesentliche Datenschutzmängel aufweist[41], übernommen werden.

[41] vgl. 2.2

Veranlasst durch die Beschwerden der Bürgerinnen und Bürger führten wir im Dezember 2004 stichprobenartig eine datenschutzrechtliche Prüfung der Bearbeitung der Anträge zum Arbeitslosengeld in vier ausgewählten bezirklichen Sozialämtern in Berlin durch. Uns ging es insbesondere darum festzustellen, wie in den Bezirksämtern mit der praktischen Eingabe der Anträge auf Arbeitslosengeld II in das System A2LL verfahren wird. Die Prüfungen konnten von uns nicht im Jahr 2004 abgeschlossen werden, da wir die Prüfung in einem Berliner Bezirksamt leider abbrechen mussten. Da das Bezirksamt unsere Prüfkompetenz zunächst anzweifelte und es zusätzlich aus technischen Gründen nicht möglich war, uns am Tag der beabsichtigten Prüfung die vollständigen Prüfunterlagen zur Verfügung zu stellen, wurde die Prüfung im Januar 2005 durchgeführt. Da die in dem Bezirk gegründete ArGe bereits zum 1. Januar 2005 ihren Betrieb aufgenommen hatte, wurden wir gebeten, die Prüfung nunmehr im JobCenter durchzuführen. Hier wurden uns Akten vorgelegt, die nicht aus dem Bezirksamt, sondern vielmehr von der Arbeitsagentur stammten. Interessant war es für uns festzustellen, dass die Bearbeitung der Anträge von den Sozialämtern und Arbeitsagenturen durchaus unterschiedlich gehandhabt wird.

Wir verglichen den Inhalt der Akten mit den in das System A2LL eingegebenen Daten. Positiv konnten wir feststellen, dass die überflüssig erhobenen personenbezogenen Daten der Antragsteller nicht in das System A2LL übernommen wurden. Bei der Prüfung der Akten stellten wir allerdings fest, dass die Sozialämter eine Vielzahl von Unterlagen der Antragsteller, wie z. B. Personalausweise, Lohnsteuerkarten, Sozialversicherungsausweise, vollständige Mietverträge, Scheidungsurteile, ungeschwärzte Kontoauszüge etc. in Fotokopie zu den Akten nahmen. In den von der Arbeitsagentur bearbeiteten Akten fanden wir in der Regel weniger Fotokopien von Unterlagen der Betroffenen. Für uns stellt sich bei einigen Unterlagen die Frage, ob und inwiefern sie tatsächlich für die Bearbeitung des Antrages erforderlich sind. Des Weiteren ist fraglich, zu welchen Zwecken Unterlagen in Kopie zu den Akten genommen werden, wenn ihre Vorlage zur Prüfung als Nachweis doch ausreichend erscheint. Zum gegenwärtigen Zeitpunkt sind diese Fragen noch nicht abschließend geklärt. Wir werden in Abstimmung mit den Datenschutzbeauftragen der Länder und dem Bundesbeauftragten für den Datenschutz eine Klärung dieser und weiterer im Zusammenhang mit Hartz IV stehender noch offener Fragen herbeiführen.

Wenn wir in der Vergangenheit immer wieder die mangelnden Sicherheitsvorkehrungen des Sozialhilfesystems BASIS kritisiert haben, dann haben wir Maßstäbe angelegt, die in Berlin üblich sind. Das IT-Verfahren A2LL, mit dem die Verwaltung des Arbeitslosengeldes II umgesetzt werden soll, stellt in Bezug auf seine Unsicherheit alles in den Schatten, was bisher in Berlin an Erfahrungen gemacht werden konnte. Bei der hastigen Entwicklung des Verfahrens zur Umsetzung der Hartz-IV-Reform ist offenbar zunächst die ganze Aufmerksamkeit auf die Funktionalität des Verfahrens gerichtet worden, Aspekte der Sicherheit und der Ordnungsmäßigkeit blieben weitgehend unberührt. So kann jeder Mitarbeiter einer Arbeitsagentur

oder eines Sozialamtes, später der Arbeitsgemeinschaften, auf alle A2LL-Daten bundesweit zugreifen, eine Zugriffsdifferenzierung existiert nicht. Der lediglich lesende Zugriff wird nicht einmal protokolliert.

Der Bundesbeauftragte für den Datenschutz hat diese Mängel gegenüber der Bundesagentur für Arbeit förmlich beanstandet, wir haben diese Beanstandung allen involvierten Landesbehörden zur Kenntnis gegeben. In Umsetzung einer Verabredung in der Konferenz der Datenschutzbeauftragten haben wir wie alle Landesbeauftragten von einer förmlichen Beanstandung bei den Sozialbehörden abgesehen, obwohl A2LL dort auch in der datenschutzrechtlichen Verantwortung der Berliner Behörden betrieben wird. Es bestand Konsens zwischen den Landesdatenschutzbeauftragten, dass solche Beanstandungen ins Leere laufen würden, weil die Landesbehörden keinen Einfluss auf die Gestaltung des Verfahrens nehmen konnten und es auch in absehbarer Zeit nicht können.

Auch der Anfänger-Fehler bei der Darstellung der *Kontonummern* im System (Auffüllung der Stellen mit Nullen von rechts!) macht deutlich, dass die Ordnungsmäßigkeit des Verfahrens nicht zu den primären Gestaltungszielen gehört hat. Offenkundig haben auch keine hinreichenden Tests stattgefunden. Wir werden das Verfahren in Zusammenarbeit mit dem Bundesbeauftragten und anderen Landesbeauftragten weiter im Auge behalten.

3.2 Steuergerechtigkeit oder der gläserne Bürger

Im Bereich der *Finanzverwaltung* ist in den letzten vier Jahren eine Großzahl an Gesetzen verabschiedet worden, die den Bürger in seinem Recht auf informationelle Selbstbestimmung berührt haben, so dass es uns an der Zeit erscheint, hierüber ausführlicher zu berichten. Allerdings müssen wir uns an dieser Stelle auf einen Ausschnitt der datenschutzrelevanten Gesetze beschränken, da in so viele Gesetze datenschutzrechtlich relevante Regelungen aufgenommen wurden, dass es den Rahmen dieses Berichtes sprengen würde, alle Neuregelungen aufzugreifen.

Im August 2001 wurde das Gesetz zur Eindämmung *illegaler Betätigung* im Baugewerbe verabschiedet. In diesem Gesetz wurde unter anderem das Verfahren für den Steuerabzug bei Bauleistungen neu geregelt. Zur besseren Kontrolle durch die Finanzbehörden wurde für den Leistungsempfänger eine Freistellungsbescheinigung in dem Besteuerungsverfahren eingeführt, mit der er seine persönliche Haftung für nicht oder zu niedrig abgeführte Steuern durch den Leistungserbringer ausschließen kann. Der Leistende kann in den gesetzlich geregelten Fällen eine Freistellungsbescheinigung vorlegen, die nach der Regelung des § 48 b Abs. 3 Einkommensteuergesetz (EStG) die Steuernummer und das zuständige Finanzamt des Leistenden enthalten muss.

Im Steueränderungsgesetz 2001 wurde § 48 b EStG noch dahingehend ergänzt, dass die beim Bundesamt für Finanzen zentral geführte Datei der *Freistellungsbescheinigungen* im Online-Verfahren an die Leistungsempfänger Auskünfte darüber erteilt, ob für den Leistenden tatsächlich eine gültige Freistellungsbescheinigung vorliegt. Die Zustimmung des Leistenden zur Online-Beauskunftung wird mit der Beantragung einer Freistellungsbescheinigung erteilt.

Ende 2001 wurde das *Steuerverkürzungsbekämpfungsgesetz* verabschiedet. Eingeführt wurde damit unter anderem die Angabe der Steuernummer auf Rechnungen nach § 14 Abs. 1 a Umsatzsteuergesetz (UStG). Ausgenommen wurden nur Rechnungen über Kleinbeträge.

Mit dem vierten *Finanzmarktförderungsgesetz* von 2002 wurde in das Kreditwesengesetz (KWG) § 24 c eingefügt und eine *Kontenevidenzzentrale* bei der Bundesanstalt für Finanzdienstleistungsaufsicht eingeführt. Die Banken haben danach eine Datei zu führen, die die Nummer der geführten Konten, den Namen und das Geburtsdatum der Verfügungsberechtigten sowie deren Anschrift enthält. Die Datei dient der Bundesanstalt zur Erfüllung ihrer aufsichtsrechtlichen Aufgaben aus dem Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten sowie zur Beauskunftung an bestimmte Aufsichtsbehörden. Sie dient außerdem der Beauskunftung von Anfragen der Strafverfolgungsbehörden und Gerichte sowie der Erfüllung von Aufgaben nach dem Außenwirtschaftsgesetz oder bestimmten Rechtsakten der europäischen Gemeinschaften. Die Banken erhalten von den erfolgten Abrufen keine Kenntnis. Die einzelnen Finanzbehörden sollen keine Anfragen an die Bundesanstalt für Finanzdienstleistungsaufsicht richten und keine Auskünfte erhalten können.

Mit dem Steueränderungsgesetz 2003[42] wurde eine Rechtsgrundlage für die Einführung einer Identifikationsnummer für jeden *Steuerpflichtigen* von Geburt an geschaffen (§ 139 a Abgabenordnung – AO). Die Identifikationsnummer, die vom Bundesamt für Finanzen zugeteilt werden soll, soll der einheitlichen Identifizierung des Steuerpflichtigen dienen und an die Stelle der bisherigen je nach Steuerart unterschiedlichen Steuernummern treten. Wirtschaftlich tätige Steuerpflichtige erhalten eine *Wirtschafts-Identifikationsnummer*. Das Bundesamt für Finanzen wird in der Zentraldatei die Identifikationsnummer, den Familiennamen, frühere Namen, Vornamen, Doktorgrad, Ordens-/Künstlernamen, Tag und Ort der Geburt, die gegenwärtige oder letzte bekannte Anschrift, die zuständigen Finanzämter und den Sterbetag speichern. Die Meldebehörden sind verpflichtet, jede Geburt auch dem Bundesamt für Finanzen mitzuteilen, damit dem neuen Steuerpflichtigen unverzüglich eine Identifikationsnummer mitgeteilt werden kann, die nach Vergabe an den Meldedatensatz der Meldebehörde angefügt wird. Es ist beabsichtigt, die Identifikationsnummer im Jahre 2007 einzuführen.

[42] BGBl. I, S. 2645

Ebenfalls Ende 2003 wurde das Gesetz zur Förderung der *Steuerehrlichkeit*[43] verabschiedet. Dadurch wurde § 93 AO ergänzt. Jetzt dürfen alle Behörden, die ihr Zuständigkeitsgesetz an den Einkommensbegriff anknüpfen, oder Gerichte, die ab 1. April 2005 Finanzbehörden ersuchen, über das Bundesamt für Finanzen kontobezogene Daten aus der Kontenevidenzzentrale nach § 24 c KWG abrufen. Die Verantwortung für die Abrufe trägt die jeweilige Behörde bzw. das jeweilige Gericht. Die betroffenen Banken erhalten von den Online-Abrufen keine Kenntnis.

Gegenüber diesen ausufernden Bemühungen der Gesetzgebung der letzten Jahre blieben nach wie vor die Forderungen der Datenschutzbeauftragten des Bundes und der Länder, datenschutzrechtliche Vorschriften in die Abgabenordnung aufzunehmen, erfolglos. Nachdem erste Bemühungen hierzu bereits 1988 aufgenommen worden waren, war der Entwurf eines Abgabenordnungsänderungsgesetzes 1994, der datenschutzrechtliche Vorschriften vorsah, nicht weitergeführt worden.

Nach dem Volkszählungsurteil bedarf es zur Einschränkung des informationellen Selbstbestimmungsrechts des Einzelnen einer normenklaren Regelung. Die Verfassung von Berlin schreibt fest: Das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, wird gewährleistet. Einschränkungen dieses Rechts bedürfen eines Gesetzes.

Was haben diese datenschutzrechtlichen Regelungen gemeinsam? Der Bürger wird auf der einen Seite verpflichtet, seine Steuernummer im öffentlichen Leben immer mehr Stellen mitzuteilen, obwohl diese Steuernummer für die meisten Menschen bisher zu den persönlichen Daten gehörte, die nur gegenüber den Finanzämtern verwendet wurde, als Zuordnungsschlüssel zu den eigenen Steuerdaten beim Finanzamt. Die Steuernummer enthält keine verschlüsselten Angaben über den Bürger; sie ist jedoch der Zugangsschlüssel für die personenbezogenen Steuerdaten. Die Missbrauchsmöglichkeiten für Dritte wachsen mit der gesetzlich geregelten Pflicht zur Angabe der Steuernummer im Wirtschaftsleben.

Schwerer wiegt dagegen die Tatsache, dass es mit der Einführung des einheitlichen Identifikationsmerkmals in Zukunft eine Zentraldatei über fast alle Bundesbürgerinnen und Bundesbürger beim Bundesamt für Finanzen geben wird. Da dieses dann vergebene Identifikationsmerkmal alle bisherigen Steuernummern, wie die Kfz-Steuernummer, die Umsatzsteuernummer, die Gewerbesteuernummer oder die lohn-/einkommensbezogene Steuernummer ersetzen soll, bedeutet auch die Pflichtangabe des Identifikationsmerkmals im täglichen Leben eine Erhöhung des Missbrauchspotenzials.

Vor allem weil die Identifikationsnummer bereits mit der Geburt des Menschen vergeben und er dann beim Bundesamt als Steuerpflichtiger gespeichert wird, stellt die Zentraldatei beim Bundesamt für Finanzen eine

[43] BGBl. I, S. 2928

Form eines Bundesmelderegisters dar, zu dem sich das Bundesverfassungsgericht bereits im Volkszählungsurteil sehr deutlich ablehnend geäußert hatte. Die Datenschutzbeauftragten des Bundes und der Länder haben sich deshalb gegen ein zentrales Identifikationsmerkmal ausgesprochen[44].

Hier erscheint es geboten, die Risiken einer Zentraldatei der Steueridentifikationsnummern auf der Grundlage der verfassungsrechtlichen Bürgerrechte neu zu prüfen. Insbesondere das Gleichgewicht der Rechte gerät immer mehr in eine Schieflage zu Ungunsten des Bürgers.

Das Gesetz zur Förderung der Steuerehrlichkeit wird ab 1. April 2005 Anfragen von Behörden, die in ihrer Tätigkeit an Begriffe des Einkommensteuergesetzes anknüpfen, nach Kontoverbindungen der Bürger über das Bundesamt für Finanzen zulassen. Die Erweiterung des § 93 Abs. 8 AO macht es möglich, dass zukünftig auch andere als Steuerbehörden Auskunftsersuchen, dieses Mal mit Hilfe der Steuerbehörden, in den Bereich des Bankgeheimnisses richten können. Die ursprünglich zum Zwecke der Terrorismusbekämpfung geschaffene Kontenevidenzzentrale bei der Bundesanstalt für Finanzdienstleistungsaufsicht wird keine zwei Jahre später einer breiten Nutzungsmöglichkeit hinter dem Rücken der Banken sowie der datenschutzrechtlich Betroffenen geöffnet. Rechtsstaatliche Schranken gibt es so gut wie keine. Das Prinzip, der Zugriff auf die Bankdaten dürfe nur durch einige wenige im Gesetz ausdrücklich genannte Stellen unter enger Zweckbindung begrenzt werden, wurde außer Kraft gesetzt.

Diese Bestimmung durchbricht zudem das Regelungsgefüge der *Abgabenordnung*, in dem die Finanzbehörden erstmals als Mittler ohne eigene Verantwortung auftreten. Offen ist, wie viele Behörden bei ihrer Tätigkeit tatsächlich an Begriffe des Einkommensteuergesetzes anknüpfen. Gemeint ist offensichtlich nicht nur der Begriff „Einkommen“. Aber welche Begriffe gibt es noch? Von dem neuen Recht Gebrauch machen können in erster Linie die klassischen Leistungsträger wie Sozialleistungsbehörden, Wohngeldbehörden, Sozialgesetzbuch-II-Behörden, Bafög-Behörden, Asylbewerberleistungsbehörden; auch das Kitagesetz ist betroffen, das Prozesskostenhilfegesetz, das Erziehungsgeld sowie Versorgungsgesetze, die auf den Einkommensbegriff abstellen. Die Anknüpfung an Begriffe des Einkommensteuergesetzes ist jedenfalls nicht bestimmt genug. § 93 Abs. 8 AO weist nicht ausdrücklich darauf hin, dass die anfragende Behörde eine ausdrückliche Erhebungsbefugnis für eine Datenerhebung, die nicht beim Betroffenen erfolgt, benötigt. Dies ist jedoch der Fall. Es fehlen Regelungen zur Verhältnismäßigkeit sowie zur Zweckbindung, die sicherstellen, dass die anfragenden Behörden die abgefragten Kontendaten nicht noch zu weiteren Zwecken nutzen können, sowie zur Protokollierung der Abfragen und zur Löschung der erhobenen Daten. Da weder der Bürger noch die abgefragte Bank von dieser Datenerhebung Kenntnis erhalten, können diese die ein-

[44] Entschließung „Personennummern“ der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2004“, S. 12

zelnen Abrufe nicht gerichtlich überprüfen lassen. Auch die gesetzlich geregelte Protokollierung der Abrufe droht ins Leere zu laufen. Da auch noch immer kein Anspruch auf Akteneinsicht besteht, werden die Rechte der unmittelbar Betroffenen auf nicht akzeptierbare Weise beschnitten. Die Datenschutzbeauftragten des Bundes und der Länder haben daher auch in ihrer Entschließung dringend eine datenschutzrechtliche Überarbeitung der Vorschriften angemahnt[45].

Fraglich ist, ob die Steuerehrlichkeit tatsächlich in den letzten fünf Jahren so gesunken ist, dass der Staat die Persönlichkeitsrechte in diesem Ausmaß einschränken müsste. In der Steuerverwaltung entsteht ein immer größeres Ungleichgewicht zwischen staatlichen Rechten und Bürgerrechten. Es werden einseitig die staatlichen Rechte gestärkt, ohne dass es ein Gegengewicht in der Gesetzgebung zugunsten der Bürger geben würde. Ob Steuergerechtigkeit durch diesen Weg erreicht werden kann, muss offen bleiben. Der Preis ist aus datenschutzrechtlicher Sicht ein hoher.

3.3 Datenschutz in Detekteien

Bei einem ersten Blick in die Gelben Seiten unter *„Detekteien“* kann man feststellen, dass Detektive ihre Dienstleistung für die verschiedensten Lebensbereiche anbieten. Bei Familie und Partnerschaften ermitteln Detektive die Anschrift und die Vermögensverhältnisse von Unterhaltsverpflichteten, bei Partnerschaft oder Ehe kann man sich über den Lebenswandel und insbesondere die Treue seines Partners informieren, Verfehlungen können auch nach der Abschaffung des Schuldprinzips bei Unterhalt, Versorgungsausgleich und elterlicher Sorge Berücksichtigung finden. Besonders vorsichtige Verlobte lassen nach dem Grundsatz „Drum prüfe, wer sich ewig bindet“ vor der Hochzeit die Braut/den Bräutigam überprüfen.

Ähnlich vorsichtig sind Arbeitgeber, die Bewerber vor der Einstellung durch Detekteien überprüfen lassen. Bei einem bestehenden Arbeitsverhältnis wird erforscht, ob der krankgemeldete Arbeitnehmer tatsächlich erkrankt ist oder ob er sich für die Verrichtung von Schwarzarbeiten oder Freizeitaktivitäten „freigenommen hat“. Da der Arbeitgeber insbesondere bei Arbeitnehmern im Außendienst keine ausreichende Leistungsüberprüfung vornehmen kann, bieten Detekteien speziell die Überwachung von Außendienstmitarbeitern an. Auch bei Diebstählen oder Sabotage im Unternehmen werden Detektive eingeschaltet. Detektive ermitteln außerdem bei Patentmarken und Produktpiraterie, beim Verrat von Betriebs- und Geschäftsgeheimnissen sowie bei Verstößen gegen den unlauteren Wettbewerb. Auskünfte werden erteilt über Herkunft, Vorleben, Lebenswandel, Ruf und Einkommen einer bestimmten Person, teilweise wird die Beschaffung von Informationen *aller* Art in Aussicht gestellt. Als Ermittlungsmethoden werden von

[45] Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Steuergesetzgebung „Staatliche Kontrolle muss auf den Prüfstand!“, vgl. Anlagenband, a.a.O., S. 19

den Detekteien unter anderem Beobachtungen, Ermittlungen, verdeckte Videoüberwachung, Kriminaltechnik, technische Sonderlösungen benannt.

Während die Kunden von Banken und Versicherungen großen Wert darauf legen, dass ihr Vertragspartner die datenschutzrechtlichen Vorgaben beachtet, ist es das primäre Ziel des Kunden einer Detektei, an bestimmte Informationen zu gelangen. Welche Ermittlungsmethoden der Detektiv angewandt hat und ob diese nach dem Bundesdatenschutzgesetz überhaupt zulässig sind, ist für den Kunden meistens nur von untergeordneter Bedeutung. Für viele Kunden ist es nur wichtig, dass die Informationen der Detektei gerichtsverwertbar sind. Da ein Beweiserhebungsverbot nach den verschiedenen Prozessordnungen nicht automatisch zu einem Verwertungsverbot führt, vielmehr die erlangten Folgeerkenntnisse im Gegensatz etwa zum amerikanischen Recht (fruits of the poisoned tree) im Prozess nutzbar sind, ist der datenschutzrechtliche Standard von beweisverwertbaren Informationen nicht sehr hoch. Auch die Detektive selbst gehen davon aus, dass sie gegen das Datenschutzrecht verstoßen. Nur so ist es zu erklären, dass Detektive mit allen Mitteln versuchen, Kontrollen der Aufsichtsbehörde zu verhindern oder den Termin der Kontrolle zumindest hinauszuzögern; mal befand sich der Inhaber der Detektei in einem mehrmonatigen Urlaub, ein anderes Mal musste die vorgesehene Kontrolle wegen einer plötzlichen Erkrankung oder eines kurzfristigen Gerichtstermins verschoben werden.

Die Mehrzahl der Detekteien ermittelt personenbezogene Daten – in der Regel von bestimmten Zielpersonen –, um diese in einem Abschlussbericht an den Kunden zu übermitteln. Danach stellt die Arbeit der Detekteien in der Regel eine geschäftsmäßige Datenerhebung und -speicherung zum Zwecke der Übermittlung (§ 29 BDSG) dar. Nur einige wenige Detekteien arbeiten nicht nach dieser Vorschrift, etwa dann, wenn sich ein Detektiv auf das Aufsuchen gestohlener Pkws spezialisiert hat, oder ein Ladendetektiv, dessen Aufgabe darin besteht, Ladendiebstähle zu verhindern und Ladendiebe festzunehmen.

Automatisierte Verarbeitungen, in denen geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle zum Zwecke der Übermittlung gespeichert werden, sind vor ihrer Inbetriebnahme der zuständigen Aufsichtsbehörde nach den Maßgaben des § 4 e Nr. 1 – 9 BDSG zu melden (§ 4 e Abs. 1 i.V. m. § 4 g Abs. 2 BDSG). Die geringe Anzahl der zum Register gemeldeten Detekteien lässt die Vermutung zu, dass viele Detektive die Meldepflicht nicht beachten.

Vor der Annahme eines Ermittlungsauftrags müssen die Detekteien prüfen, ob der Kunde, dem die Ermittlungsergebnisse übermittelt werden sollen, ein berechtigtes Interesse an der Kenntnis dieser Daten glaubhaft dargelegt hat und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat (§ 29 Abs. 2 Nr. 1 a und Nr. 2 BDSG). Detekteien haben natürlich kein Interesse daran, diese Rechtsvorschrift umzusetzen, da sie hierdurch Mandate verlieren. Teils wird diese Bestimmung überhaupt nicht beachtet, teils wird das

Vorliegen eines berechtigten Interesses sehr weit ausgelegt. Ein Detektiv behauptete, das berechtigte Interesse ergebe sich daraus, dass der Kunde für die Information schließlich Geld zu zahlen habe, in einem anderen Fall ging eine Detektei davon aus, dass ein berechtigtes Interesse immer dann vorläge, wenn ein Anwalt eine Information einholte.

Der Kunde einer Detektei wird in vielen Fällen ein berechtigtes Interesse an der Kenntnis der erwünschten Information haben. Ein Unterhaltsberechtigter – aber auch jeder andere Gläubiger – hat ein Interesse daran, den Aufenthaltsort eines flüchtigen Schuldners zu ermitteln und festzustellen, ob er über Vermögenswerte und Einkommen verfügt, in welches vollstreckt werden kann. Ein Arbeitgeber hat das Recht, wegen Fehlbeträgen in der Kasse detektivische Hilfe in Anspruch zu nehmen.

In anderen Fällen ist das Recht des Kunden auf Informationserlangung beschränkt. Die Krankschreibung eines Mitarbeiters gibt dem Arbeitgeber noch nicht das Recht, die Korrektheit durch einen Detektiv überprüfen zu lassen. Dieses Recht besteht erst, wenn der Arbeitgeber zumindest über gewisse Hinweise verfügt, dass der Arbeitnehmer „krankfeiert“, etwa um schwarzzuarbeiten. Da es bei der Einstellung neuer Mitarbeiter vereinzelt vorkommt, dass Bewerber gefälschte Zeugnisse und Dokumente vorlegen, darf ein Arbeitgeber die von dem Bewerber eingereichten Unterlagen durch einen Detektiv auf ihre Echtheit überprüfen lassen. Da die Detekteien hier Informationen von öffentlichen Stellen einholen müssen, ist es sinnvoll, sich vor der Überprüfung die Einwilligung des Bewerbers geben zu lassen. Da der Arbeitgeber aber keinen Anspruch auf einen bestimmten „Lebenswandel“ seiner Mitarbeiter hat, hat er kein berechtigtes Interesse daran, bestimmte Informationen aus dem Privatleben seines zukünftigen Mitarbeiters zu erhalten. Dies gilt auch bei der Besetzung von Führungspositionen.

Bei der Ermittlungstätigkeit müssen Detektive die Datenerhebungsvorschriften (§ 4 Abs. 2 und 3 BDSG) beachten. Die Einhaltung dieser Vorschriften fällt Detekteien besonders schwer. Um an Informationen zu gelangen, arbeiten Detektive häufig mit so genannten Legenden. Sie offenbaren sich nicht als Detektive, sondern geben sich etwa als Erbenermittler oder Versicherungsvertreter aus, um von der Zielperson oder einem Dritten bestimmte Informationen zu erlangen. Teilweise geben sich Detektive auch – etwa gegenüber Behörden – als der Betroffene selbst aus. Auf unsere Frage an einen Detektiv, ob sein Unternehmen Legenden verwenden würde, antwortete dieser: „Wir arbeiten ausschließlich mit Legenden, sonst könnte ich meinen Laden dichtmachen.“

Die Verwendung von *Legenden* ist dann rechtswidrig, wenn ihr Inhalt eine Amtsanmaßung darstellt, etwa wenn sich der Detektiv als Beamter bei der Bundesversicherungsanstalt für Angestellte vorstellt. Das Gleiche gilt, wenn eine Detektei mittels einer Legende an Daten von einer Stelle gelangt, die diese nicht an Detekteien übermitteln dürfte. Danach darf diese sich nicht als der Betroffene ausgeben und bei der Bank den Kontostand oder in einer

Arztpraxis die Diagnose abfragen. Auch die Datenerhebung bei der Zielperson selbst unter Verwendung einer Legende ist rechtswidrig. Auch der Betroffene, bei dem personenbezogene Daten erhoben werden, ist von der verantwortlichen Stelle über die Identität der verantwortlichen Stelle sowie die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung zu informieren (§ 4 Abs. 3 Nr. 1 und 2 BDSG).

Die Befragung Dritter ist zulässig, wenn der Geschäftszweck die Erhebung bei Dritten erfordert (§ 4 Abs. 2 Nr. 2 a BDSG). Der Ausnahmetatbestand „Erforderlichkeit für Geschäftszwecke“ ist eng auszulegen. Er greift nur, wenn im Einzelfall keine Anhaltspunkte dafür bestehen, dass dadurch überwiegende schutzwürdige Interessen der betroffenen Person beeinträchtigt werden. Allerdings kann auch der Geschäftszweck von Detekteien zu einer Datenerhebung bei Dritten berechtigen. Ist dies zu bejahen, hat jedoch immer noch eine Interessenabwägung im Einzelfall stattzufinden. Bei der Befragung in der Nachbarschaft ist insbesondere zu berücksichtigen, dass hier besonders stark in die Privatsphäre des Betroffenen eingegriffen wird. Ist die Befragung Dritter gestattet, stellt die Benutzung von Legenden häufig sogar ein milderes Mittel dar, da den Dritten der Zweck der Datenerhebung, wie möglicherweise die Aufklärung eines kriminellen Verhaltens, verschwiegen bleibt und damit der Eingriff in die Privatsphäre des Betroffenen geringer ist.

Auch bei der Anwendung technischer Überwachungsmethoden enthält das Bundesdatenschutzgesetz Einschränkungen. So ist eine heimliche Videoüberwachung öffentlich zugänglicher Räume nach § 6 b Abs. 2 BDSG rechtswidrig. Nicht unter § 6 b BDSG fällt die heimliche Videoüberwachung eines beweglichen Ziels, etwa einer bestimmten Zielperson. Bei der Frage, ob diese rechtmäßig ist, sind die Interessen des Kunden der Detektei und die der Zielperson gegeneinander abzuwägen. Zu berücksichtigen ist, zu welchem Zweck die Videoüberwachung dient.

Bestehen bei der Aufsichtsbehörde Zweifel an der Rechtmäßigkeit der Datenerhebung, kann sie dies häufig nicht belegen, wenn die Detekteien die Herkunft der Daten nicht speichern. In diesem Fall hat die Aufsichtsbehörde das Recht, nach § 38 Abs. 5 Satz 1 BDSG anzuordnen, dass die verantwortliche Stelle die notwendigen Maßnahmen dazu trifft, überprüfen zu können, von welchem Mitarbeiter welche Information wann und wie ermittelt worden ist[46].

Bei der Erstellung des Abschlussberichts wollen die Detekteien häufig gegenüber dem Kunden dokumentieren, wie umfangreich ihre Arbeit zur Durchführung des Auftrags war. Aus diesem Grunde erstellen Detektive häufig sehr „ausschweifende“ Abschlussberichte. Wie bei der Frage, ob die Detektei das Mandat überhaupt annehmen darf, ist auch bei den einzelnen übermittelten Daten nach § 29 Abs. 2 Nr. 1 a und 2 BDSG zu prüfen, ob der Kunde ein berechtigtes Interesse an der Kenntnis dieses Datums hat und ob

[46] JB 2003, 4.6.3

Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. In der Regel hat der Betroffene überwiegende schutzwürdige Interessen daran, dass Detekteien nur Tatsachen, nicht jedoch – dies geschieht nicht selten – Vermutungen übermitteln. Informationen, die der Kunde für den von ihm benannten Zweck nicht benötigt, dürfen in einem Abschlussbericht nicht übermittelt werden. So war es für eine Reiserücktrittsversicherung ohne Belang, dass die Zielperson (Verdacht des Versicherungsbetrugs) im Arbeitsamt als „problematisch“ eingestuft worden sei, ebenso, dass ein Zeuge mit ausländischem Akzent gesprochen habe.

Detektive machen häufig Werbung damit, dass sie diskret arbeiten, d. h. in der Regel, dass die Zielperson weder vor noch während noch nach Erledigung des Auftrags Informationen über die Beauftragung einer Detektei erhält. Demgegenüber regelt § 33 Abs. 1 Satz 2 BDSG, dass Detekteien den Betroffenen von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen haben. Das Recht auf Benachrichtigung ist ein sehr wesentliches Element des informationellen Selbstbestimmungsrechts, da nur hierdurch Betroffene in die Lage versetzt werden, ihre datenschutzrechtlichen Rechte (Auskunft, Berichtigung, Löschung etc.) durchzusetzen.

Nur in Ausnahmefällen kann auf eine Benachrichtigung verzichtet werden. Nach § 33 Abs. 2 Nr. 1 BDSG besteht eine Pflicht zur Benachrichtigung dann nicht, wenn der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat. Dies ist etwa der Fall, wenn der Kunde die Zielperson – etwa im Rahmen eines Zivilprozesses – über die Beauftragung der Detektei informiert. Eine Pflicht zur Benachrichtigung besteht ferner nicht, wenn die Daten ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen (§ 33 Abs. 2 Nr. 3 BDSG). Dritter kann auch der Kunde (Datenempfänger) der Detektei sein. Ein Entfallen der Benachrichtigungs- (und Auskunfts-)pflicht kommt aber nur in Betracht, wenn das Bekanntwerden des Datenempfängers seine Geschäftszwecke bzw. Rechte erheblich gefährden würde. Erforderlich sind konkrete *rechtliche* Gründe, eine bloße Vereinbarung zwischen Detektei und Kunde, dass der Vorgang „diskret“ behandelt wird, ist demgegenüber als „Vertrag zu Lasten Dritter“ ohne Bedeutung. Nach § 33 Abs. 2 Satz 2 BDSG hat die verantwortliche Stelle schriftlich festzulegen, unter welchen Voraussetzungen von einer Benachrichtigung abgesehen wird.

3.4 RFID – eine Technologie setzt sich durch

Der Einstieg in die bereits beschriebene *RFID-Technik* wird über die automatische Identifikation von Produkten und die Erfassung ihrer Daten erfolgen. Sie fungiert als attraktive und zukunftsweisende Ergänzung zur herkömmlichen Strichcodetechnologie. RFID hat einen entscheidenden Vorteil gegenüber dem Strichcode: Jedes Produkt kann individuell mit dieser Technik ausgestattet und ohne Sichtkontakt erkannt und identifiziert werden.

RFID-Tags bestehen mindestens aus einem Speicherchip, der z. B. Produktinformationen wie Produktcode und Herstellungs- bzw. Haltbarkeitsdatum enthält, und einer Antenne. Chip und Antenne gibt es in verschiedenen Ausführungen und Bauformen, die entsprechend ihren jeweiligen Einsatzzwecken angepasst werden können. RFID-Tags funktionieren nach dem Prinzip eines Transponders, bei dem die Tags über elektromagnetische Wellen „angesprochen“ und ihre Informationen ausgelesen werden. Dabei übermitteln sie ihre Identität dem Lesegerät, welches die Anfrage initiiert hat. Die Entfernung, über die ein RFID-Tag ausgelesen werden kann, schwankt aufgrund der Ausführung, benutztem Frequenzbereich, Sendestärke und Umwelteinflüssen zwischen wenigen Zentimetern und maximal 30 Metern. RFID-Tags gibt es prinzipiell in zwei Ausführungen: Aktive RFID-Tags haben eine eigene Stromversorgung, meistens eine Batterie. Ihr Speicherchip kann sowohl gelesen als auch beschrieben werden. Passive RFID-Tags hingegen beziehen ihre Energie zur Übertragung der Information aus den empfangenen Funkwellen eines Lesegeräts. Die gespeicherten Daten können nur gelesen werden, außerdem ist die Speicherkapazität wesentlich geringer als bei aktiven Tags.

Um einzelne Gegenstände mit Hilfe von RFID-Tags zu identifizieren, müssen sie in ein RFID-System eingebunden werden. Die zurzeit verfügbaren Systeme bestehen in der Regel aus folgenden Komponenten:

- dem Transponder, der an das zu identifizierende Objekt angebracht wird und die zu übermittelnden Informationen enthält,
- dem Schreibgerät zum Schreiben von Daten auf den Transponder und
- dem Lesegerät, welches die im Transponder enthaltenen Informationen ausliest.

Schreib- und Lesegerät können zu einer Einheit zusammengefasst werden. Diese Einheit wird in der Regel mit einer zusätzlichen Schnittstelle ausgestattet, um die vom RFID-Tag empfangenen Daten an ein Hintergrundsystem (z. B. Datenbank, Automatensteuerung) weiterzuleiten[47].

RFID-Standards

Bis heute gibt es keinen gemeinsamen weltweiten RFID-Standard. In Europa und den USA basiert die Entwicklung der Technologie auf verschiedenen Grundlagen. Die europäischen Strich- bzw. Barcodes enthalten die EAN (*European Article Number*), eine Produktnummer für Handelsartikel, die Produktgruppen kennzeichnet. Diese Nummer unterscheidet sich grundsätzlich vom amerikanischen Produktcode UPC (*Universal Product Code*).

[47] Finkenzeller, Klaus: RFID-Handbuch: Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten. 3. Aufl. München: Carl Hauser Verlag, 2002

Nachfolger beider soll im Rahmen weltweiter RFID-Standards der EPC (*Electronic Product Code*) werden, welcher weltweit eindeutige Produktnummern ausweist. Wegbereiter für diese Standardisierungsinitiative ist die Interessengemeinschaft EPCglobal[48]. Im Gegensatz zur bisher verwendeten EAN hat der EPC mit einer Länge von 96 Bit eine ausreichende Kapazität, um Unternehmen 16 Millionen Objektklassen für ihre Produkte zur Verfügung zu stellen. In jeder Objektklasse lassen sich wiederum bis zu 68 Milliarden eindeutige Seriennummern vergeben. Der EPC kann auch auf einfachen passiven RFID-Tags gespeichert werden. Mit entsprechend leistungsfähigen Datenbanken im Hintergrund soll es somit möglich sein, jedes Produkt weltweit eindeutig zu identifizieren.

Szenarien und Einsatzgebiete

Die RFID-Technologie ist vielseitig einsetzbar und wird in der einfachen Form im Alltag bereits eingesetzt. Als Diebstahlsicherung in Geschäften und Kaufhäusern werden RFID-Tags schon seit langem verwendet, wobei sie z. B. in Etiketten von *Bekleidung* in ca. drei bis fünf Zentimeter große Hartplastikscheiben integriert werden können. Diese enthalten einen winzigen 1-Bit-Transponder, der mit dem Bezahlen der Ware entfernt oder deaktiviert wird. Sollte ein Kunde das Geschäft mit einem aktiven Etikett verlassen wollen, so lösen Lesegeräte im Ausgangsbereich einen akustischen oder optischen Alarm aus.

Eine Diebstahlsicherung kann auch als Wegfahrsperre bei *Kraftfahrzeugen* eingesetzt werden. Der RFID-Tag wird dabei in den Autoschlüssel integriert und das Lesegerät in die Nähe des Zündschlosses platziert. Ohne Schlüssel kann ein solches Fahrzeug nicht mehr gestartet werden. Auch das Fälschen eines Autoschlüssels wird durch kryptografische Verfahren zur Authentifizierung zwischen Schlüssel und Fahrzeug verhindert.

Ein weiteres Anwendungsgebiet für RFID-Technologie sind *Zutrittskontrollsysteme*. Das Passieren einer mit einem Lesegerät gesicherten Tür wäre bei ausreichender Reichweite des Transponders möglich, ohne dass dieser aus der Tasche geholt werden muss. Mittlerweile sind solche Transponder auch in Skipässen eingebaut, um eine berührungslose und schnelle Zutrittskontrolle bei den Skiliften zu ermöglichen.

Gleichzeitig könnten solche Transponder auch zur *Zeiterfassung* dienen, die damit weitgehend automatisiert werden kann. In diesem Zusammenhang finden RFID-Systeme bei Sportveranstaltungen und im Bankwesen Anwendung. So können Transponder in die Schuhe von Marathonläufern integriert werden, um auch bei großer Teilnehmerzahl die zurückgelegte Strecke und die benötigte Zeit exakt zu messen. Zur Fußballweltmeisterschaft 2006 in Deutschland sollen die Eintrittskarten mit RFID-Tags versehen werden, um

[48] www.epcglobalinc.org

Ticketfälschungen zu erschweren und sicherzustellen, dass nur Personen, die ihr Ticket offiziell erworben haben, Zugang zu den WM-Stadien haben. Die Europäische Zentralbank (EZB) erwägt, ab 2005 in Euro-Scheine Transponder zu integrieren, um ebenfalls Fälschungen zu erschweren und die Geldzirkulation besser kontrollieren zu können.

In *Bibliotheken* und Büchereien könnten Informationen wie Exemplarnummer, Autor, Bibliothekskennung, Standort in der Bibliothek, Systematikgruppe, Status (entliehen, bestellt) in RFID-Tags enthalten sein und würden somit zur schnellen Erfassung und Auffindbarkeit einzelner Bücher aus dem Medienbestand beitragen.

RFID-Systeme haben sich bereits als sehr hilfreich bei der Identifikation von *Tieren* erwiesen. Statt mit Markierungen wie Brandzeichen oder Tätowierungen werden Rinder und Schafe inzwischen mit Transpondern, die eine Seriennummer gespeichert haben, ausgestattet. Diese können sich in Ohrmarken oder Halsbändern der Tiere befinden. Darüber hinaus erleichtert die kontaktlose automatische Identifikation den Herkunftsnachweis, die Güteklasse, den Gesundheitszustand und den Transport der Tiere. Eine individuelle Erfassung ist damit möglich, die unter anderem die Fütterung automatisiert und optimiert. Das im vergangenen Jahr verabschiedete Berliner Hundegesetz schreibt vor, dass künftig Hunde in Berlin einen derartigen Chip tragen müssen[49].

Forschung, Entwicklung, Pilotprojekte

Der bisherige Einsatz von Transponder-gestützten Identifikationssystemen beschränkt sich auf Pilotprojekte und Testphasen einiger Forschungsunternehmen in Kooperation mit Konzernen der Konsumgüterindustrie, aber auch im Logistikbereich von Großhandel und Lagern werden RFID-Tags auf ihre Funktionsfähigkeit getestet. Der konkrete Einsatz im Alltag ist dabei noch die Ausnahme, kommt aber im kleineren Rahmen bereits vor.

Seit April 2003 entwickelt ein Handelskonzern gemeinsam mit drei großen IT-Unternehmen einen *Supermarkt* der Zukunft. Im einem nordrhein-westfälischen Supermarkt wird unter realen Bedingungen der Einsatz und die Akzeptanz der RFID-Technologie im Handel getestet. Das Ziel sind nutzerorientierte Lösungen, die sowohl dem Handel als auch dem Kunden Vorteile bringen sollen. Darüber hinaus sollen mit Hilfe dieser Technologie Prozessabläufe optimiert und Kosten gesenkt werden.

Allerdings äußerten im Februar 2004 die Bielefelder Datenschutzaktivistengruppe *FoeBuD* (Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e. V.) wie auch schon die US-amerikanische Verbraucherorganisation *Caspian* (Consumers Against Supermarket Privacy

[49] vgl. 4.4.2

Invasion And Numbering) große Bedenken hinsichtlich der Kundenaufklärung im Supermarkt. Der Konzern hatte die Verbraucher nicht ausreichend über den Einsatz der RFID-Technologie informiert. Verschiedene Produkte waren mit RFID-Etiketten bestückt worden, ebenso enthielten die Kundenkarten Transponder, mit denen ein Bezug zwischen Produkt und Kunde hergestellt werden konnte. Über die Risiken für die Privatsphäre gab es im Supermarkt keine Hinweise.

Besonders bemerkenswert ist, dass die am RFID-Einsatz als Produzenten, Systementwickler und Anwender interessierten Unternehmen bei Einwänden, die Befürchtungen für die Persönlichkeitsrechte zum Inhalt haben, stets betonen, dass diese Befürchtungen grundlos sind, weil es nur um die Verarbeitung produktbezogener Daten ginge. Eine Gefahr für die Persönlichkeitsrechte könne nur dann bestehen, wenn die produktbezogenen Daten mit personenbezogenen Angaben von Käufern oder Benutzern der Produkte zusammengeführt werden. Ausgerechnet beim ersten wichtigen Feldversuch dieser Technologie sollte genau dies geschehen – ohne Wissen der Betroffenen.

Wertvolle Rasierklingen sind vergleichsweise teuer und können wegen ihrer geringen Größe leicht gestohlen werden. Aus diesem Grund hat ein Hersteller die Verpackungen seiner Rasierklingenmarke mit RFID-Chips versehen. Ein Pilotprojekt lief im Juli 2003 bei einer britischen Supermarktkette. Caspian hatte herausgefunden, dass der Supermarktbetreiber zusätzlich jeden Kunden heimlich fotografierte, der nach den mit RFID-Tags ausgestatteten Rasierklingen griff. Auch an den Kassen waren Kameras postiert, die alle Kunden filmten, die mit einer RFID-gekennzeichneten Ware den Laden verließen. Diese Bilder wurden dann von einem Sicherheitsdienst mit den Fotos vom Rasierklingen-Regal verglichen.

Ein italienischer Bekleidungshersteller plant, RFID-Tags künftig in seine Produkte einzunähen, die eine chemische Reinigung überstehen sollen. Der 22 mm große ultradünne Transponder verfügt über einen 2-kBit-Speicher und soll Kleidungsstücke eindeutig und fälschungssicher identifizierbar machen. Auf den Transpondern können Daten über Größe, Stil, Farbe und Bestimmungsort gespeichert werden.

Ein nordamerikanischer Internet-Dienstleister entwickelt seit einigen Jahren eine in den menschlichen Körper implantierbare Datenübertragungseinheit auf Basis der RFID-Technologie. Der *VeriChip* (Verification Chip) wird in den Medien auch Digital Angel genannt. Er besteht aus einer Sende- und Empfangseinheit und soll mit einer elektromagnetischen Energieversorgung ausgestattet sein, die den notwendigen Strom aus Muskelbewegungen des Körpers gewinnt. Die Einheit soll an das satellitengestützte Global Positioning System (GPS) angebunden werden, das den Träger des Geräts jederzeit lokalisieren könne. Das Unternehmen nennt das Lokalisierungssystem auch Global VeriChip Subscriber (GVS). Es bestünde die Möglichkeit, damit Gesundheitsdaten von Personen zu messen. Bestimmte Risiko-Patienten,

wie z. B. Zuckerkranke, Alzheimer-Kranke, aber auch verschwundene oder verwirrte Menschen sowie Strafgefangene im offenen Vollzug könnten mit dieser Technologie ausgestattet werden.

Datenschutzrechtliche Aspekte

Obwohl sich der Einsatz der RFID-Technologie bisher hauptsächlich auf logistische und distributive Bereiche beschränkt und nur in vereinzelten Pilotprojekten mit personenbezogenen Daten getestet wird, ist in den nächsten Jahren mit einer Einführung auf breiter Ebene zu rechnen.

Zusammenfassend ergeben sich für den Datenschutz folgende Risiken:

– RFID-Systeme arbeiten drahtlos, so dass das Auslesen der Daten ohne Wissen des Besitzers erfolgen kann.

– RFID-Tags werden in Bauformen angeboten, die ein verstecktes Anbringen auf Waren ermöglichen. Der Käufer kann keine Schutzmaßnahmen ergreifen, wenn er über die Existenz des RFID-Tags nichts weiß.

– RFID-Tags ermöglichen eine weltweit eindeutige Kennzeichnung von einzelnen Gegenständen. Erworbene Produkte könnten somit weltweit eindeutig einzelnen Personen zugeordnet werden.

– Durch die Zusammenführung der Informationen aus RFID-Tags mit personenbezogenen Daten (z. B. aus Kundenkarten) lässt sich das Kaufverhalten einzelner Kunden detailliert analysieren.

Daraus folgt die Forderung nach folgenden Maßnahmen:

- Die betroffenen Personen müssen umfassend über Einsatz, Verarbeitungszweck und Inhalt von RFID-Chips informiert werden.
- Kommunikationsvorgänge mit RFID-Chips, die eine Verarbeitung personenbezogener Daten auslösen, müssen für die betroffenen Personen transparent und eindeutig erkennbar sein.
- Daten auf RFID-Chips dürfen nur so lange gespeichert sein, wie es zur Erreichung des Zwecks erforderlich ist.
- Möglichkeiten zur Deaktivierung bzw. Löschung der Daten von RFID-Chips müssen geschaffen werden.
- Die Vertraulichkeit der gespeicherten und der übertragenen Daten muss durch wirksame Authentisierung der beteiligten Peripheriegeräte und durch Verschlüsselung sichergestellt werden.
- Bei RFID-Technologie mit Verarbeitungsfunktion müssen Systeme angeboten werden, die keine Seriennummern tragen.

Reaktionen

Auf der Basis der Verarbeitung der von uns geleiteten Internationalen Arbeitsgruppe Datenschutz in der Telekommunikation hat die Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre in Sydney am 20.11.2003 in einer gemeinsamen Entschließung auf die Risiken der RFID-Technologie hingewiesen. Folgende Grundsätze wurden im Einzelnen formuliert:

- Jeder Datenverarbeiter sollte vor der Einführung von RFID-Etiketten, die mit personenbezogenen Daten verknüpft sind oder die zur Bildung von Konsumprofilen führen, zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen erreichen.
- Falls der Datenverarbeiter darlegen kann, dass personenbezogene Daten unverzichtbar sind, müssen diese offen und transparent erhoben werden.
- Personenbezogene Daten dürfen nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und sie dürfen nur so lange aufbewahrt werden, wie es zur Erreichung dieses Zwecks erforderlich ist.
- Soweit RFID-Chips im Besitz von Personen sind, sollten diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung bzw. Zerstörung der Chips haben.

Auf nationaler Ebene wurde auf der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 der im Wesentlichen auf deutsche Initiative verabschiedete internationale Beschluss übernommen[50]. Weiterhin wurde beschlossen, eine Informationsschrift zu entwickeln, die als Leitfaden sowohl Anwendern (z. B. Handelskonzernen) als auch Trägern (Käufern, Konsumenten) von RFID-Chips dienen soll und neben RFID-Szenarien und deren datenschutzrechtlicher Bewertung auch die Technik und mögliche Risiken umfasst. Diese Arbeit, die unter der Federführung des Bundesbeauftragten für den Datenschutz entsteht, ist noch nicht abgeschlossen.

Ende Mai 2004 nahm die Bundesregierung erstmals offiziell Stellung zum Thema RFID. Vorausgegangen war dieser Stellungnahme eine Kleine Anfrage einer FDP-Bundestagsabgeordneten, ob die Bundesregierung durch die Ermöglichung von Bewegungsprofilen besondere Missbrauchsgefahren hinsichtlich des Einsatzes von RFID-Technologie sehe. Nach Auffassung der Bundesregierung deckt das Bundesdatenschutzgesetz auch die neuen Fragen hinsichtlich der Funkidentifikation ab. Eine Kombination aus Produkt- und Käuferdaten werde von Unternehmen in Deutschland nach Kenntnis der

[50] Entschließung „Radio-Frequency Identifikation“, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2004“, S. 12

Bundesregierung nicht eingesetzt. Aus diesem Grund sei nach dem gegenwärtigen Stand der Technik im Bereich der elektronischen Produktlabel kein ergänzender datenschutzrechtlicher Regelungsbedarf erkennbar.

Der Bundesbeauftragte für den Datenschutz sieht allerdings Regelungsbedarf. Er fordert eine Änderung des Datenschutzgesetzes zur Regulierung der RFID-Chips. Dazu gehören eine Kennzeichnungspflicht für Produkte mit Chips und das Recht, die darin gespeicherten Informationen einsehen zu können und den Chip nach dem Kauf permanent deaktivieren zu lassen. Bislang würden RFID-Chips vom Gesetz nicht erfasst: Theoretisch müssen Unternehmen ihre Kunden nicht darüber informieren, wenn sie Chips in Produkte integrieren – sondern erst dann, wenn sie persönliche Daten damit verknüpfen. Dritte, die die Chips ebenfalls unbemerkt auslesen könnten, seien von einer solchen Regelung ohnehin nicht betroffen.

3.5 Drahtlose Netze

Drahtlose Kommunikation bietet zahlreiche Vorteile wie Portabilität und Flexibilität, erhöhte Produktivität sowie niedrigere Installationskosten und wird deshalb zunehmend populär. Sie deckt eine breite Auswahl unterschiedlicher Funktionen ab, ausgerichtet auf verschiedene Anwendungen und Bedürfnisse. Drahtlose lokale Netzwerke (Wireless local area networks – WLAN) erlauben den Nutzern z. B., sich mit mobilen Systemen innerhalb der Reichweite des Netzes zu bewegen, ohne dass dafür Kabel notwendig wären und die Verbindung verloren geht.

Kostenintensive Baumaßnahmen durch das Verlegen von Kabeln entfallen. Insbesondere bei einem Umzug werden die Vorteile besonders deutlich. Anstelle einer sorgfältigen Planung der Verkabelung, die meist sehr wohl überlegt und damit auch aufwendig ist, ist beim heutigen Preisverfall ein *WLAN* schnell installiert. Allerdings führen Fehler bei der Installation oft zu Sicherheitslücken oder unzureichender Netzabdeckung. Es gibt viele Risiken bei der Nutzung von drahtloser Technologie, weil die Funkverbindung für Angriffe offen ist. Gegen diese Risiken sind angemessene Sicherheitsvorkehrungen zu treffen.

Bei drahtlosen Netzen ist es möglich, sich ohne großen Aufwand in ein vorhandenes Netzwerk zu integrieren. Benötigt wird lediglich ein mobiler Rechner, der mit einer Funknetzwerkkarte ausgestattet ist. Sobald sich der Rechner im Empfangsbereich eines Funknetzwerkes befindet, meldet sich dieser automatisch an. Es kommt jetzt darauf an, ob netzseitig geprüft wird, ob diese Anmeldung akzeptiert werden kann oder nicht.

Sicherheitsprobleme und Lösungsansätze

Funkwellen kennen keine räumlichen Barrieren, die das Senden und Empfangen einschränken könnten, wenn man nicht spezielle Sicherheitsvor-

kehrungen trifft. Es fehlt der Schutz des Kabels. Der Parkplatz vor der Firma könnte der Ausgangspunkt eines Angriffs auf das WLAN der Firma sein, für den bei unzureichenden Sicherheitseinstellungen eine Funknetzwerkkarte für das Notebook und eine Richtantenne, mit der die Empfangsmöglichkeiten noch erhöht werden können, ausreichend sind. Die Datenströme können einfach empfangen, aufgezeichnet, manipuliert und verfälscht zurück- oder weitergesendet werden.

Mit den datenschutzrechtlichen Risiken hat sich die Internationale Arbeitsgruppe Datenschutz in der Telekommunikation auf ihrer Frühjahrssitzung am 14./15. April 2004 in Buenos Aires befasst und ein entsprechendes Arbeitspapier verabschiedet[51].

Folgende erste Schritte zur Absicherung eines WLANs sollten vom Administrator unternommen werden. Sie erfordern weder zusätzliche Programme noch Kosten und sind sehr einfach und leicht umzusetzen:

- Da die Geräte bei der Auslieferung mit Standard-Parametern wie z. B. einem „Administrator Passwort“ ausgeliefert werden, müssen diese unverzüglich verändert werden. Anderenfalls wird das Eindringen in ein fremdes Netz einem Hacker sehr erleichtert, da er meist anhand der MAC-Adresse des Access Points den Hersteller herausfinden und sich somit die entsprechenden Handbücher mit den Standardpasswörtern aus dem Internet ziehen kann.
- Mit der Service Set Identity Description (SSID = Netzwerkname) sind gleich zwei Möglichkeiten zur Steigerung der Sicherheit möglich:

  Erstens sollte die SSID umbenannt und so gewählt werden, dass keine Rückschlüsse auf die Organisation möglich sind. Wird beispielsweise der Behördenname verwendet, so kann ein Hacker unmittelbar erkennen, ob in diesem Netz für ihn Daten von Interesse transportiert werden.

  Zweitens sollte die Bekanntgabe der SSID deaktiviert werden. Mit dem Ausschalten der Broadcast-SSID kann das Wireless LAN mit relativ einfachen Mitteln vor „fremden“ Rechnern verborgen werden, es wird sozusagen unsichtbar. Angreifer müssen den Namen des Netzes wissen, damit es angegriffen werden kann. Dieser Schritt kann ohne Mehrkosten durch die örtliche Systemverwaltung vollzogen werden.
- Aktivierung der Wireless Equivalent Privacy (WEP)-Verschlüsselung. Dies soll verhindern, dass ein Abhören der Funksignale möglich ist. Dieses Verschlüsselungsverfahren gilt jedoch nicht als hinreichend sicher, weil erhebliche Fehler in dem WEP-Algorithmus festgestellt wurden. Es sollte daher immer eine LAN-weite zusätzliche Verschlüsselung, beispielsweise IPSec, zum Einsatz kommen.

[51] Arbeitspapier zu potenziellen Risiken drahtloser Netzwerke, vgl. Anlagenband, a.a.O., S. 74

- Die ACL-Zugangskontrollliste dient der Eingabe der eindeutigen MAC-Adresse der Funknetzwerkkarten am Access Point. Dadurch wird die Kommunikation mit anderen – nicht eingetragenen – Funknetzwerkkarten unterbunden. Dies stellt eine sehr einfache Möglichkeit dar, mit Hilfe der Adressfilterung der MAC-Adressen unberechtigte Funknetzclients abzuwehren.
- Durch die Bildung von Subnetzen können Bereiche mit einfachen Mitteln getrennt werden, so dass sensible Teilnetze von anderen Netzen geschützt werden können.
- Nicht benötigte Komponenten sollten deaktiviert sein.
- Die Administration des Access Points sollte ausschließlich über die drahtgebundene Verbindung erfolgen, da sonst die drahtlose Verbindung abgehört werden könnte.

Weiterführende Sicherheitsmaßnahmen

Die Verarbeitung von personenbezogenen Daten in einem Wireless-LAN, das dem Standard 802.11b entspricht, ist ohne den Einsatz zusätzlicher Sicherheitsmaßnahmen nicht zulässig – es sei denn, die Daten weisen nur einen geringen Schutzbedarf auf.

Zur Gewährleistung der Vertraulichkeit, Integrität und Authentizität der übertragenen Daten sind weiterreichende Maßnahmen erforderlich. Die folgende Aufzählung soll kurz aufzeigen, wie eine weitere Reduzierung der Risiken durch technische Maßnahmen erreicht werden kann:

- Die Trennung von Internet, Intranet und WLAN durch eine Firewall sollte obligatorisch sein. Damit werden unberechtigte Zugriffe auf ein Netz oder Netzsegment blockiert. Zwar könnten die übertragenen Daten abgehört werden, aber das interne Netz bleibt hinter der Firewall geschützt.
- Die automatisierte Zuteilung von IP-Adressen (mittels DHCP-Server) sollte unterbunden werden, da ansonsten ein Angreifer – automatisch – eine gültige IP-Adresse zugeteilt bekommt. Bei der nicht automatisierten Vergabe der IP-Adressen muss der Hacker zuerst den IP-Adressraum herausbekommen. Weiterhin sollte darauf geachtet werden, dass der Adressraum nicht zu groß bemessen ist.
- Für die Absicherung des Datenstroms auf der Funknetzstrecke sollte ein VPN- (Virtuell Private Network-) Tunnel aufgebaut werden, der die auszutauschenden Daten zwischen dem WLAN-Client und der Firewall durch Verschlüsselungstechnik – z. B. IPSec – schützt.
- Mit Hilfe eines Radius-Servers kann für eine gesichertere Authentifikation bei der Anmeldung an die Basisstation gesorgt werden.

– Da weder die Firewall noch der VPN-Tunnel einen hundertprozentigen Schutz vor Hackern gewährleistet, kann als zusätzlicher Schutz ein Intrusion-Detection-System (IDS) eingesetzt werden. Damit kann der Versuch eines Einbruchs z. B. dem Administrator rechtzeitig angezeigt werden.

– Letztlich darf natürlich auch die Sicherheit der Clients am WLAN nicht vergessen werden, da der Komfort dieser mobilen Computer leider auch Angriffsmöglichkeiten durch Schadsoftware wie z. B. Viren nach sich zieht. Dadurch könnten Daten verfälscht oder gelöscht werden. Da die Sicherheitsmechanismen eines Betriebssystems meist nicht ausreichen, kann durch den Einsatz einer Personal Firewall, die meist durch den Nutzer selbst installiert, konfiguriert und verwaltet wird, sehr wirksam den Angriffen z. B. aus dem Internet begegnet werden. Die Entwicklung lässt sogar vermuten, dass die Hersteller in naher Zukunft weitere Sicherheitslösungen wie ein VPN oder Virenschutz in die Personal Firewall integrieren.

Auf der Grundlage der beschriebenen Sicherheitsmechanismen können die Risiken für WLANs durch die bekannten Angriffstechniken minimiert werden. Durch ein Sicherheitsmanagement muss die Sicherheit stets überprüft und verbessert werden, um auch auf neue Gefahren reagieren zu können.

4. Aus den Arbeitsgebieten

4.1 Öffentliche Sicherheit

4.1.1 Polizei und Feuerwehr

Abschaffung der Schleierfahndung und andere Anträge

Im Rahmen der parlamentarischen Beratungen über unsere Berichte zu den wenig beeindruckenden Ergebnissen von verdachts- und anlassunabhängigen Kontrollen der Polizei (*„Schleierfahndung“*)[52] im Unterausschuss „Datenschutz und Informationsfreiheit“ des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses hat die Fraktion Bündnis 90/Die Grünen einen Gesetzesantrag mit dem Ziel der Abschaffung der Schleierfahndung eingebracht. Dieser Antrag, ein weiterer Antrag der Fraktion Bündnis 90/Die Grünen mit dem Ziel, die *Rasterfahndung* einzugrenzen, sowie ein Antrag der Fraktion der CDU, den Begriff von „Straftaten von erheblicher Bedeutung“ (§ 17 Abs. 3 ASOG) erneut zu modifizieren, sind in ein Änderungsgesetz zum Allgemeinen Sicherheits- und Ordnungsgesetz (*ASOG*) eingeflossen[53]. Wesentliche Punkte sind

– die Erweiterung der erst 2003 neu gefassten Definition der „Straftaten von erheblicher Bedeutung“ um einige abschließend aufgezählte Delikte (Aufnahme von Straftaten, die keine Verbrechen oder Straftaten nach § 100 a StPO sind, jedoch im Höchstmaß mit einer Freiheitsstrafe von bis zu zehn Jahren bestraft werden bzw. die den Anforderungen entsprechen, die das Bundesverfassungsgericht für besonders schwere Straftaten zugrunde gelegt hat),

– die Befugnis zur Erhebung personenbezogener Daten zur vorbeugenden Bekämpfung – über die Straftaten von erheblicher Bedeutung hinaus – von sonstigen Straftaten, die organisiert, insbesondere banden-, gewerbs- oder serienmäßig begangen werden und mit einer Höchststrafe von mehr als drei Jahren bedroht sind,

– die Abschaffung der Schleierfahndung, nachdem auch der Polizeipräsident in Berlin eingeräumt hat, dass die Vorschrift schon aufgrund ihrer Tatbestandsvoraussetzungen und ihres Maßnahmenkataloges kaum effiziente Handlungsmöglichkeiten schafft,

– die Befugnis zur Inaugenscheinnahme mitgeführter Sachen an Kontrollstellen und

– die Eingrenzung der Rasterfahndung, wobei die Voraussetzungen unter gleichzeitigem Wegfall der Klarstellung, dass Berufs- und Amtsge-

[52] JB 2000, 4.1.2; JB 2001, 4.1.2

[53] GVBl. 2004, S. 174

heimnisse unberührt bleiben, präzisiert werden. Die besondere Form des Datenabgleiches muss auch bei „Gefahr im Verzug“ vom Richter angeordnet werden. Dem Antrag sind die Errichtungsanordnung, das Datensicherheitskonzept, die Risiko-Analyse und die Beschreibung der technisch-organisatorischen Maßnahmen beizulegen. Die Polizei hat uns künftig fortlaufend über die Maßnahmen zu unterrichten.

Weitere Anträge hatten keinen Erfolg:

Die Schaffung der Kennzeichnungspflicht für Polizeibeamte wurde zurückgestellt. Hier sollen ein Modellversuch des Polizeipräsidenten in Berlin und der Bericht dazu abgewartet werden.

Die CDU-Anträge, die DNA-Profile den Fingerabdrücken gleichzustellen, wurden unter Hinweis auf den Verhältnismäßigkeitsgrundsatz ebenso abgelehnt wie der Antrag, die Möglichkeiten der Videoüberwachung auszuweiten. Dabei wurde eingeräumt, dass die Videoüberwachung zwar das subjektive Sicherheitsgefühl erhöht, bei einem Überfall aber selbst keine Hilfe gewährleisten könne wie ein Polizist. Wenn flächendeckende Videoüberwachung wirkungsvoll wäre, dürfte es in London keine Kriminalität mehr geben …

DNA-Analyse

Im Jahresbericht 2002[54] hatten wir über die erste *DNA-Reihenuntersuchung* in Berlin berichtet. Nach den Beratungen im Unterausschuss „Datenschutz und Informationsfreiheit“ hat das Abgeordnetenhaus von Berlin am 13. Mai 2004 den Senat aufgefordert, dafür zu sorgen, dass der Polizeipräsident die Verfahrensweise bei der Durchführung von DNA-Reihenuntersuchungen innerhalb des ersten Halbjahres 2004 durch eine Geschäftsanweisung regelt, die die von uns entwickelten Kriterien berücksichtigt.

Im Juni wurde ein erster Entwurf für eine Geschäftsanweisung vorgelegt. Danach soll zwischen Probeentnahmen – auf freiwilliger Basis – und der Untersuchung bzw. Analyse selbst – nach richterlicher Anordnung – differenziert werden. Der Grund dafür wird allerdings nicht hinreichend deutlich. Zwar könnte die Polizei die Proben auf diese Weise auch ohne richterliche Anordnung mit der ausdrücklichen Einwilligung des Betroffenen erheben, aber das für die Strafverfolgungsbehörden entscheidende Ergebnis kann erst nach richterlicher Anordnung der Untersuchung erzielt werden. Es muss in jedem Fall eine richterliche Anordnung beantragt werden. Wir haben deshalb empfohlen, die richterliche Anordnung bereits *vor* der Probeentnahme einzuholen.

[54] vgl. 3.3

Retrograde Erfassung für die DNA-Analyse-Datei

Das Bundeszentralregister (BZR) wurde nach der Novellierung des DNA-Identitätsfeststellungsgesetzes (DNA-IFG) im Jahr 1999 ermächtigt, im Zeitraum vom 2. Juni 1999 bis zum 30. Juni 2001 den Staatsanwaltschaften zu 41 Katalogstraftaten (Anlage zu § 2 c DNA-IFG) die Daten der für eine DNA-Analyse in Betracht kommenden Verurteilten zu übermitteln. Diese Daten dienten ausschließlich dem Aufbau der *DNA-Analyse-Datei* beim Bundeskriminalamt. Am 23. März 2001 wurde dem Landeskriminalamt Berlin eine Datenbank, bestehend aus 62.032 Datensätzen, aus dem Bestand des BZR einschließlich Erziehungsregister zur Verfügung gestellt. Die Datenbank enthält alle mit Berliner Aktenzeichen verurteilten Straftäter, die für eine retrograde Erfassung in Betracht kommen. Die Polizei hat der Staatsanwaltschaft bei dem Landgericht Berlin die Personendatensätze mit aktueller Meldeanschrift, zugrunde liegender Verurteilung und aktuellen kriminalpolizeilichen Erkenntnissen zur Überprüfung vorzulegen, ob ein richterlicher Beschluss zur Vornahme einer DNA-Analyse herbeigeführt werden soll.

Wozu dies führen konnte, zeigt folgender Fall:

Eine Jugendliche wurde 1993 wegen räuberischer Erpressung in Tateinheit mit Körperverletzung nach dem Jugendgerichtsgesetz (JGG) richterlich ermahnt. Obwohl die Daten der Jugendlichen im „Informationssystem Verbrechensbekämpfung“ (ISVB) der Berliner Polizei längst gelöscht, die dazugehörigen Unterlagen vernichtet und auch zum Zeitpunkt der Überprüfung die Daten im BZR getilgt waren, wurde die Staatsanwaltschaft bei dem Landgericht Berlin formularmäßig um Prüfung gebeten, ob die Betroffene für eine retrograde Erfassung in Betracht kommt.

Da die Polizei nicht berechtigt ist, selbst Abfragen beim BZR zum Aufbau der DNA-Datei zu stellen, konnte sie nicht überprüfen, ob die Daten der Betroffenen im BZR überhaupt noch vorhanden waren. Obwohl in einer vom Generalstaatsanwalt in Absprache mit der Justizverwaltung erstellten Prioritätenliste bei Raub eine Verurteilung zu mindestens drei Jahren Freiheitsstrafe Voraussetzung für die Identitätsfeststellung war, durfte die zuständige Arbeitsgruppe der Polizei danach keine Vorselektion vornehmen und musste die Daten demgemäß an die Staatsanwaltschaft weiterleiten, obwohl nach der Prioritätenliste klar war, dass gar keine Identitätsfeststellung durchzuführen war. Erst im März 2004 wurde die Polizei wegen fehlender Aussicht auf eine gerichtliche Anordnung ermächtigt, in einer Reihe von Fallkonstellationen selbst die Daten auszusondern; hierzu gehören unter anderem Verurteilungen zu Raub oder Erpressung zu weniger als drei Jahren Freiheitsstrafe. Der vorliegende Fall würde also inzwischen von vornherein zu keiner Datenübermittlung an die Staatsanwaltschaft mehr führen.

Die heruntergefallenen DNA-Proben

Einer Reinigungskraft im Landeskriminalamt Berlin waren mehrere für eine DNA-Untersuchung erhobene Speichelproben heruntergefallen. Die Speichelproben müssen zunächst bei Zimmertemperatur ca. 12 Stunden trocknen, da die DNA ansonsten durch Mikroorganismen zerstört würde. Dazu werden die Wattestäbchen mit den Speichelproben locker in Schutzröhrchen gesteckt. Da diese offen herumstanden, wurden die Proben versehentlich heruntergestoßen.

Wegen der möglichen Kontamination und Vermischung der Proben untereinander mussten von den Betroffenen erneut Speichelproben entnommen werden. Der Vorgang wurde zum Anlass genommen, ab sofort Speichelproben außerhalb der Dienstzeiten nur noch in verschlossenen Schränken zu trocknen.

Die Fußball-Weltmeisterschaft 2006 wirft ihre Schatten voraus

Die Organisatoren der Fußball-Weltmeisterschaft 2006 in Deutschland haben zusammen mit der Polizei auch Strategien zu entwickeln, um gewaltbereiten Fans den Zugang zu den Stadien zu verwehren. In die Eintrittskarten sollen RFID-Tags mit personenbezogenen Daten der Käufer integriert werden, damit der rechtmäßige Kartenkäufer das WM-Spiel besuchen kann und der Schwarzhandel wesentlich erschwert wird.

Die FIFA als Veranstalterin der *Fußball-Weltmeisterschaft 2006* hat die Einzelheiten des Eintrittskartenverkaufes noch nicht abschließend festgelegt. Das bei dem Deutschen Fußballbund (DFB) angesiedelte Organisationskomitee arbeitet zurzeit die Vorgaben der FIFA ab. Für den Eintrittskartenverkauf soll jedenfalls auf die bei dem DFB als Dachverband des deutschen Fußballsports geführte Datei der von den Vereinen der 1. und 2. Bundesliga sowie von den Regionalligen ausgesprochenen Stadienverboten zugegriffen werden.

Die Erteilung von Stadienverboten beruht auf dem nationalen Konzept „Sport und Sicherheit“, das auf eine gemeinsame Initiative des Bundesministeriums des Innern, der Innenminister-, Sozialminister- und Jugendministerkonferenz, des Bundesministeriums für Frauen und Jugend, des Deutschen Städtetages, des Deutschen Sportbundes sowie des DFB zurückgeht. Der DFB und die Vereine der Lizenz- und Regionalligen erkennen diese Grundlagen noch einmal durch gesonderte schriftliche Erklärung an. Zusätzlich geben sämtliche Teilnehmer der Lizenz- und Regionalligen die „Erklärung zu den bundesweit wirksamen Stadienverboten“ ab. In ihr ermächtigen die Vereine sich untereinander sowie den DFB noch einmal ausdrücklich zur Erteilung von bundesweit wirksamen Stadienverboten.

Die wesentlichen Voraussetzungen und Verfahrensregelungen bei der Erteilung von Stadienverboten finden sich in den „Richtlinien zur einheitlichen Festsetzung und Verwaltung von Stadienverboten“ (Richtlinien). In diesen Bestimmungen wird als Zweck des Stadienverbotes festgelegt, durch den Ausschluss von Platz- bzw. Hallenanlagen die von den Betroffenen ausgehenden Gefahren künftig zu vermeiden und sie zu friedfertigem Verhalten anzuhalten. Stadienverbote erfolgen auf der Grundlage des Hausrechts. Sie dienen präventiv der Erfüllung der Verkehrssicherungspflicht des Veranstalters und damit der Sicherheit der Veranstaltung und ihrer Besucher. Voraussetzung für ein überörtliches Stadienverbot ist, dass entweder ein Ermittlungs- oder sonstiges Verfahren wegen eines in dem abschließenden Straftatenkatalog der Richtlinien genannten Vergehens eingeleitet worden ist oder dass ein bestimmter Sachverhalt Anlass zu polizeilichen Maßnahmen gegeben hat, die die Annahme rechtfertigen, dass von dem Betroffenen auch künftig Gefahren ausgehen werden. Da es sich bei dem Stadienverbot um eine Präventiv-Maßnahme handelt, gilt auch die Unschuldsvermutung nicht. Entscheidend ist vielmehr die aufgrund eines bestimmten Sachverhaltes festgelegte objektive Möglichkeit einer von dem Betroffenen ausgehenden Gefahr. In den Richtlinien ist auch geregelt, wann ein Stadionverbot endet bzw. vorzeitig aufgehoben oder in seiner Dauer reduziert werden kann.

In der Praxis liegen der Erteilung von Stadienverboten entweder eigene Feststellungen der Ordnungskräfte der Vereine oder – und dies ist der Regelfall – Mitteilungen über relevante Sachverhalte durch Polizei zugrunde. Der von der Polizei mitgeteilte Sachverhalt wird dabei von der das Stadionverbot aussprechenden Stelle überprüft. Wird ein Stadionverbot verhängt, erfolgt eine formularmäßige Mitteilung an den Betroffenen und den DFB bzw. die Deutsche Fußball-Liga als verwaltende Zentralstelle. Der Betroffene wird sodann in die Liste „Bundesweite Stadienverbote“ aufgenommen, die wiederum von dem DFB per Post an die Sicherheitsbeauftragten der Vereine, die zuständige Bundesgrenzschutzdirektion und die „Zentrale Informationsstelle Sport-Einsätze“ (ZIS) bei dem Landeskriminalamt Nordrhein-Westfalen versandt wird. Die Deutsche Fußball-Liga stellt diese Liste zur Information der Lizenzvereine in das Extranet der Fußball-Bundesliga ein. Für die entsprechenden Seiten haben ausschließlich die Sicherheitsbeauftragten ein Leserecht.

Nicht mit der Datei der Stadienverbote verwechselt werden darf die Datei der „Gewalttäter Sport“. Diese Datei ist dem nationalen Konzept „Sport und Sicherheit“ zuzuordnen und wird von den Sicherheitsbehörden verwaltet (Verbunddatei bei dem Bundeskriminalamt). Die Vereine und der DFB erhalten keinerlei Daten aus der Datei „Gewalttäter Sport“. Der Polizeipräsident in Berlin hat uns dazu mitgeteilt, dass eine Weitergabe der bei der Polizei gespeicherten Daten über Fußball-Gewalttäter auch nicht beabsichtigt ist.

Offen ist die technische Frage der Eingangskontrolle in den Stadien. Die Zuschauer müssen nach dem internen Pflichtenheft der FIFA mit einer Plas-

tikkarte, auf der ein Chip – voraussichtlich ein RFID-Tag[55], der die gespeicherten personenbezogenen Daten des Zuschauers enthält – aufgebracht ist, an einem Lesegerät vorbeigehen. So wird die Zutrittsberechtigung elektronisch geprüft. Danach treten sie durch ein Drehkreuz, an dem eine Signalanlage vorzusehen ist. Eine weitere Vorgabe der FIFA lautet, dass das System ein Jahr vor der Fußball-Weltmeisterschaft im Spielbetrieb reibungslos funktionieren muss. Die Einzelheiten werden wir in der kommenden Bundesliga-Saison prüfen, sobald die Systeme installiert sind.

Aufzeichnung von Notrufgesprächen in der Leitstelle der Berliner Feuerwehr

Bei jedem eingehenden *Notruf* in der Leitstelle der Berliner *Feuerwehr* wird automatisch die Rufnummer des Anrufers übermittelt und dem Bearbeiter auf dem Bildschirm angezeigt. Gleichzeitig wird im Hintergrund auf eine bei der Berliner Feuerwehr geführte Namens- und Adressdatenbank zugegriffen, um über eine Inverssuche den Inhaber des Anschlusses zu ermitteln, von dem aus der Notruf erfolgt. Findet sich ein Datenbankeintrag zur Rufnummer, werden Name und Anschrift dem Bearbeiter ebenfalls auf dem Bildschirm angezeigt und er kann diese übernehmen. Werden keine Namens- und Adressinformationen gefunden, werden die Daten im Gespräch ermittelt.

Die verwendete Namens- und Adressdatenbank stammt aus dem Datenbestand der Deutschen Telekom. Rufnummer, Name und Anschrift des Anschlussinhabers, Zeit und Dauer des Notrufgespräches, die Lagebeschreibung und weitere Informationen zum Ablauf des Einsatzes werden in einer Einsatz-Datei gespeichert. Nach Abwicklung des Einsatzes wird diese Datei in eine Langzeitdokumentation überführt. An mehreren Stellen kann auf die Langzeitdokumentation zugegriffen werden. Die entsprechende Datenbank ist zwar passwortgeschützt; es gibt allerdings nur ein allgemeingültiges Passwort, das bisher noch nicht geändert worden ist. Damit hat jeder Mitarbeiter die Möglichkeit zum Zugriff auf den Datenbestand. Eine Protokollierung der Zugriffe erfolgt nicht. Ebenso wenig besteht ein Löschungskonzept für die Einsatz-Dateien. Die Daten werden mindestens zehn Jahre aufbewahrt. Eine Sperrung der Daten nach Abwicklung des Einsatzes wird nicht vorgenommen.

Neben den eigentlichen Notrufgesprächen wird auch die gesamte Kommunikation zwischen der Einsatzleitzentrale und den anderen Feuerwachen oder den Einsatzfahrzeugen sowie die zwischen den Einsatzfahrzeugen untereinander aufgezeichnet und für drei Monate gespeichert. Die Gespräche sind ohne großen Aufwand abhörbar.

[55] vgl. 3.4

Schließlich wird für jeden Notruf eine Datei angelegt, in der nur die Rufnummer, von der der Notruf ausging, sowie Anfang und Ende des Gespräches gespeichert werden. Diese Datensätze werden ebenfalls für drei Monate aufbewahrt. Die gespeicherten Daten über die Notrufe werden in erster Linie benötigt, um Anfragen der Polizei zu bedienen, die bei Ermittlungen auf die Informationen zurückgreifen will. Ferner dienen die Aufzeichnungen der Gesprächsinhalte der Bearbeitung von Beschwerden. Schließlich werden sie auch zu Aus- und Fortbildung und zu arbeits- und disziplinarrechtlichen Maßnahmen verwendet.

Die Übermittlung der Rufnummern der Anrufer durch die jeweiligen Telekommunikationsnetzbetreiber an die Leitstelle der Feuerwehr beruht auf einer gesetzlichen Verpflichtung (§ 108 Abs. 1 Satz 2 Nr. 1 Telekommunikationsgesetz – TKG) und ist damit zulässig.

Datenschutzrechtlich von Bedeutung ist die Zulässigkeit der Aufzeichnung der eingehenden Notrufgespräche und deren nachfolgende Verwendung. Das Telekommunikationsgesetz trifft hierzu keine Regelungen. Die Leitstelle der Feuerwehr kann nur auf der Basis einer landesrechtlichen Befugnisnorm die eingehenden Daten in zulässiger Weise erheben und verarbeiten. An einem solchen gesetzlichen Erlaubnistatbestand fehlt es allerdings. Einschlägige spezialgesetzliche Regelungen sind nicht ersichtlich. So erlaubt zwar § 4 Abs. 1 Satz 1 Nr. 1 Gesetz über den Rettungsdienst für das Land Berlin die Datenverarbeitung bei der Notfallrettung, soweit dies für die Durchführung und zum Nachweis der ordnungsgemäßen Abwicklung des Einsatzes erforderlich ist. Damit sind aber gerade die von der Feuerwehr vorgebrachten Zwecke nicht gedeckt. Zudem betreffen die bei der Feuerwehrleitstelle eingehenden Notrufe keineswegs nur die Notfallrettung. Ein Rückgriff auf die allgemeinen Erhebungsbefugnisse zur Gefahrenabwehr in den §§ 18, 19 ASOG kommt ebenfalls nicht in Betracht.

Im Übrigen kann die bestehende Dienstvereinbarung über den Einsatz und den Betrieb der Sprachdokumentationsanlage bei der Feuerwehrleitstelle aus dem Jahr 2002 keine ausreichende Rechtsgrundlage für die Gesprächsaufzeichnung bilden. Sie erfüllt weder die Anforderungen des § 6 Abs. 1 Satz 1 Nr. 1 oder 2 BlnDSG noch kann sie die Rechte außen stehender Personen, hier also die der betroffenen Anrufer, wirksam einschränken.

Eine Einwilligungslösung wird derzeit nicht praktiziert und wird auch künftig keine praktikable Option darstellen. Zum einen findet schon beim Zustandekommen der Verbindung eine Aufzeichnung statt. Zum anderen kann angesichts der Stresssituation, in der sich der Anrufer befindet, nicht von der Freiwilligkeit der Einwilligung (§ 6 Abs. 5 BlnDSG) ausgegangen werden.

Neben der fehlenden Rechtsgrundlage für die Aufzeichnung und Verwendung der Notrufgespräche haben wir folgende Mängel festgestellt:

– Es fehlt an einer ordnungsgemäßen Passwortvergabe für die Zugriffe auf die Langzeitdokumentation.

– Die Zugriffe auf die Langzeitdokumentation werden nicht protokolliert. Damit ist eine Revisionsfähigkeit nicht gewährleistet.

– Es fehlt an einem notwendigen Löschungskonzept für die in der Langzeitdokumentation enthaltenen Daten. Darin müssten präzise Höchstspeicherfristen festgelegt werden, die sich streng an der Erforderlichkeit der Daten für die Aufgabenerfüllung orientieren.

4.1.2 Verfassungsschutz

Die Anti-Terror-Datei

Auch das Jahr 2004 stand unter dem Zeichen der Diskussion um die innere Sicherheit des Landes. Ein Terroranschlag in Spanien verstärkte die Bestrebungen, die Verfassungsschutzbehörden und die Polizeibehörden des Bundes und der Länder stärker zusammenarbeiten zu lassen, als dies nach den derzeitigen Regelungen des Grundgesetzes und den Bundes- und Landesgesetzen möglich ist.

Einen ersten Gesetzentwurf zur Führung einer *Anti-Terror-Datei* legte im August das Land Niedersachsen in Form einer Bundesratsinitiative vor[56].

Der Gesetzentwurf will die rechtlichen Grundlagen für die gemeinsame Bekämpfung des islamistischen Extremismus und Terrorismus durch die Verfassungsschutzbehörden und die Polizeibehörden des Bundes und der Länder sowie die Zollbehörden schaffen. Zu diesem Zweck soll eine gemeinsame Datei beim Bundesamt für Verfassungsschutz eingerichtet werden, die alle Daten über Personen und Vorgänge, die im Zusammenhang mit dem islamistischen Extremismus oder Terrorismus stehen, enthalten soll. Die Datei soll der gegenseitigen Information vom Bundesamt für Verfassungsschutz, der Landesverfassungsschutzbehörden, des Bundeskriminalamtes, der Landeskriminalämter, des Bundesgrenzschutzes, des Militärischen Abschirmdienstes, der Zollkriminalämter und des Bundesnachrichtendienstes dienen. Gespeichert werden sollen in der Datei nur Namen, Objekte, Kommunikationsmittel und Aktenfundstellen.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich auf ihrer Konferenz am 28./29. Oktober 2004 in Saarbrücken entschieden dagegen ausgesprochen, dass in der geplanten Datei auch Daten zum islamistischen Extremismus gespeichert werden sollen. Die Polizeibehörden haben für die Beobachtung des islamistischen Extremismus keine gesetzliche Befugnis und damit auch keine Berechtigung, auf diese Daten zuzugreifen. Eine Zugriffsbefugnis von Polizei- und auch Zollbehörden bedeutet eine Infragestellung des Trennungsgebotes von Polizei und Verfassungsschutz.

[56] BR-Drs. 657/04

Weitergehende Überlegungen wurden von den Innenministern des Bundes und der Länder heftig diskutiert. Der Bundesinnenminister will dem Bundeskriminalamt wesentlich mehr Befugnisse gesetzlich einräumen und in diesem Zusammenhang auch ein Weisungsrecht des Bundeskriminalamtes gegenüber den Landeskriminalämtern gesetzlich regeln. Die Mehrzahl der Bundesländer hat sich jedoch gegen eine solche Zentralisierung der Aufgaben der Terrorismusbekämpfung gewandt.

4.2 Ordnungsverwaltung

4.2.1 Melde-, Personenstands- und Ausländerwesen

Ende einer unendlichen Geschichte in Sicht?

> *Alljährlich haben wir seit der ersten Änderung des Melderechtsrahmengesetzes (MRRG) im Jahr 1994 ohne Ergebnis eine Novellierung des Landesmeldegesetzes (MeldeG) angemahnt. Anfang des Jahres wurde ein Entwurf eines neuen MeldeG vorgelegt. Damit sollen nunmehr drei Melderechtsrahmenänderungsgesetze und mehrere Artikelgesetze in Landesrecht umgesetzt werden.*

Ein wesentliches Element des Entwurfes ist die Schaffung der rechtlichen Voraussetzung zum Einsatz elektronischer Dienste unter Anwendung der Vorschriften des Signaturgesetzes und insbesondere ein elektronischer Zugang für den Betroffenen zu seinen über ihn im Melderegister gespeicherten Daten. Die beabsichtigten Regelungen hinsichtlich der Öffnung des Internets sind vertretbar, aber sehr allgemein gehalten. Die Details werden erst bei der technischen Umsetzung eine Rolle spielen (Sicherheitskonzept für die Internet-Zugänge und -Portale). Ansonsten lehnt sich der Entwurf sehr eng an das Rahmenrecht an.

So soll eine bereits bei der Änderung des Rahmenrechts umstrittene Regelung zur Datenübermittlung *an* die *Meldebehörden* geschaffen werden. Dabei werden die gesetzlichen Geheimhaltungsvorschriften sowie besondere Berufs- und Amtsgeheimnisse durchbrochen. Die Daten der Sozialleistungsträger unterliegen dem Sozialgeheimnis nach § 35 des I. Buches Sozialgesetzbuch (SGB I). Sofern ein Sozialleistungsträger Daten übermittelt, die nach dem *Meldegesetz* gespeichert werden dürfen, handelt es sich um eine Offenbarung von Sozial-, nicht jedoch schon um Meldedaten mit der Folge, dass eine korrespondierende Befugnis nach den §§ 67 ff. SGB X erforderlich wäre.

Auch rechtssystematisch ist das Meldegesetz für die Durchbrechungen der Geheimhaltungsvorschriften sowie der Berufs- und Amtsgeheimnisse nicht die richtige Stelle. Vielmehr wären in diesem Zuge die bundesrecht-

lichen Regelungen dahingehend zu ändern, dass diesen Stellen eine Befugnis zur Übermittlung eingeräumt wird.

Die Übermittlung melderechtsfremder Daten wie z. B. über Waffenscheine, Wahlberechtigungen oder Steuerdaten einschließlich Religionszugehörigkeit soll unter bestimmten Bedingungen zugelassen werden. Es wird nicht hinreichend deutlich, warum auch anderen als den Behörden, die ausnahmsweise melderechtsfremde Daten im Melderegister speichern können, der Zugang zu den Daten eröffnet werden soll. Damit wird eine Regelung aufgeweicht, die der Senator für Inneres am 16. November 1984 noch wie folgt begründet hat: „Dem Grundsatz der Verhältnismäßigkeit entspricht es, wenn lediglich die sogenannten ‚Zusatzdaten' nach § 2 Abs. 2, nicht aber die sogenannten ‚Grunddaten' nach § 2 Abs. 1 unter das strikte Zweckbindungsgebot fallen. Es ist gerade Ausfluss des multifunktionellen Charakters des Meldewesens, die für eine Vielzahl denkbarer Empfänger gespeicherten Daten nach § 2 Abs. 1 von einem strikten Zweckbindungsgebot auszunehmen."

Nach der derzeitigen Rechtslage werden nur die Datenübermittlungen protokolliert, die über den Umfang einer einfachen Melderegisterauskunft (§ 28 Abs. 1 MeldeG) hinausgehen. Selbst diese eingeschränkte Protokollierung soll durch den Entwurf noch weiter eingeschränkt werden. Die beabsichtigte Regelung ist nicht mit § 5 Abs. 2 Nr. 5 BlnDSG vereinbar. Danach muss festgestellt werden können, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit). Dazu gehören die Aufzeichnungen, an welche Stellen Daten übermittelt worden sind. Zwar sind die Vorschriften in den Datenschutzgesetzen nur Auffangnormen, denen bereichsspezifische Regelungen vorgehen; die Bestimmungen des Berliner Datenschutzgesetzes zur Datensicherheit sind aber als Mindeststandard anzusehen, hinter dem spezielle Regelungen nicht zurückbleiben dürfen (vgl. § 6 Abs. 1 Satz 3 BlnDSG). Die bestehenden Protokollierungspflichten müssen nicht nur bestehen bleiben, vielmehr müssen darüber hinaus mindestens auch die Übermittlungen der Grunddaten an andere öffentliche Stellen protokolliert werden.

Erörterungsbedürftig ist die Verordnungsermächtigung zur Regelung von Online-Abrufen. Sie verlangt bisher allgemein, dass die zum Abruf bereitgehaltenen Daten ihrer Art nach für den Empfänger erforderlich sind und das Bereithalten der Daten zum Abruf durch den Empfänger unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist.

Die Anlage 5 zu § 3 Nr. 2 DVO-Meldegesetz enthielt bislang diejenigen Stellen, deren Aufgabenstellung einen Zugriff auf unterschiedlich geschnittene Datenprofile erforderlich macht. Die Erörterungen zur 2. Verordnung zur Änderung der Verordnung zur Durchführung des Meldegesetzes im Jahr 2003[57] haben gezeigt, dass mehr und mehr Stellen den Zugang begehren, für

[57] JB 2003, 4.2.1

die lediglich der Zugriff auf den in § 28 Abs. 1 enthaltenen Grunddatenbestand erforderlich ist. Da der Zugriff auf darüber hinausgehende Daten nur durch den Gesetzgeber selbst gestattet werden sollte, muss die Verordnungsermächtigung entsprechend begrenzt werden. Realisiert werden könnte dies durch eine Aufzählung der in der Anlage 5 zu § 3 Nr. 2 DVO-MeldeG alter Fassung genannten Stellen (Bezirksämter, Feuerwehr, Polizeipräsident, Personalausweis- und Passbehörde, Kfz-Zulassungsstelle und Verkehrsordnungswidrigkeitenstelle). Für alle anderen Stellen sollte die Verordnungsermächtigung nur den Abruf der Daten nach § 28 Abs. 1 ermöglichen. Insbesondere darf die Verordnungsermächtigung nicht den Zugriff auf melderechtsfremde Daten (§ 2 Abs. 2) durch dritte Stellen umfassen.

Zu begrüßen ist, dass die Meldebehörden gesetzlich verpflichtet werden, künftig in Fällen einer Auskunftssperre die für weitere Wohnungen des Einwohners zuständigen Meldebehörden von dieser Tatsache zu unterrichten.

Die *Auskunftssperre* soll den Betroffenen vor Nachteilen schützen, die ihm aus der Offenbarung seiner Daten gegenüber privaten Dritten entstehen können. Um die allgemeine Auskunftssperre zu erhalten, muss der Betroffene Tatsachen glaubhaft machen, die die Annahme rechtfertigen, dass durch die Melderegisterauskunft ihm oder einer anderen Person eine Gefahr für Leben, Gesundheit, Freiheit oder ähnliche schutzwürdige Belange erwachsen kann. Die Betroffenen, die ihrerseits gegenüber der Meldebehörde sensible Einzeldaten zur Gefährdungssituation offenbaren müssen, müssen sich darauf verlassen können, dass denjenigen, von denen die Bedrohung ausgeht, nicht nur der direkte Zugriff auf die Daten, die im Rahmen der einfachen Melderegisterauskunft mitgeteilt werden dürften, verwehrt wird, sondern darüber hinaus jeder Anreiz für gezielte Umgehungsstrategien, beispielsweise durch die Einschaltung Dritter, genommen wird. Die Risiken können auch bei der Weitergabe an öffentliche Stellen bestehen. Deshalb sollte die anstehende Novellierung zum Anlass genommen werden, die Schutzwirkung der melderechtlichen Auskunftssperre auch – wie beispielsweise in Schleswig-Holstein – gegenüber den öffentlichen Stellen zu erweitern.

Unabhängig davon haben wir teilweise mehr als 15 Jahre alte Forderungen wiederholt. So sollte jedem Meldepflichtigen die Möglichkeit eingeräumt werden, auf freiwilliger Basis zusätzliche Angaben darüber speichern zu lassen, welche Person in einem Unglücksfall benachrichtigt werden soll. Damit würde die oft beklagte Folge des bestehenden Melderechts entfallen, dass wegen der fehlenden Verknüpfung zwischen Volljährigen und dem bisherigen gesetzlichen Vertreter die Benachrichtigung bei Unglücksfällen von nahestehenden Personen erschwert bis unmöglich gemacht wird. Das Problem wurde in der Vergangenheit oft als Beispiel für überzogene Regelungen des Datenschutzrechts genannt.

Bis zum Jahresende hat sich der Senat nicht mit dem Entwurf befasst. Es bleibt also abzuwarten, ob das Jahr tatsächlich das Ende der unendlichen Geschichte bringen wird.

Automatisierte Abrufverfahren im Bezirksamt

Seitdem das Landeseinwohneramt ein elektronisches *Portal für Behördenauskünfte* entwickelt hat, sind auch entgegen den nach der DVO zulässigen Abrufmöglichkeiten in den Bezirken verschiedene Stellen mit Terminals ausgestattet worden. Bei einer Prüfung haben wir festgestellt, dass – ohne Kenntnis des Landeseinwohneramtes als die das Melderegister führende Stelle – in Standes-, Sozial-, Jugend- und Wohnungsämtern sowie in einer Bezirkskasse Terminals aufgestellt wurden. In anderen Fällen war als Standort lediglich „Rathaus“ vermerkt, was im Hinblick auf den funktionalen Behördenbegriff viel zu unbestimmt ist. Zwar lässt die bestehende Rechtsverordnung bereits jetzt den Abruf abschließend festgelegter Daten durch die Bezirksämter – jeweils zuständige Stelle – zu, soweit im Einzelfall die Kenntnis der Daten zur Erfüllung der dem Bezirksamt durch Rechtsvorschrift obliegenden Aufgaben erforderlich ist. Wir haben aber der Senatsverwaltung für Inneres wiederholt mitgeteilt, dass diese Regelung zu unbestimmt ist. Vielmehr hat der Verordnungsgeber explizit zu definieren, welche Stelle der Bezirksämter vor dem Hintergrund des funktionalen Behördenbegriffs (§ 4 Abs. 3 Nr. 1 BlnDSG) gemeint ist. Mit der Senatsverwaltung für Inneres besteht Einvernehmen darüber, dass das Problem in einer „zweiten Welle“ der Anpassung der DVO angegangen wird. Darüber hinaus bestand Einvernehmen darüber, dass wir *vor* der Einrichtung eines neuen Abrufverfahrens die Gelegenheit der Stellungnahme erhalten. Daran hat man sich allerdings nicht gehalten.

Grundsätzlich haben wir keine Einwände, wenn eine Abrufmöglichkeit für die Grunddaten (Name, Vorname, gegenwärtige Anschriften, akademische Grade und ggf. die Tatsache, dass der Einwohner verstorben ist) für alle Stellen des Bezirksamtes geschaffen wird.

Ein Abruf der über die Grunddaten hinausgehenden Daten der Nr. 2 der Anlage 5 zu § 3 Nr. 2 DVO-MeldeG kann nur dann zulässig sein, wenn die Erforderlichkeit im Einzelfall deutlich gemacht wird. Dabei sind hohe Anforderungen an die Begründung zu stellen, der insbesondere zu entnehmen sein muss, warum die Erhebung dieser Daten beim Betroffenen nicht sachgerecht ist und wie sich die Abrufmöglichkeit mit dem Grundsatz der Datensparsamkeit verträgt.

Die Schaffung einer Abrufmöglichkeit von auch darüber hinausgehenden Daten kann nicht auf die bestehende Regelung gestützt werden. Das wäre nach derzeitiger Rechtslage unzulässig. Dafür ist die Schaffung einer völlig neuen Befugnis in der DVO-MeldeG erforderlich, wobei wir sehr hohe Anforderungen an die Begründung stellen.

Reform des Personenstandsrechts

Die Bund-Länder-Arbeitsgruppe „Reform des *Personenstandsrechts*“ hat einen Vorentwurf eines Gesetzes vorgelegt, der die Ablösung des geltenden Personenstandsgesetzes vorsieht. Schwerpunkte der Reform sind die

- Einführung elektronischer Personenstandsregister anstelle der bisherigen Personenstandsbücher,
- Ersetzung des Familienbuches durch Beurkundung in den Personenstandsregistern,
- Reduzierung der Beurkundungsdaten auf das für die Dokumentation des Personenstandes erforderliche Maß und
- Neuordnung der Nutzung der Personenstandsbücher.

Die beabsichtigte Neuregelung zum Zugang zu den im Register gespeicherten Daten ist zu begrüßen. Das gilt insbesondere für die von Genealogen immer wieder mit Unverständnis begegnete Anknüpfung an das rechtliche Interesse auch bei den Daten Verstorbener. Mit der Neufassung, dass ein berechtigtes Interesse nach Ablauf von 30 Jahren nach dem Tod oder, falls der Todestag nicht bekannt ist, 110 Jahren nach der Geburt ausreicht, wird diesem Interesse Rechnung getragen, ohne dass die schutzwürdigen Belange der Betroffenen unverhältnismäßig zurückstehen müssten. Damit wird eine langjährige Forderung der Datenschutzbeauftragten des Bundes und der Länder berücksichtigt.

Die Register sollen künftig elektronisch geführt werden. Den geforderten Einsatz der elektronischen Signatur bei der Beurkundung begrüßen wir. Es sind allerdings noch einige Ergänzungen erforderlich. Bisher sind keine Regelungen für die Übermittlung bzw. Auskunft über das Internet enthalten. Daraus schließen wir, dass dies nicht ermöglicht werden soll. Anderenfalls wären hier noch entsprechende Befugnisse zu schaffen.

Künftig soll in den Personenstandsregistern auf die Speicherung des Berufes, des Wohnsitzes sowie der Religionszugehörigkeit verzichtet werden (§§ 14, 16, 20, 31 PStG-E). Diese Regelungen begrüßen wir ebenfalls, weil sie dem Grundsatz der Erforderlichkeit und der Datensparsamkeit Rechnung tragen.

Die Erforderlichkeit für die Einrichtung eines zentralen landesweiten Personenstandsregisters ist nicht erkennbar. Die Gesetzesbegründung führt dazu aus, dass mit der Einrichtung eines zentralen landesweiten Personenstandsregisters allen Standesämtern unbeschränkter Lesezugriff ermöglicht werden soll. Damit könne jeder Nutzungsberechtigte bei jedem Standesamt innerhalb des Bundeslandes Auskunft erhalten. Dieses Verfahren diene der Verwaltungsvereinfachung. Dass ein öffentliches Interesse die schutzwürdigen Belange der Betroffenen erheblich überwiegt und damit das Verfahren rechtfertigt, ist bislang nicht überzeugend dargelegt. Allein Gründe der Verwaltungsvereinfachung vermögen die Einrichtung eines zentralen landesweiten Personenstandsregisters nicht zu rechtfertigen.

Auch fehlen für die vorgesehene Erteilung elektronischer Auskünfte und Einsichten die Vorgaben für die Datensicherheit (beispielsweise Verschlüsselung auf den Leitungen). Sofern die Absicht besteht, auch die Antragstellung

auf elektronischem Weg zuzulassen, wird nicht hinreichend deutlich, wie das rechtliche Interesse dargelegt bzw. übermittelt werden kann. Regelungen zu Protokollierungen, die erforderlich sind, um den Betroffenen die Auskunft erteilen zu können, an wen wann welche Daten übermittelt bzw. zur Verfügung gestellt wurden, fehlen völlig.

Automation im Einbürgerungsverfahren

Über die Einführung neuer Automationsvorhaben und wesentliche Änderungen automatisierter Verfahren sind wir von den Behörden und sonstigen öffentlichen Stellen zu informieren (§ 24 Abs. 3 Satz 3 BlnDSG). Von der beabsichtigten Einführung des bundesweiten Standardproduktes „Einbürgerungen von Ausländern" (EvAStA) haben wir durch den Anruf des behördlichen Datenschutzbeauftragten eines Bezirksamtes erfahren, dem die Unterlagen zur Prüfung vorgelegt wurden, ob von ihm eine Vorabkontrolle (§ 5 Abs. 3 Satz 2 BlnDSG) durchgeführt werden oder er uns einschalten muss (§ 24 Abs. 1 Satz 3 BlnDSG), weil das Verfahren verwaltungsübergreifend eingesetzt werden soll, oder ob er uns dazu zur fachlichen Unterstützung konsultieren möchte.

Die Informationspflicht uns gegenüber wurde nicht beachtet. Zwar macht das Gesetz keine näheren Angaben zum Zeitpunkt der Unterrichtung; sie macht jedoch nur Sinn, wenn sie so rechtzeitig erfolgt, dass uns Gelegenheit zur Stellungnahme gegeben wird und unsere Hinweise noch in die Gestaltung des Verfahrens einfließen können. Erfolgt die Unterrichtung so spät, dass unter Berücksichtigung einer angemessenen Bearbeitungszeit eine Stellungnahme keinen Sinn mehr macht – weil beispielsweise der Termin der Inbetriebnahme kurz bevorsteht –, sehen wir grundsätzlich von einer Stellungnahme ab und kontrollieren das Verfahren im Echt-Betrieb und beanstanden möglicherweise bestehende Verstöße gegen Datenschutzbestimmungen.

Der behördliche Datenschutzbeauftragte hat inzwischen eine Vorabkontrolle durchgeführt und im Wesentlichen mit den Verfahrensverantwortlichen Einigung erzielt. Offen blieb die Frage, ob die Daten nach Abschluss des Verfahrens vollständig gelöscht oder zum Teil weiter vorrätig gehalten werden, um später einer bestehenden Beweisnot des Betroffenen abhelfen zu können (beispielsweise Ausstellung einer beglaubigten Kopie einer verloren gegangenen Einbürgerungsurkunde).

Das Staatsangehörigkeitsgesetz und dessen Nebenbestimmungen enthalten keine Datenverarbeitungsbefugnisse. Die Absicht, diese zu schaffen, ist immer wieder erklärt worden. Solange ist auf die allgemeinen Regelungen des BlnDSG zurückzugreifen. Diese unterscheiden nicht zwischen manueller und automatisierter Datenverarbeitung, sondern umfassen alle Datenverarbeitungen ungeachtet des jeweiligen Verfahrens. Danach sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die Daten verarbeitenden Stellen zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden (§ 17 Abs. 3 BlnDSG). Sofern Grund zu der Annahme der Beeinträchtigung schutzwürdiger Belange des Betroffenen besteht – wie beispielsweise bei dem Zweck, dem Betroffenen bei einer bestehenden Beweisnot helfen zu können –, sind die für die eigentliche ordnungsgemäße Aufgabenerfüllung nicht mehr erforderlichen Daten zu sperren (§ 17 Abs. 2 Satz 2 BlnDSG). Die gesperrten Daten dürfen dann nur noch mit ausdrücklicher Einwilligung des Betroffenen zu wissenschaftlichen Zwecken oder zur Behebung dieser Beweisnot genutzt werden.

Die Verwaltung wollte die Daten aber nicht nur für diese Zwecke nutzen, sondern auch beispielsweise um bei einem neuen Antrag nach Ablehnung auf die Altakten ebenso zurückgreifen zu können wie zum Zwecke der Rücknahme von *Einbürgerungen*. Das wäre unzulässig.

4.2.2 Straßen- und Verkehrsverwaltung

Aus dem Tollhaus – die Einführung der Lkw-Maut auf Autobahnen

Die technischen, politischen und wirtschaftlichen Probleme bei der Entwicklung und (termingerechten) Einführung der automatisierten Erfassung und Erhebung einer streckenbezogenen Autobahnbenutzungsgebühr für Lastkraftwagen (Lkw-Maut) sind durch die umfassende Berichterstattung in den Medien hinlänglich bekannt. Weitestgehend unbemerkt von der breiten Öffentlichkeit bestehen jedoch auch gravierende datenschutzrechtliche Aspekte, die mit der Einführung des elektronischen Mautsystems verbunden sind.

Das von einem Betreiberkonsortium entwickelte elektronische Lkw-Mauterfassungs- und Abrechnungssystem umfasst unter anderem Technologien aus den Bereichen der Satellitennavigation, der Mobilfunkkontrolle und der Videoüberwachung.

Die Mautabrechnung erfolgt (vorrangig) mit Hilfe von so genannten *OnBoardUnits* (OBUs), die von den Kfz-Haltern – zumeist Speditionen – in den Lastkraftwagen zu installieren sind. Die OBUs sind mit einem Mobiltelefon ausgestattet. Sie vergleichen ständig die aktuellen GPS-Koordinaten mit einer im Gerät gespeicherten Straßenkarte. Wird durch den Datenabgleich festgestellt, dass sich das Fahrzeug auf einer mautpflichtigen Strecke befindet, beginnt die Gebührenerfassung. Nach dem Verlassen der mautpflichtigen Strecke werden die Fahrdaten, die per GPS ermittelten Positionen des Fahrzeugs und die errechnete Mautgebühr durch das installierte Mobilfunkgerät automatisch an die Zentrale des Betreibers weitergegeben.

Um zu überprüfen, ob alle mautpflichtigen Fahrzeuge ihre Fahrten auch tatsächlich abrechnen, wurden über den Autobahnen Kontrollbrücken mit Videoüberwachungsgeräten und Infrarotsensoren errichtet. Diese Geräte erfassen die Frontbilder von sämtlichen Fahrzeugen – also auch der Pkws –, die die Kontrollstelle passieren, per Video. Die Kfz-Kennzeichen werden über ein automatisches Mustererkennungsverfahren eingelesen und die Fahrzeuge automatisch vermessen. Ergibt sich dabei, dass keine Mautpflicht besteht (z. B. weil es sich um einen Pkw handelt), werden die zu dem Fahrzeug gehörenden Videodaten gelöscht. Eine Datenlöschung erfolgt ebenfalls, wenn vom OBU per Infrarotsignal mitgeteilt wird, dass der Mautpflicht entsprochen wird. Die Halter von LKWs ohne installierte OBU haben die Möglichkeit, Strecken unter Angabe des Kfz-Kennzeichens über Internet oder an Bezahlterminals der Betreiber vorzubuchen. Stimmt das eingelesene Kennzeichen mit dem der Vorbuchung überein, so werden auch diese Bilder automatisch gelöscht. Ergibt der Datenabgleich an den Kontrollstellen, dass der Mautpflicht nicht nachgekommen wurde, wird das aufgenommene Foto als Beweismittel gespeichert und dem Kfz-Halter ein Bußgeldbescheid zugestellt. Kurz vor Inbetriebnahme des Systems, am 20. Dezember 2004, hat das Bundesamt für Sicherheit in der Informationstechnik dem Betreiber das IT-Grundschutzzertifikat verliehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits im Jahr 2001 in einer gemeinsamen Entschließung[58] auf die datenschutzrechtlichen Probleme, die mit der Einführung eines derartigen Mautsystems verbunden sind, hingewiesen und bei der Einführung einer Mauterfassung eine datensparsame Technik gefordert.

Das vom Betreiberkonsortium entwickelte und am 1. Januar 2005 in Betrieb gegangene Verfahren der Lkw-Mauterhebung entspricht dieser Empfehlung nicht.

Da an den Kontrollstellen nicht nur die mautpflichtigen Lkws, sondern alle Fahrzeuge (auch Pkws) durch die Videoanlagen erfasst werden, wurde eine technische Infrastruktur geschaffen, die es ermöglicht – auch wenn entsprechende Absichten (noch) vehement abgestritten werden –, umfassende Streckenprofile von einer Vielzahl von unbeteiligten (auch privaten) Kraftfahrern zu erstellen. Durch den Einsatz eines Mobiltelefons im OBU können die Mobilfunkverbindungsdaten zur Lokalisierung und somit Aufenthaltsbestimmung des Lkw (und seines Fahrers) auf wenige hundert Meter genutzt werden. Eine Manipulation der bzw. ein Angriff (z. B. durch Viren) auf die Abrechnungsdaten oder das GPS-Signal ist nicht auszuschließen.

Dass insbesondere die Befürchtungen einer zweckfremden Nutzung der Mautdaten nicht realitätsfremd sind, wird durch die anhaltende Diskussion über die Auslegung der datenschutzrechtlichen Regelungen im Autobahnmautgesetz deutlich. Das *Autobahnmautgesetz* (ABMG) bestimmt ausdrücklich, dass die Mauterhebungs- und Mautkontrolldaten ausschließlich zum Zwecke des ABMG verarbeitet und genutzt werden dürfen. Trotz des insofern eindeutigen Wortlautes wird (vereinzelt) die Auffassung vertreten, dass die nach dem ABMG erhobenen Daten an Strafverfolgungs- und Ordnungswidrigkeitenbehörden übermittelt werden dürfen.

[58] vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2001“, S. 33

Vor diesem Hintergrund ist zu begrüßen, dass der Gesetzgeber durch Änderung der §§ 4 Abs. 2 Satz 4 und 7 Abs. 2 Satz 3 ABMG klargestellt hat: „Eine Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften ist unzulässig.“

Datenabgleich zwischen Sozialhilfebehörden und Fahrzeugregister

Im Wege des automatisierten Datenabgleichs wird den Sozialhilfebehörden des Landes Berlin vom Landeseinwohneramt mitgeteilt, ob ein Sozialhilfeempfänger Halter eines Kraftfahrzeuges ist. Das Landeseinwohneramt beabsichtigte den Datenabgleich zwischen den Sozialhilfebehörden und dem örtlichen Fahrzeugregister dahingehend zu erweitern, dass zukünftig auch Informationen zum Kennzeichen, Fahrzeughersteller, Datum der Erstzulassung, Datum der Zulassung, Fahrzeugstatus (zugelassen/stillgelegt), Halterstatus (Halter/Erwerber) und Verkaufsdatum (zunächst das Datum des Verkaufs, wenn nicht vorhanden, das Datum des Eingangs des Kaufvertrags bei vollständigen Kaufverträgen) übermittelt werden.

Das Landeseinwohneramt stützt diese Erweiterung des Datenabgleichs auf § 35 Abs. 3 Nr. 1e Straßenverkehrsgesetz (StVG). Diese Norm sei als Rechtsgrundlage für die Datenübermittlung anzusehen. Der Datenumfang werde durch § 35 Abs. 5 StVG bestimmt. Nach dem Wortlaut dieser Vorschrift dürften die nach § 33 Abs. 1 StVG gespeicherten Fahrzeug- und Halterdaten regelmäßig von den Zulassungsbehörden zur Prüfung nach § 117 Abs. 3 Satz 4 f Bundessozialhilfegesetz (BSHG) übermittelt werden.

Die vom Landeseinwohneramt vertretene Rechtsauffassung ist unzutreffend. Die Zulässigkeit des automatisierten Datenabgleichs zwischen den Sozialhilfebehörden und dem örtlichen *Fahrzeugregister* beim Landeseinwohneramt ist abschließend in § 117 Abs. 3 Satz 1 BSHG i.V.m. § 117 Abs. 3 Satz 4 f BSHG geregelt. Danach dürfen die Sozialhilfebehörden zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe (vgl. § 117 Abs. 3 Satz 1 BSHG) im Wege des automatisierten Datenabgleichs ausschließlich die „Eigenschaft als Kraftfahrzeughalter“ überprüfen.

Ergeben sich aus diesem Datenabgleich Verdachtsmomente für einen Sozialhilfemissbrauch, kann dem im Wege der Einzelfallprüfung konkret nachgegangen werden. Für eine solche Einzelfallprüfung wurde vom Bundesgesetzgeber die Vorschrift des § 35 StVG geschaffen, die der gegebenen Interessenlage entspricht. In § 35 Abs. 3 Nr. 1e StVG und § 35 Abs. 5 Nr. 6 StVG wird ausdrücklich auf die Prüfung des Datums „Eigenschaft als

Kraftfahrzeughalter“ nach § 117 Abs. 3 Satz 4 f BSHG Bezug genommen. Es ist nicht davon auszugehen, dass der Bundesgesetzgeber die Regelungen zum automatisierten Datenabgleich im Sozialrecht durch Regelungen im StVG erweitern wollte. Daher ist die Befugnis für die Kraftfahrzeugzulassungsstelle zur regelmäßigen Übermittlung der in § 33 Abs. 1 StVG gespeicherten Fahrzeug- und Halterdaten (vgl. § 35 Abs. 5 StVG) bei Datenübermittlungen an die Träger der Sozialhilfe durch die konkretisierende Regelung des § 35 Abs. 5 Nr. 6 StVG auf die Daten beschränkt, die „für Prüfungen nach § 117 Abs. 3 Satz 4 f Bundessozialhilfegesetz“ erforderlich sind.

Identitätsausweis in Taxen

Mehrere angestellte Taxifahrer haben sich bei uns darüber beschwert, dass die Taxiunternehmen, bei denen sie beschäftigt sind, von ihnen verlangen würden, dass sie im Taxi ein Schild mit ihrem Foto und ihrem Namen gut sichtbar anbringen. Sie äußerten ihre Bedenken hinsichtlich der Identifizierbarkeit ihrer Person und der dadurch gesteigerten Gefahr der Belästigung und Diffamierung durch Fahrgäste.

Es trifft zu, dass Taxifahrer seit dem 1. Dezember 2004 einen derartigen *Identitätsausweis* anzubringen haben. Rechtsgrundlage für diese Maßnahme ist § 6 Abs. 4 *Taxenordnung*[59]. Danach sind Taxifahrer verpflichtet, während des Bereithaltens des Taxis und der Ausführung von Beförderungsaufträgen im Wageninnern an einer für den Fahrgast gut sichtbaren Stelle ein Schild mit ihrem Lichtbild und ihrem Ruf- und Familiennamen anzubringen.

Wir haben vor Erlass der neuen Taxenordnung ausführlich auf die datenschutzrechtlichen Bedenken, die mit der Einführung eines Identitätsausweises in Taxis verbunden sind, hingewiesen[60]. Die Bedenken ergeben sich im Wesentlichen daraus, dass die Verpflichtung der Taxifahrer, während der Berufsausübung ständig einen Ausweis mit Namen und Lichtbild bei sich zu tragen und für Dritte gut sichtbar im Innenraum der Taxis anzubringen, einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht der Taxifahrer darstellt. Die Verordnungsermächtigung des Landesgesetzgebers in § 47 Abs. 3 Satz 3 Nr. 3 PBefG ist keine ausreichende Rechtsgrundlage für derartige Einschränkungen des informationellen Selbstbestimmungsrechts.

Bereits der Wortlaut des § 47 PBefG steht einer derartig weiten Auslegung entgegen. Die Vorschrift ermächtigt den Verordnungsgeber lediglich zur Regelung „der Einzelheiten des Dienstbetriebs“. Dazu zählt nach § 47 Abs. 3 Satz 2 Nr. 3 PBefG insbesondere der „Fahr- und Funkbetrieb“. Zum

[59] eingeführt durch die Erste Verordnung zur Änderung der Taxenordnung vom 31. August 2004; GVBl., S. 369

[60] JB 2000, 4.2.3

Fahrbetrieb zählt aber nicht die Einführung einer Ausweispflicht für den Fahrer. Dies folgt auch aus dem Regelungszweck des § 47 PBefG. Dieser besteht allein in der Organisation des technischen Ablaufes des Taxibetriebes. Unabhängig davon hat der Bundesgesetzgeber bereits detaillierte Regelungen darüber, welche Fahrzeugpapiere bei Taxifahrten mitzuführen und wem sie auszuhändigen sind, geschaffen. In § 27 BOKraft ist geregelt, dass die Ordnungsnummer des Taxis sowie Name und Betriebssitz des Unternehmens gut sichtbar im Taxi anzubringen sind. Nach § 17 Abs. 4 PBefG ist die erforderliche personenbeförderungsrechtliche Genehmigung auf Verlangen den zuständigen Personen zur Kontrolle auszuhändigen. Weitergehende Eingriffe in das Persönlichkeitsrecht der Taxifahrer – z. B. durch die Einführung der Ausweispflicht in § 6 Abs. 4 Taxenordnung – stellen einen Verstoß gegen den Verhältnismäßigkeitsgrundsatz dar.

Die Taxenordnung wurde vom Senat – entgegen den von uns vorgetragenen datenschutzrechtlichen Bedenken – in der genannten Form geändert. Zur Begründung wurde angeführt, dass der Grundrechtseingriff zum Schutz überwiegender Allgemeininteressen erfolge und somit gerechtfertigt sei. Die Maßnahme sei geeignet, durch das dem Fahrgast mit der Aufhebung der Anonymität gegebene Vertrauen, die Sicherheit im Taxiverkehr zu steigern, Taxifahrer von der Begehung von Ordnungswidrigkeiten abzuhalten und insgesamt die Kundenfreundlichkeit zu verbessern. Demgegenüber sei eine unzumutbare Härte für den Taxifahrer durch die Offenbarung seiner Daten nicht ersichtlich. Besondere Gefahren, denen der Taxifahrer durch die Nennung seines Namens ausgesetzt sein könnte, seien nicht erkennbar.

Parkgebühr mittels Handy

Im Rahmen des von der Europäischen Kommission geförderten Projektes TELLUS ist in Berlin ein Feldtest zur Erprobung und Demonstration einer innovativen Telematik-Lösung in der Parkraumbewirtschaftung vorgesehen. Dem Kraftfahrer wird – unabhängig von der bisherigen Bezahlung am Parkscheinautomaten – ermöglicht, die Parkgebühr über sein Mobiltelefon zu entrichten.

Dazu wählt er jeweils zu Beginn und am Ende des Parkens eine kostenfreie Rufnummer an. Die *Parkgebühr* wird minutengenau von seinem „virtuellen Gebührenkonto“ abgezogen. Das persönliche Gebührenkonto kann vom Benutzer mittels Banküberweisung, Einzugsermächtigung oder SMS aufgeladen werden. Eine Abrechnung über die Handy-Rechnung ist in Vorbereitung. Kraftfahrer, die an dem Verfahren teilnehmen wollen, müssen sich zuvor über das Internet, per Fax oder herkömmliche Post beim Projektbetreiber registrieren lassen. Dazu müssen sie Name, Anschrift, Geburtsdatum, E-Mail-Adresse, Mobilfunknummer, Kraftfahrzeugkennzeichen und ihre Bankverbindung angeben. Mit der Teilnahmebestätigung erhält der Benutzer eine Vignette. Diese enthält das Kraftfahrzeugkennzeichen in barcodierter Form und ist gut sichtbar im Fahrzeug (auf der Windschutzscheibe)

anzubringen. Da der Barcode-Sticker nicht als Parkschein gilt, hat der Kraftfahrer, der an dem Verfahren teilnehmen will, unabhängig von der Registrierung beim Projektbetreiber bei der Straßenverkehrsbehörde eine Ausnahmegenehmigung zu beantragen. Bei den Kontrollen im Rahmen der Parkraumbewirtschaftung wird der Barcode von den Kontrolleuren mit einem GPRS-Handy ausgelesen und an die Zentrale übersandt. Diese überprüft, ob das betreffende Fahrzeug eine Parkberechtigung hat oder nicht und sendet ausschließlich diese Information an den Kontrolleur zurück.

Anlässlich der Registrierung beim Projektbetreiber und der Beantragung der Ausnahmegenehmigung bei der Straßenverkehrsbehörde werden personenbezogene Daten der Teilnehmer am Feldversuch verarbeitet. Da für die Teilnahme die Freiwilligkeit gewahrt bleibt, genügt hier die informierte Einwilligung der Versuchsteilnehmer. Aus Gründen der Verfahrensvereinfachung sollen die für die Ausnahmegenehmigung erforderlichen Daten ebenfalls vom Projektbetreiber erhoben werden. Dies ist datenschutzrechtlich im Wege der Auftragsdatenverarbeitung für die Straßenverkehrsbehörde zulässig, soweit dafür vom Versuchsteilnehmer eine gesonderte Einwilligung eingeholt wird. Die Anmeldung zum Versuch und Beantragung der Ausnahmegenehmigung kann durch ein gemeinsames Antragsformular über das Internet erfolgen. Voraussetzung dafür ist, dass die beiden Einwilligungen für den Versuchsteilnehmer im Antragsformular deutlich zu unterscheiden sind und – in beiden Fällen gesondert – durch eine einfache elektronische Signatur erfolgen.

4.3 Justiz und Finanzen

4.3.1 Justiz

Urteil des Bundesverfassungsgerichts zum Großen Lauschangriff

Als ein Meilenstein für den Datenschutz ist das Urteil des *Bundesverfassungsgerichts* vom 3. März 2004[61] zu bewerten. Das Gericht hat entschieden, dass die den „*Großen Lauschangriff*“ regelnden Vorschriften der Strafprozessordnung in wesentlichen Teilen verfassungswidrig sind, und den Gesetzgeber aufgefordert, bis spätestens zum 30. Juni 2005 einen verfassungsmäßigen Zustand herzustellen. Angesichts der in den letzten Jahren mit Sorge zu beobachtenden ständigen Bestrebungen, die Datenschutzrechte der Betroffenen zugunsten von Sicherheits- und Strafverfolgungsinteressen immer weiter zurückzudrängen, ist die Entscheidung des Bundesverfassungsgerichts aus Datenschutzsicht besonders erfreulich.

61 1 BvR 2378/98

Es ist zu begrüßen, dass die von uns und anderen Landesdatenschutzbeauftragten vorgetragenen verfassungsrechtlichen Bedenken gegen die angegriffenen Vorschriften im Wesentlichen berücksichtigt wurden. Das Bundesverfassungsgericht bekräftigt mit seinem Urteil den hohen Rang des Grundrechts auf Unverletzlichkeit der Wohnung und des Rechts auf informationelle Selbstbestimmung und stellt den engen Bezug zwischen der Unverletzlichkeit der Wohnung und der Menschenwürde heraus. Das Gericht stellt klar, dass der absolut geschützte Kernbereich privater Lebensgestaltung nicht zugunsten der Strafverfolgung eingeschränkt werden darf. Damit darf es keine Strafverfolgung um jeden grundrechtlichen Preis geben[62].

Das Bundesverfassungsgericht hat betont, dass die *Privatwohnung* als „letztes Refugium“ ein Mittel zur Wahrung der Menschenwürde ist. Dies verlange zwar nicht einen absoluten Schutz der Räume der Privatwohnung, wohl aber absoluten Schutz des Verhaltens in diesen Räumen, soweit es sich als individuelle Entfaltung im Kernbereich privater Lebensgestaltung darstelle. Diese Anforderung des Gerichts gilt es in die Praxis umzusetzen.

Die einschlägigen Vorschriften sind nach den Maßstäben der Entscheidung des Bundesverfassungsgerichts zu überarbeiten. Zu beachten ist, dass nicht nur die Regelungen zum Großen Lauschangriff betroffen sind, sondern vielmehr auch andere heimliche Eingriffsbefugnisse, die den Bereich privater Lebensgestaltung zwangsläufig berühren, wie etwa die präventive Telekommunikationsüberwachung, die längerfristige Observation, der verdeckte Einsatz technischer Mittel, der Einsatz nachrichtendienstlicher Mittel und von verdeckten Ermittlern und andere Formen der verdeckten Datenerhebung. Auch diese Eingriffsbefugnisse sind nach den vom Bundesverfassungsgericht aufgestellten Maßstäben zu prüfen.

Nachdem das Bundesministerium der Justiz im Juni 2004 einen Referentenentwurf vorgelegt hatte, der lediglich eine minimale Umsetzung der Vorgaben des Bundesverfassungsgerichts vorsah, hat die Bundesregierung im September 2004 einen Gesetzentwurf zur Neuregelung der *akustischen Wohnraumüberwachung* vorgelegt[63]. Wie die Datenschutzbeauftragten des Bundes und der Länder auf ihrer letzten Konferenz im Oktober 2004 festgestellt haben, wird das Urteil des Bundesverfassungsgerichts vom 3. März 2004 in großen Teilen umgesetzt. Allerdings sind zentrale Punkte wie die Begriffsbestimmung des „unantastbaren Kernbereichs der privaten Lebensgestaltung“ und die Bestimmung des Kreises der Menschen des „persönlichen Vertrauens“ offen geblieben[64].

62 Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 2004, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2004“, S. 14

63 BR-Drs. 722/04

64 Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. Oktober 2004, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2004“, S. 15

Max-Planck-Gutachten: die Evaluierung der akustischen Wohnraumüberwachung

Nach der Entscheidung des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung legte das *Max-Planck-Institut* für ausländisches und internationales Strafrecht sein Gutachten zur Evaluierung der *akustischen Wohnraumüberwachung* vor. Das Gutachten „Rechtswirklichkeit und Effizienz der akustischen Wohnraumüberwachung" („Großer Lauschangriff") nach § 100 c Abs. 1 Nr. 3 StPO basiert auf der Untersuchung aller im Zeitraum 1998 bis 2001 bundesweit durchgeführten akustischen Wohnraumüberwachungen. Es handelt sich dabei um 119 Verfahren, wovon sechs Verfahren nach § 100 e StPO auf das Land Berlin entfallen.

Nach der Erhebung des Max-Planck-Instituts wurden 13 % der von den Staatsanwaltschaften beantragten Anordnungen einer akustischen Wohnraumüberwachung abgelehnt. Bei weiteren 19 % wurde die Maßnahme trotz eines gerichtlichen Anordnungsbeschlusses nicht umgesetzt, weil es bei der Umsetzung zu technischen Schwierigkeiten gekommen war. Bei immerhin 40 % der Maßnahmen gab es technische Schwierigkeiten mit der Sprach- und Aufzeichnungsqualität. Diese Erkenntnisse haben dann auch das Max-Planck-Institut dazu veranlasst, an einer Stelle des Gutachtens von „Grundrechtsschutz durch technische Unzulänglichkeit" zu sprechen. Da die Installation der Wanzen nicht immer unmittelbar im Anschluss an den Anordnungsbeschluss des Gerichtes erfolgte, gab es Probleme im Hinblick auf den Fristbeginn der Maßnahme, da die Beschlüsse offensichtlich von einer unverzüglichen Aufnahme der Wohnraumüberwachung ausgehen. Allerdings wurde auch festgestellt, dass die Vier-Wochen-Frist nur in 59 % der Fälle tatsächlich voll ausgeschöpft wurde.

Eine Erkenntnis zieht sich wie ein roter Faden durch das Gutachten. Den durchgeführten akustischen Wohnraumüberwachungen liegen zum großen Teil die Delikte Mord/Totschlag/Völkermord zugrunde, dicht gefolgt von der Gruppe der Betäubungsmitteldelikte. Die beiden Deliktsgruppen unterscheiden sich stark in ihrer Struktur. Wo die Tötungsfälle zumeist typische Ermittlungen im sozialen Nahraum mit sich bringen, meist nicht dem Bereich der organisierten Kriminalität zuzurechnen sind und in 88 % der Fälle zum Abhören der Wohnung geführt haben, sind die Betäubungsmittelfälle eher der organisierten Kriminalität zuzurechnen und bringen ein hoch konspiratives Verhalten der Beteiligten mit sich, oft auch einen Auslandsbezug, so dass dann entsprechend nur in 55 % der Fälle die Wohnung abgehört worden ist, in 32 % andere Räumlichkeiten als beispielsweise auch der Geschäftsraum der Betroffenen. Insofern wird immer wieder von tief greifenden strukturellen Unterschieden im Max-Planck-Gutachten gesprochen, die sich in den Evaluierungsergebnissen wiederfinden.

Bei den Tötungsdeliktsfällen lag die Erfolgsquote der akustischen Wohnraumüberwachung weit unter dem Gesamtergebnis, nach dem 30 % aller Maßnahmen erfolgreich oder bedingt erfolgreich waren. Bei den Tötungsdelikten waren dagegen ca. 50 % der Überwachungen ergebnislos und ein großer weiterer Teil nur indiziell belastend. Die Erfolgsquote in den Betäubungsmittelverfahren lag dagegen deutlich höher. In der Gesamtschau aller Verfahren waren immerhin 29 % der durchgeführten Maßnahmen inhaltlich ergebnislos, 12 % wegen technischer Probleme unverwertbar und 11 % durch die Betroffenen entdeckt worden.

Das Max-Planck-Institut weist zu der Frage der Intensität des Grundrechtseingriffs darauf hin, dass gerade die Verfahren wegen Tötungsdelikte den sozialen Nahbereich betreffen und damit eine ganz andere Kernbereichsrelevanz für die Grundrechte der Betroffenen haben. Dagegen kommt es in Verfahren wegen Betäubungsmitteldelikte nicht zu einer dem Kernbereich zuzuordnenden Kommunikation. Hier besteht nach Auffassung des Max-Planck-Instituts eher die Gefahr, dass der Schutzraum zur Organisation und Begehung von Straftaten missbraucht wird.

Mängel hat die Evaluation insbesondere bei der Benachrichtigung der Betroffenen und auch der Dokumentation festgestellt sowie der Verwertungsproblematik in weiteren Verfahren. Verbesserungsbedarf besteht auch hinsichtlich des Beginns der Vier-Wochen-Frist, die nicht berücksichtigt, dass der technische Verlauf in der Regel mehr Zeit benötigt.

Datenschutzrechtliche Prüfung der akustischen Wohnraumüberwachung in Berlin

Auch wir haben die in Berlin im Zeitraum von 1998 bis 2001 durchgeführten *akustischen Wohnraumüberwachungen* überprüft.

Die vom Max-Planck-Institut festgestellten Strukturen und Besonderheiten decken sich mit den von uns gewonnenen Erkenntnissen. Insbesondere die strukturellen Unterschiede zwischen akustischen Wohnraumüberwachungen in Verfahren wegen Tötungsdelikte und in Betäubungsmittelverfahren auf der anderen Seite sind besonders hervorzuheben. Bei Tötungsdelikten spielt das soziale Umfeld in der Regel eine herausragende Bedeutung bei den Ermittlungen, so dass der Kernbereich der Grundrechte besonders intensiv betroffen ist. Darüber hinaus ist in der Regel der Kreis der von der Maßnahme betroffenen Dritten zu einem großen Teil bestimmbar und meistens relativ festgelegt.

Die vom Max-Planck-Institut dargelegten Verbesserungspunkte gelten auch für die Berliner Wohnraumüberwachungen. Ungeachtet dessen darf man davon ausgehen, dass die Zahl der beantragten akustischen Wohnraumüberwachungen sinken wird, da die praktischen Anforderungen des Bundesverfassungsgerichts an die Umsetzung der akustischen Wohnraumüberwachung nur mit großem finanziellem und personellem Aufwand realisierbar sind. Vielleicht wird es dann „Grundrechtsschutz durch Geldaufwand" heißen.

Datenschutz bei der Rechtsanwaltskammer

Eine Bürgerin berichtete uns, sie habe sich in einer gebührenrechtlichen Angelegenheit an die Rechtsanwaltskammer Berlin gewandt und diese um Prüfung gebeten. Die Rechtsanwaltskammer habe daraufhin die von ihr vorgelegten Unterlagen an die Beschwerdegegnerin übersandt, ohne zuvor ihr Einverständnis eingeholt zu haben. Auf unsere Aufforderung zur Stellungnahme wurde uns mitgeteilt, der Berliner Beauftragte für Datenschutz und Informationsfreiheit sei nicht berechtigt, die bei der Rechtsanwaltskammer zu einem Beschwerdeverfahren geführten Unterlagen und Akten einzusehen.

Wir haben die *Rechtsanwaltskammer* darauf hingewiesen, dass der Berliner Beauftragte für Datenschutz und Informationsfreiheit nach § 28 Berliner Datenschutzgesetz (BlnDSG) die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den Behörden und sonstigen öffentlichen Stellen des Landes Berlin kontrolliert. Die Stellen sind verpflichtet, ihn bei der Erfüllung seiner Aufgaben zu unterstützen. Die kontrollierten Stellen haben Auskunft sowie Einsicht in alle Unterlagen und Akten zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, namentlich in die gespeicherten Daten und in die Datenverarbeitungsprogramme.

Auch Berufs- und Amtsgeheimnisse entbinden die speichernden Stellen nicht von der Unterstützungspflicht. Berufsrechtliche Vorschriften der Rechtsanwälte über die Verschwiegenheitspflicht ändern nichts an der Verpflichtung der Rechtsanwaltskammer, uns Auskunft über den Inhalt der Unterlagen des Beschwerdeverfahrens zu erteilen.

In dem uns vorliegenden Fall haben wir der Rechtsanwaltskammer empfohlen, vor einer Übermittlung von Beschwerdevorgängen die Einwilligung des jeweiligen Betroffenen einzuholen. Eine Übermittlung personenbezogener Daten ist nach § 13 BlnDSG nämlich nur dann zulässig, wenn der Betroffene eingewilligt hat oder eine Rechtsvorschrift dies erlaubt. Leider hat es die Rechtsanwaltskammer im konkreten Fall versäumt, das Einverständnis der Bürgerin vor der Weitergabe des Beschwerdevorgangs einzuholen. Eine abschließende Stellungnahme der Rechtsanwaltskammer steht noch aus.

Untersuchungshaftvollzugsgesetz

Nachdem der im Jahre 1999 vorgelegte Gesetzentwurf der Bundesregierung zu einem *Untersuchungshaftvollzugsgesetz* nicht weiterverfolgt worden war, hat das Bundesministerium der Justiz nunmehr einen Referentenentwurf eines Gesetzes zur Regelung des Vollzugs der Untersuchungshaft vorgelegt. Grundsätzlich ist es zu begrüßen, dass der Gesetzgeber den Handlungsbedarf erkannt hat, den Vollzug der Untersuchungshaft umfassend

gesetzlich zu regeln. Wir haben gegenüber der Senatsverwaltung für Justiz zu dem Referentenentwurf Stellung genommen und auf die aus datenschutzrechtlicher Sicht noch bestehenden Bedenken hingewiesen. Insbesondere sollte von einer inhaltlichen Überwachung der Unterhaltung mit Besucherinnen und Besuchern sowie des Schriftwechsels nicht nur in Ausnahmefällen abgesehen werden können. Vielmehr sollte nach Haftgründen differenziert werden. Lediglich im Falle der Untersuchungshaft wegen Verdunkelungsgefahr sollten diese Maßnahmen generell durch das Untersuchungshaftvollzugsgesetz vorgeschrieben werden. In den übrigen Fällen sollte eine Überwachung nur im Einzelfall aufgrund richterlicher Anordnung erfolgen dürfen. Diese Forderungen waren bereits 1999 von den Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung aufgestellt worden[65]. Ihre Umsetzung im weiteren Gesetzgebungsverfahren wäre sehr zu begrüßen.

Vorsorgeregister der Bundesnotarkammer

Um die Vormundschaftsgerichte in die Lage zu versetzen, bereits in einem frühen Stadium eines Betreuungsverfahrens Kenntnis vom Vorhandensein einer Vorsorgevollmacht zu erlangen und auf diese Weise überflüssige Betreuungen zu vermeiden, wurde die *Bundesnotarkammer* nach §§ 78 a bis 78 c der Bundesnotarordnung (BNotO) verpflichtet, ein *zentrales Vorsorgeregister* zu führen. Das Bundesministerium der Justiz wurde hierzu in § 78 a Abs. 3 BNotO ermächtigt, in einer zustimmungspflichtigen Rechtsverordnung die näheren Bestimmungen über die Ausgestaltung und Führung des Registers zu treffen. Ursprünglich sah der Entwurf in § 4 vor, dass eine Eintragung personenbezogener Daten des Bevollmächtigten in dieses Register nur dann erfolgen durfte, wenn dieser zuvor schriftlich eingewilligt hatte. Diese Lösung war aus unserer Sicht datenschutzrechtlich unbedenklich. Der aktuelle Entwurf der Rechtsverordnung sieht nunmehr vor, dass der Bevollmächtigte, der nicht schriftlich eingewilligt hat, schriftlich über die Speicherung seiner personenbezogenen Daten zu unterrichten und darüber aufzuklären ist, dass die Löschung der Daten aus dem Register jederzeit verlangt werden kann. Auf eine schriftliche Einwilligung des Bevollmächtigten kann insofern bei der Eintragung in das Register verzichtet werden. Die gewählte Widerspruchslösung führt zu einer Verschlechterung des Datenschutzes für den Bevollmächtigten. Eine Eintragung seiner Daten in das Vorsorgeregister ohne Vorlage einer schriftlichen Einwilligungserklärung ist mit datenschutzrechtlichen Grundsätzen nicht vereinbar und kann aus unserer Sicht auch durch eine Aufklärung der Bevollmächtigten durch die Bundesnotarkammer nicht ersetzt werden.

---

[65] Entschließung vom 16. August 1999, vgl. Anlagenband „Dokumente zum Datenschutz 1999“, S. 11

Mitteilung von Änderungen im Grundbuch an Verstorbene

In einer Eingabe wurde uns geschildert, das Grundbuchamt eines Amtsgerichts habe Bekanntmachungen von Grundbuchänderungen an eine längst verstorbene, jedoch noch immer im Grundbuch eingetragene Berechtigte übersandt. Der selbst als Berechtigter im Grundbuch eingetragene Petent sah darin einen datenschutzrechtlichen Verstoß und hat uns um unsere datenschutzrechtliche Bewertung gebeten.

Die Übermittlung von personenbezogenen Daten an Personen und andere Stellen außerhalb des öffentlichen Bereichs ist nach § 13 Berliner Datenschutzgesetz (BlnDSG) zulässig, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Rechtsgrundlage für die Datenübermittlung des Grundbuchamtes ist § 55 *Grundbuchordnung* (GBO). Danach soll jede Eintragung in das Grundbuch dem einreichenden Notar, dem Antragsteller und dem eingetragenen Eigentümer sowie allen aus dem Grundbuch ersichtlichen Personen bekannt gemacht werden. Die Eintragung soll neben dem Antragsteller und dessen Notar vor allem dem Eigentümer bekannt gemacht werden, damit dieser über das ihm gehörende Grundstück und den Inhalt des dazu gehörenden Grundbuchs stets informiert ist. Die Unrichtigkeit des Grundbuchs stellt die Ausnahme und nicht den Regelfall dar. Insbesondere genießt das Grundbuch nach §§ 891 ff. Bürgerliches Gesetzbuch (BGB) öffentlichen Glauben, so dass der Rechtspfleger grundsätzlich davon ausgehen kann und muss, dass die Eintragungen im Grundbuch richtig sind. Auch bei Unrichtigkeit des Grundbuchs kann sich das Grundbuchamt bei Bekanntmachungen an die Eintragungen halten. Es ist nicht zu Ermittlungen verpflichtet. Vielmehr würde es die Arbeit des Grundbuchamtes erheblich erschweren und verzögern, wenn bei jeder neuen Eintragung die Richtigkeit des Grundbuchs infrage gestellt werden müsste. Die Versendung von Bekanntmachungen an den eingetragenen Berechtigten ist also – auch wenn dieser inzwischen verstorben ist – von der Rechtsgrundlage des § 55 Abs. 1 GBO gedeckt. Einen Verstoß gegen datenschutzrechtliche Bestimmungen durch das Grundbuchamt konnten wir nicht feststellen.

4.3.2 Finanzen

Nachklang zur Parkkralle

In unserem Jahresbericht 2003 hatten wir über den Einsatz der *Parkkralle* in *Vollstreckungsverfahren* gegen säumige Kraftfahrzeugschuldner berichtet[66]. Wir hatten den Einsatz der Parkkralle als Druckpfändung und damit

[66] JB 2003, 4.3.2

datenschutzrechtlich unzulässig kritisiert. Durch eine Bürgerin wurden wir darauf aufmerksam gemacht, dass die Finanzverwaltung in einem Steuerfall bereits bei einem Steuerrückstand von 89,– € bei der Ankündigung von Vollstreckungsmaßnahmen auf den möglichen Einsatz der Parkkralle hingewiesen hat. Bei dem Schreiben handelte es sich offenbar um ein Formular, das in zahlreichen Fällen genutzt wird. Der Unterausschuss Datenschutz hat sich in seiner 31. Sitzung im August 2004 mit diesem Thema befasst. Auch wenn die Mitglieder des Unterausschusses Datenschutz nur zum Teil unsere Kritik an der Prangerwirkung der Parkkralle teilen, bestand jedoch Einigkeit darüber, dass bei der Frage des möglichen Einsatzes der Parkkralle immer auch der Grundsatz der Verhältnismäßigkeit zu beachten ist und dies auch bereits dann, wenn Vollstreckungsmaßnahmen angedroht werden. Eine Steuerschuld von 89,– € dürfte jedenfalls nicht den Einsatz der Parkkralle rechtfertigen; diese Höhe dürfte in den meisten Fällen eine Vollstreckung des Kraftfahrzeuges nicht rechtfertigen. Selbst der Einsatz der Parkkralle als solcher dürfte schon teurer sein als die hier in Rede stehende Steuerschuld.

Wir werden den Einsatz der Parkkralle weiter beobachten.

Aufregung bei den Steuerberatern – ein betrieblicher Datenschutzbeauftragter wird gebraucht

Seit Mitte des Jahres 2004 häuften sich bei uns die Anfragen von *Steuerberatern*, die sich nach der neuen Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten erkundigten. Auslöser dieser Anrufe waren zahlreiche Veröffentlichungen der Steuerberaterverbände, die mit Überschriften wie „Datenschutzbeauftragter vs. 25.000,– € Bußgeld … die Schonfrist ist am 23. Mai 2004 abgelaufen!“[67] auf datenschutzrechtliche Pflichten, die sich aus dem BGB ergeben, hinwiesen. Die Verunsicherung bei den Steuerberatern war groß.

Was war geschehen? Am 14. Januar 2003 war im Bundesgesetzblatt das Bundesdatenschutzgesetz (BDSG) neu bekannt gemacht worden. Die Umsetzung der Europäischen Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 war bereits mit der Änderung des Bundesdatenschutzgesetzes vom 18. Mai 2001[68] erfolgt. Nach vier kleineren Änderungen des Bundesdatenschutzgesetzes in so genannten Artikelgesetzen war das Bundesdatenschutzgesetz zur besseren Lesbarkeit im Januar 2003 neu gefasst worden. Eine Übergangsfrist von drei Jahren in der Novellierung des Bundesdatenschutzgesetzes vom 18. Mai 2001 hatte die Unternehmen verpflichtet, innerhalb von drei Jahren die Neuregelungen bis zum 23. Mai 2004 umzusetzen.

Bereits vor der Umsetzung der Europäischen Datenschutzrichtlinie gab es eine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten für

[67] BGBl. I 2003, S. 66

[68] BGBl. I, S. 904

nicht-öffentliche Stellen, wenn mindestens fünf Arbeitnehmer ständig mit der automatisierten Datenverarbeitung beschäftigt waren (§ 36 BDSG alte Fassung). Mit der Umsetzung der EU-Datenschutzrichtlinie wurden den betrieblichen Datenschutzbeauftragten allerdings mehr Pflichten übertragen, so dass der Gesetzgeber zur Umsetzung dieser Pflichten eine Übergangsfrist vorgesehen hatte[69].

4.4 Sozialordnung

4.4.1 Personaldatenschutz

Zugriff des Steuerungsdienstes auf IPV-Daten

Von dem behördlichen Datenschutzbeauftragten eines Bezirksamtes erhielten wir den Hinweis, dass dort der Steuerungsdienst lesenden Zugriff auf IPV und somit auf alle dort gespeicherten Personaldaten der Mitarbeiter erhalten soll.

Nach § 56 Abs. 3 Landesbeamtengesetz (LBG), der auf alle Beschäftigungsgruppen im öffentlichen Dienst entsprechend anzuwenden ist, dürfen Zugang zu *Personalaktendaten* nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist. Dies gilt auch für den Zugang im automatisierten Abrufverfahren.

Nach § 2 Abs. 4 Verwaltungsreform-Grundsätze-Gesetz (VGG) berät und unterstützt der Steuerungsdienst die Behördenleitung nach Maßgabe einer mit ihm abgeschlossenen Zielvereinbarung. Ferner berät und unterstützt er die Leistungs- und Verantwortungszentren sowie die Serviceeinheiten bei der Erarbeitung von Zielvereinbarungen und nimmt Controllingaufgaben wahr. Da der Dienstherr im Rahmen seiner Organisationsfreiheit regeln kann, welche Teile der Behörde personalverwaltende Aufgaben wahrnehmen sollen, kann auch die Zielvereinbarung zwischen Steuerungsdienst und Behördenleitung aufschlussreich sein.

Unabhängig davon lässt sich dem Leitfaden zu Einrichtung und Aufbaustrategie von Steuerungsdiensten in der Berliner Verwaltung (Stand: 30. Oktober 1998) unter Punkt 3.1 entnehmen:

1. Kennzeichnendes Merkmal für das steuerungsunterstützende Funktionsbild des Steuerungsdienstes ist seine „Proaktivität“ (vorausschauendes Denken und initiatives Handeln im Zuge eines strategischen, insbesondere betriebswirtschaftlichen Controllings, Prognose des Handlungsbedarfs).
2. Zur Erfüllung dieser Kernaufgaben sichert sich der Steuerungsdienst spezielle Methoden und Planungsinstrumente wie
   - Initiierung bzw. Erarbeitung zukunftsorientierter Entscheidungsmodelle für Steuerungszwecke,
   - Mittelausstattung,
   - Analysetätigkeiten.

Aus dieser Beschreibung ergibt sich, dass der Steuerungsdienst als eine über der Personalverwaltung agierende Stelle Strategie-/Planungs- und Querschnittsaufgaben beim Bezirksamt wahrnimmt, nicht dagegen die Verfolgung bzw. Bearbeitung von Einzelpersonalvorgängen.

Insoweit sieht der Leitfaden unter Nr. 4.2.2 konsequenterweise auch eine Trennung zwischen Steuerungsdienst und Personalservice vor, der dem Steuerungsdienst für seine nicht routinemäßig vorzunehmenden, zum Teil situationsabhängigen entscheidungsvorbereitenden und unterstützenden Arbeiten die *notwendigen* Informationen zur Verfügung zu stellen hat.

Zur Bewältigung der dem Steuerungsdienst insoweit auferlegten Aufgaben reicht es daher aus, Personalstatistiken zur Verfügung zu stellen, um anhand der dort ersichtlichen Strukturen die erforderlichen Planungen vornehmen zu können. Keinesfalls ist es erforderlich, zu jeder Zeit auf sämtliche Personaldaten bzw. Personalaktendaten der Beschäftigten Zugriff zu nehmen. Ob darüber hinaus in Einzelfällen Akteneinsichts- bzw. Zugangsrechte zu Personalaktendaten der Beschäftigten bestehen, ist dabei unter anderem maßgeblich von der Zielvereinbarung abhängig. Der behördliche Datenschutzbeauftragte teilte uns mit, dass der Steuerungsdienst keinen Zugriff auf IPV erhalten hat.

Übermittlung von Daten an das Zentrale Überhangmanagement (ZeP)

Ein Petent ist in einem Landesamt tätig und befindet sich derzeit im Personalüberhang. Seit dem 1. Mai 2004 wird seine Personalakte vom Zentralen Überhangmanagement (ZeP) geführt. Nach diesem Zeitpunkt hatte er bei dem Landesverwaltungsamt Berlin (LVwA) in üblicher Verfahrensweise Beihilfe beantragt. Der Betrag wurde – ohne dass ihm ein Bescheid zugegangen war – auf sein Konto überwiesen. Seine Nachfrage bei dem LVwA ergab, dass der Bescheid von dort bereits abgesandt worden sei, jedoch nicht direkt an ihn persönlich, sondern – gemäß einer Anweisung des ZeP – an das LVwA über den ZeP an ihn. Das ZeP konnte ihm jedoch keine Auskunft über den Verbleib des Bescheides geben. Später teilte uns der Petent mit, der Beihilfebescheid

[69] vgl. 4.8.1

des Landesverwaltungsamtes sei mit dreiwöchiger Verzögerung, bedingt durch den Umweg über das ZeP, nunmehr unter seiner privaten Postanschrift eingetroffen, aber offensichtlich im ZeP vorher geöffnet worden.

Das ZeP teilte hierzu mit, dem Landesverwaltungsamt seien nach § 8 a Abs. 1 Allgemeines Zuständigkeitsgesetz (AZG) die Aufgaben der Dienstbehörde bei der Berechnung, Festsetzung und Zahlbarmachung der Beihilfen für die Dienstkräfte des ZeP übertragen worden. Alle Angelegenheiten der *Beihilfe* für die Dienstkräfte des ZeP würden auf dieser Grundlage vom Landesverwaltungsamt – Beihilfestelle – selbständig wahrgenommen. Hierzu gehöre auch der Versand der erlassenen Beihilfebescheide. Eine Vereinbarung zu einer besonderen Versandart der Beihilfebescheide zwischen dem Landesverwaltungsamt und dem ZeP sei nicht getroffen worden.

Zum Versand der Beihilfebescheide greife das Landesverwaltungsamt auf die zwischen dem Beihilfe-DV-Programm BABSY und dem landesweiten Personalabrechnungsverfahren *IPV* eingerichtete Schnittstelle zum so genannten Verteiler zu. In diesem „Verteiler" sei im IPV-System regelmäßig die Beschäftigungsbehörde, die einsetzende Dienststelle sowie das Bearbeiterzeichen der jeweiligen Dienstkraft hinterlegt.

Sofern eine Dienstkraft z. B. beurlaubt oder langfristig erkrankt sei, könne eine Übersendung des Beihilfebescheides an die Dienstanschrift der Dienstkraft nach diesem Verteiler nicht erfolgen. In diesen Fällen werde der Beihilfebescheid an die personalaktenführende Stelle zur Weiterleitung übersandt. Das Gleiche gelte, wenn ein zustellfähiger „Verteiler" nicht angegeben werden kann. Dies könne insbesondere bei Personalüberhangkräften der Fall sein, wenn in den Einsatzdienststellen eine Personalüberhangkraft ohne Bearbeiterzeichen beschäftigt ist.

Das Landesverwaltungsamt habe auf Nachfrage des ZeP mitgeteilt, dass die Dienstkräfte selbst zum Beihilfeantrag Angaben zu besonderen Versandanschriften machen können, beispielsweise wenn nur Versand an die Privatanschrift erfolgen soll. Hierauf hätte die personalaktenführende Stelle keinen Einfluss.

Im beanstandeten Fall sei der Beihilfebescheid vom Landesverwaltungsamt der personalaktenführenden Stelle zu Weiterleitung übersandt worden. Wegen urlaubsbedingter Abwesenheit der zuständigen Bearbeiterin wäre die Absendung des Beihilfebescheides an den Petenten verzögert und mit zweiwöchiger Verspätung nachgeholt worden. Unzutreffend sei allerdings der Vorhalt, der Beihilfebescheid wäre geöffnet worden. Der Bescheid sei vielmehr ungeöffnet dem Petenten zugeleitet worden.

Die Ausführungen des ZeP zur Sach- und Rechtslage waren zutreffend und in der Sache nachvollziehbar. Insbesondere ist eine klare Zuordnung von Überhangkräften zu Beschäftigungsbehörden und Einsatzdienststellen dann nicht möglich, wenn eine Personalüberhangkraft ohne Bearbeiterzeichen beschäftigt ist und damit ein zustellfähiger Verteiler nicht angegeben werden kann. Ein Verstoß gegen geltendes Datenschutzrecht konnte daher nicht festgestellt werden.

Informationsfreiheit beim Personalüberhang

Eine Petentin beschwerte sich über die Ablehnung des Antrags ihres Rechtsanwalts auf Einsichtnahme in Verwaltungsvorgänge durch die Senatsverwaltung für Finanzen. Die Vorgänge betrafen ihre Zuordnung zum Personalüberhang und ihre vorgesehene Umsetzung. Die Ablehnung des Antrags erfolgte unter Hinweis auf § 3 Informationsfreiheitsgesetz (IFG). Die Petentin bat um Prüfung, ob das Informationsfreiheitsgesetz nicht doch als Rechtsgrundlage für die begehrte Einsichtnahme herangezogen werden kann.

Der Antrag, soweit er sich auf die Einsichtnahme in die *Personalunterlagen* der Petentin bezieht, stützt sich bei einer Landesbeamtin auf § 56 c Landesbeamtengesetz (LBG). Diese Vorschrift verdrängt als speziellere Vorschrift das Informationsfreiheitsgesetz.

In § 56 c Abs. 4 LBG ist auch geregelt, dass bei Beamten ein Recht auf Einsicht in andere Akten besteht, die personenbezogene Daten über sie enthalten und für ihr Dienstverhältnis verarbeitet oder genutzt werden, soweit gesetzlich nichts anderes bestimmt ist. Beantragt wurde hier die *Akteneinsicht* in die Verwaltungsvorgänge, die sich auf die Anbringung des kw-Vermerks bei der Stelle der Petentin beziehen. Im ablehnenden Bescheid der Senatsverwaltung für Finanzen heißt es, dass die Verwaltungsvorgänge, in die Akteneinsicht begehrt wurde, Personaldaten enthalten. Soweit es sich um Personaldaten der Petentin handelt, kann sie sich auf § 56 c LBG als Anspruchsgrundlage berufen.

Wenn die Einsichtnahme deswegen unzulässig ist, weil die Daten der Betroffenen mit Personaldaten von anderen Beschäftigten oder geheimhaltungsbedürftigen nicht-personenbezogenen Daten derart verbunden sind, dass eine Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist, dann ist der Beamtin nach § 56 c Abs. 4 Satz 3 LBG jedenfalls Auskunft zu erteilen.

Einrichtung von Telearbeitsplätzen

Die AOK Berlin beabsichtigte im Bereich Firmen- und Privatkundenberatung im Außendienst die Einführung von Telearbeitsplätzen für einzelne Mitarbeiter/Mitarbeiterinnen. Diese sollten einen Zugriff auf das EDV-System zur Versichertenverwaltung und somit auch einen Zugriff auf die Sozialdaten der Versicherten in elektronischer Form erhalten.

Um den ordnungsgemäßen Umgang mit den personenbezogenen Daten sicherzustellen, wurde im April 2003 eine Dienstvereinbarung für die Pilotierung der Telearbeit zwischen dem Vorstand und dem Personalrat unterzeichnet. Diese Dienstvereinbarung beinhaltete auch Regelungen zum Datenschutz. In einer Nebenabrede zum Arbeitsvertrag/Anstellungsvertrag sowie in einer Verpflichtungserklärung zum Telearbeitsplatz sollte sich der/die Telearbeiter/in zur Einhaltung der datenschutzrechtlichen Vorschriften verpflichten.

Aus datenschutzrechtlicher Sicht bestanden gegen die Einrichtung von *Telearbeitsplätzen* grundsätzlich keine Bedenken[70]. Da es sich bei *Sozialdaten* der Versicherten jedoch um besonders sensibles Datenmaterial handelt, haben wir die AOK auf folgende Punkte ausdrücklich hingewiesen:

1. Wegen des hohen Schutzniveaus von Sozialdaten sollte zunächst geprüft werden, ob eine anonymisierte oder pseudonymisierte Datenverarbeitung am Telearbeitsplatz möglich ist.
2. Die Dauer der Wahrnehmung der Aufgaben in Form von alternierender Telearbeit sollte zunächst auf einen Zeitraum von maximal zwei Jahren begrenzt werden; Verlängerungen sind möglich, wenn die dienstlichen und persönlichen Voraussetzungen weiterhin gegeben sind.
3. Es sollten nur Mitarbeiterinnen und Mitarbeiter an der Telearbeit teilnehmen, deren Beschäftigungszeit mindestens ein Jahr im Aufgabengebiet beträgt.
4. Es ist eine schriftliche Einverständniserklärung der Haushaltsangehörigen für die Kontrollen des Dienstherrn und der Datenschutzkontrollinstanzen in der Wohnung einzuholen sowie die Verpflichtung zur Anzeige von Änderungen im häuslichen Bereich.
5. Die Teilnehmer an der Telearbeit sind schriftlich über die Bestimmungen zu Straftaten und Ordnungswidrigkeiten nach §§ 43, 44 BDSG zu informieren.
6. Die Teilnehmer sind auf das Datengeheimnis nach § 5 BDSG zu verpflichten.
7. Die Einrichtung von Telearbeitsplätzen muss für jeden Einzelfall in Abstimmung mit dem betrieblichen Datenschutzbeauftragten erfolgen.
8. Es sollte geregelt werden, was geschieht, wenn der Zutritt zum häuslichen Bereich (Telearbeitsplatz) verweigert wird. Hier kann es sinnvoll sein, die Möglichkeit vorzusehen, dass das Telearbeitsverhältnis außerordentlich beendet wird.
9. In der Vereinbarung mit dem Telearbeiter sollte auch ein Rückholrecht des dienstlichen Geräts, auch zu Prüfzwecken durch den Arbeitgeber, festgeschrieben werden.

[70] JB 1998, 3.2

Wir empfahlen der AOK darüber hinaus, bestimmte Daten (insbesondere Patientendaten, die der ärztlichen Schweigepflicht unterliegen, sowie Personaldaten) nicht auf Telearbeitsplätzen zu verarbeiten.

Bericht des Rechnungshofs

Ein Bürger hatte im Rechnungshofbericht zur Prüfung der Personalausgaben für Arbeiter bei der Berliner Feuerwehr detaillierte Angaben zu seiner Person vorgefunden, die nur seiner Personalakte entnommen worden sein konnten, und fragte nach, ob Dritte seine Personalakte lesen dürften.

Nach § 88 Landeshaushaltsordnung (LHO) hat der *Rechnungshof* die Aufgabe, die gesamte Haushalts- und Wirtschaftsführung Berlins einschließlich seiner Sondervermögen und Betriebe zu prüfen. Dabei erstreckt sich die Prüfung nach § 90 LHO auf die Einhaltung der für die Haushalts- und Wirtschaftsführung geltenden Vorschriften und Grundsätze. Unterlagen, die der Rechnungshof zur Erfüllung dieser Aufgaben für erforderlich hält, sind ihm nach § 95 Abs. 1 LHO auf Verlangen fristgemäß vorzulegen.

Letztgenannte Vorschrift enthält jedoch keinen Hinweis auf die Einsichtnahme oder Übermittlung in bzw. von Personalakten und entspricht als Rechtsgrundlage nicht den Grundsätzen der Normenklarheit, Zweckbindung und Verhältnismäßigkeit. Daher fordern die Datenschutzbeauftragten seit geraumer Zeit eine eigenständige normenklare Regelung für die Einsichtnahme in Personalakten.

Nach § 11 Abs. 4 Berliner Datenschutzgesetz (BlnDSG) ist der Zugriff auf personenbezogene Daten zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen der Rechnungsprüfung ebenfalls nur insoweit zulässig, als er für die Ausübung dieser Befugnisse unverzichtbar ist. Insoweit reicht im ersten Schritt eine anonymisierte Übermittlung der angeforderten Daten aus. Sollte der Rechnungshof in einzelnen Fällen noch Prüfungsbedarf anmelden, sind ihm in einem weiteren Schritt die erforderlichen Daten zur Verfügung zu stellen. Bei Nachfragen wären auch personenbezogene Daten zu übermitteln, wenn dies vom Rechnungshof gewünscht wird.

Übermittlung von Personaldaten an Dritte

Ein Bürger hatte sich danach erkundigt, ob und welche Datenschutzvorschriften es der Deutschen Bahn AG verbieten würden, den Namen eines Mitarbeiters, der ihm am DB-Schalter eines Bahnhofs unhöflich begegnet sei bzw. schlecht bedient hatte, zu benennen.

Das Übermitteln personenbezogener Daten des Betroffenen (hier: des Beschäftigten der Deutschen Bahn AG) ist zulässig, soweit dies zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und kein Grund zu der

Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung und Nutzung hat (§ 28 Abs. 3 Nr. 1 BDSG).

Ein Anspruch auf Nennung des *Mitarbeiternamens* gegen die Deutsche Bahn AG besteht daher nur dann, wenn dies zur Wahrung des berechtigten Interesses des Bürgers erforderlich ist. Insoweit müsste er darlegen, weshalb die Kenntnis des Namens des Beschäftigten zur Wahrung bzw. Durchsetzung seiner Belange vonnöten ist.

Wenn ein derartiges Interesse vorläge, müsste zusätzlich durch die Deutsche Bahn AG als Arbeitgeberin geprüft werden, ob das schutzwürdige Interesse des Mitarbeiters die Übermittlung seines Namens an Dritte ausschließt. Zwar werden zunehmend Namen von Beschäftigten im Zuge der Bestrebungen nach mehr Verwaltungstransparenz und Bürger-/Kundenfreundlichkeit von Unternehmen und Verwaltungen preisgegeben, jedoch besteht umgekehrt kein Anspruch des Bürgers bzw. Kunden auf Nennung von Namen der Beschäftigten, wenn sich anstehende Probleme auch ohne diese Nennung erledigen lassen.

Heimliches Mithören im Call-Center der DB Dialog

Von der Mitarbeiterin eines Tochterunternehmens der Deutschen Bahn AG erhielten wir den Hinweis, dass Telefongespräche der Beschäftigten im Call-Center mit Kunden ohne deren Wissen zur Qualitätskontrolle mitgehört werden.

Die Deutsche Bahn AG teilte mit, dass durch eine entsprechende Bandansage die Kunden zu Beginn eines Anrufs über das *Mithören* und ihre Widerspruchsmöglichkeit informiert würden. Dagegen würden die Mitarbeiter nicht über diese Maßnahme in Kenntnis gesetzt. Sie würden jedoch generell über Abhörmaßnahmen in Kenntnis gesetzt, nicht zuletzt aufgrund einer entsprechenden Verankerung im Rahmentarifvertrag. Der Betriebsrat habe im Übrigen dem Mithören zum Zwecke der Qualitätssicherung zugestimmt.

Das unbemerkte Ab- und Mithören von Telefonaten im Bereich von *Call-Centern* greift in unzulässiger Weise in grundrechtliche Positionen der Beschäftigten ein, da sie insbesondere in ihren allgemeinen Persönlichkeitsrechten, im Recht am eigenen Wort und in ihrem Recht auf informationelle Selbstbestimmung tangiert werden. So genannte Mystery-Calls, bei denen Anrufe durch ein beauftragtes Unternehmen erfolgen, die als Testanrufe gestaltet werden und deren Ergebnisse Qualitätsabweichungen bei Standardgesprächsszenarien wiedergeben, sind dagegen datenschutzrechtlich dann zulässig, wenn die Identität der getesteten Telefonagenten dabei nicht erfasst und auch nicht im weiteren Prozedere verwendet wird (unpersonalisierte Mystery-Calls).

In Zukunft soll das Verfahren folgendermaßen durchgeführt werden:

1. Dem Kunden wird im Fall des Mithörens durch eine Bandansage ein Einspruchsrecht gegeben.
2. Macht der Kunde von seinem Einspruchsrecht Gebrauch, wird nicht weiter mitgehört.
3. Der Mitarbeiter wird darüber in Kenntnis gesetzt, dass innerhalb eines halben Arbeitstages bzw. maximal vier Stunden ein Mithören als Qualitätskontrolle erfolgen wird.

Speicherung von Bewerberdaten

Ein Bürger hatte sich bei einer Stiftung um ein Stipendium beworben und musste dazu eine Einverständniserklärung bezüglich der Speicherung und Weitergabe seiner Bewerbungsdaten unterschreiben. Da seine Bewerbung nicht erfolgreich war, widerrief er das Einverständnis. Dieser Widerruf wurde jedoch mit der Begründung zurückgewiesen, es sei erforderlich, die Daten weiterhin zu speichern, um den Ausschluss einer erneuten Bewerbung sicherzustellen.

Bewerberdaten dürfen nur bis zum Zeitpunkt der Entscheidung verwendet werden. Sobald die Auswahl stattgefunden hat, sind die Unterlagen so lange zu sperren, wie noch mit Rechtsstreitigkeiten zu rechnen ist, und dann zu vernichten oder dem Betroffenen zurückzugeben. Die speichernde Stelle darf deshalb dem Bewerber weder den Wunsch unterstellen, sich auch weiterhin zu bewerben, noch auf das eigene Interesse verweisen, sich z. B. im Hinblick auf künftige Vakanzen rechtzeitig mit Informationsmaterial zu versorgen. Die Entscheidung über eine Verlängerung des Verarbeitungszeitraums liegt daher allein bei dem Betroffenen, ohne dessen Einwilligung eine Weiterverwendung unzulässig wäre.

Im vorliegenden Fall wurde dem Bewerber eine „freiwillige“ Einverständniserklärung zur Verwendung seiner Bewerbungsunterlagen und Speicherung seiner Bewerberdaten auch für den Fall seiner Ablehnung vorgelegt. Eine Einwilligung als Verarbeitungsregulativ kann jedoch nur so lange akzeptiert werden, wie sich der Betroffene nicht in einer Situation befindet, die ihn praktisch dazu nötigt, sich mit der Verarbeitung der jeweils verlangten Daten einverstanden zu erklären. Zwar können sich die Bewerber vorliegend auch als Stipendiaten bei anderen Förderwerken bewerben, so dass ein existenzieller Druck für sie nicht besteht. Dennoch bleibt fraglich, ob es sich angesichts der nicht unwesentlichen Geld- und Bildungsvorteile um eine wirklich „freie“ Entscheidung des Betroffenen handelt. Die Speicherung der „Stammdaten“ (Name, Studienfach, Anschrift) von abgelehnten Bewerbern hielten wir bei Vorliegen einer entsprechenden Einverständniserklärung nach Maßgabe des § 4 a BDSG für einen Zeitraum von längstens fünf Jahren für zulässig. Die Einverständniserklärung war jedoch dahingehend zu konkretisieren, welche Daten der abgelehnten Bewerber aus welchen Gründen und für welchen Zeitraum gespeichert werden.

In der uns vorliegenden Einverständniserklärung des Studienförderwerkes wurden im Übrigen freiwillige Erklärungen (zur Einbehaltung bzw. Vernichtung von Bewerberunterlagen) und obligatorische Erklärungen zur Speicherung der Stammdaten vermischt. Wir haben empfohlen, in der Erklärung klarzustellen, dass der Bewerber auf Wunsch seine Unterlagen zurückerhält.

Ebenso verhielt es sich mit der Erklärung zur Weitergabe von Anschrift, Telefonnummer, Hochschulort und Studiengang an Mitstipendiaten, Vertrauensdozenten und Referate. Der Stiftung empfahlen wir, in der Einverständniserklärung sowohl Daten als auch Adressaten einzeln aufzuführen, so dass der Bewerber entscheiden kann, ob und ggf. welches Datum an welchen Adressaten übermittelt werden darf.

4.4.2 Gesundheit

Gesundheitsmodernisierung – Wirkungen und Nebenwirkungen

Das Gesetz zur *Modernisierung der gesetzlichen Krankenversicherung* (GMG) zeigte erste Wirkungen. Während die meisten Menschen die finanziellen Auswirkungen, z. B. die Einführung einer *Praxisgebühr*, beschäftigten, war das Jahr 2004 im Datenschutz vor allem durch Diskussionen zur *elektronischen Gesundheitskarte* geprägt. Viele Details um die Konzeption der Gesundheitskarte sind noch ungeklärt. Gegenwärtig erarbeitet eine Unterarbeitsgruppe des Arbeitskreises Gesundheit und Soziales der Datenschutzbeauftragten von Bund und Ländern eine gemeinsame Position. Dabei geht es insbesondere um die Frage der Feingliedrigkeit der Zugriffsrechte, mit denen die Regelungen des § 291 a Sozialgesetzbuch V (SGB V) umgesetzt werden, sowie um die Telematikstruktur. So ist zu prüfen, ob durch die technischen Optionen nicht etwa ein faktischer Zwang auf die Patienten zur Offenbarung von Daten ausgeübt wird. Mit besonderer Aufmerksamkeit werden die Ergebnisse der Tests in den verschiedenen Modellregionen verfolgt, zu denen Berlin nicht gehört.

Zu den ab 1. Januar 2004 geltenden Neuregelungen in der gesetzlichen Krankenversicherung gehört auch, dass die Krankenkassen seither Fahrtkosten zu einer ambulanten Behandlung bei entsprechender Selbstbeteiligung nur nach vorheriger Genehmigung und in besonderen Ausnahmefällen übernehmen. Dazu ist es erforderlich, dass der behandelnde Arzt ein Formular „Verordnung einer Krankenbeförderung“ bei der Krankenkasse einreicht. Dieses Formular übergibt der Patient dann beispielsweise einem Taxifahrer zum Verbleib, damit dieser gegenüber der Krankenkasse die Fahrtkosten nach Abzug der Selbstbeteiligung des Patienten verrechnet bekommt. Dabei muss der Patient dem Taxifahrer seine Diagnose offenbaren. Nach massiver Kritik der Datenschutzbeauftragten von Bund und Ländern einigten sich zunächst die Spitzenverbände der gesetzlichen Krankenkassen und die Kassenärztliche Bundesvereinigung darauf, dass auf dem Exemplar für den Transporteur die Diagnose nicht genannt wird. Parallel hatten die Spitzenverbände der gesetzlichen Krankenkassen und die Kassenärztliche Bundesvereinigung zugesichert, dass ab 1. Januar 2005 ein neues Verordnungsmuster in Umlauf gebracht wird. Bis Anfang Dezember konnte trotz der grundsätzlichen Einigung dem Bundesbeauftragten für den Datenschutz kein neuer Verordnungsentwurf vorgelegt werden, so dass die Zwischenlösung sicherlich noch einige Monate fortgeführt werden muss.

Meldedaten für Mammographie-Screening

Im Dezember 2003 beschloss der Bundesausschuss der Ärzte und Krankenkassen im Rahmen der Krebsfrüherkennungsrichtlinien, die Früherkennung von Brustkrebs durch ein *Mammographie-Screening* zu ergänzen. Dazu soll jede Frau, unabhängig davon, ob sie gesetzlich, privat oder gar nicht krankenversichert ist, ab dem Alter von 50 Jahren bis zum Ende des 70. Lebensjahres im Zweijahresabstand persönlich und schriftlich zu einer für die Frauen kostenlosen Untersuchung auf freiwilliger Basis eingeladen werden. Für die Einladungen sollen Daten der Melderegister verwendet werden. Lediglich wenn Einzuladende bereits an Brustkrebs erkrankt sind, soll eine Einladung unterbleiben.

Dies setzt voraus, dass die Daten der Einzuladenden mit den Daten der Krebsregister abgeglichen werden. Da die Daten im Gemeinsamen Krebsregister der neuen Bundesländer und Berlin unter einem Pseudonym gespeichert sind, muss also aus den Meldedaten dieses Pseudonym wieder erzeugt werden. Damit sind die Voraussetzungen für eine regelmäßige Datenübermittlung an eine öffentliche Stelle nach § 26 Abs. 2 Berliner Meldegesetz gegeben, für die eine besondere Rechtsvorschrift Voraussetzung ist.

Der Datenabgleich selbst soll in einer gesonderten „Zentralen Stelle“ durchgeführt werden. Welche das sein sollte, war zunächst unklar. Schließlich wurde vorgeschlagen, dass diese Stelle bei der Kassenärztlichen Vereinigung Berlin angesiedelt werden soll. Da dies aber weder als eine gesetzliche Aufgaben der Kassenärztlichen Vereinigung festgelegt ist, noch eine Befugnis zur Verarbeitung personenbezogener Daten für diese Zwecke vorliegt, gibt es für diese Organisationsform keine Rechtsgrundlage. Hinzu kommt, dass diese Zentrale Stelle auch Daten privatversicherter Frauen verarbeiten soll. Da sich die Regelungen zur Kassenärztlichen Vereinigung bisher nur auf Mitglieder der gesetzlichen Krankenversicherung beziehen, kann eine Lösung des Problems nur darin bestehen, dass der Berliner Landesgesetzgeber ein „Errichtungsgesetz“ für eine Zentrale Stelle erlässt. Nach längeren Diskussionen mit der Senatsverwaltung für Gesundheit, Soziales und Verbraucherschutz und dem Verweis darauf, dass die Rechtslage in den anderen Bundesländern von den dortigen Datenschutzbeauftragten ähnlich gesehen wird, soll ein Referentenentwurf für ein entsprechendes Gesetz erarbeitet werden.

Qualitätssicherungsrichtlinie Dialyse

Kurz vor Jahresende erhielten wir zur Stellungnahme vom Gemeinsamen Bundesausschuss den Entwurf für eine Richtlinie zur Sicherung der Qualität von Dialysebehandlungen. In den vergangenen Jahresberichten[71] berichteten wir bereits über die bislang auf freiwilliger Grundlage organisierte *Qualitätssicherung für die Nierenersatztherapie* (QuasiNiere). Nunmehr werden alle Behandlungseinrichtungen verpflichtet, sich an diesen Qualitätssicherungsmaßnahmen zu beteiligen. Die datenschutzrechtlich gute Lösung des bisherigen Verfahrens ersetzt die Namen und andere identifizierende Daten der Patienten durch Pseudonyme und lässt diese von einem Notar als Datentreuhänder nach festen Regeln verwalten, ohne dass Dritte darauf Zugriff haben.

Mit dieser Richtlinie sollen die Ärzte verpflichtet werden, ohne Information der Patienten oder Einholung einer Einwilligungserklärung Gesundheitsdaten über die Kassenärztlichen Vereinigungen an einen Datenanalysten zu senden. Der Entwurf sieht außerdem eine Honorierung der Ärzte für ihre Leistungen nur dann vor, wenn sie Daten aller ihrer gesetzlich versicherten Patienten in dieses Qualitätssicherungssystem einliefern.

In der gegenwärtig noch nicht abgeschlossenen Diskussion kommen eine Reihe von Datenschutzbeauftragten der Länder – wie auch unsere Behörde – und der Bundesbeauftragte zu dem Schluss, dass durch dieses Verfahren das informationelle Selbstbestimmungsrecht der Patienten vollständig negiert wird. Der Patient wird faktisch über den Arzt zur Teilnahme an der Maßnahme verpflichtet. Eine Einwilligungslösung fehlt vollständig und Auskunftsrechte der betroffenen Patienten, insbesondere hinsichtlich der über den gesamten Zeitraum der Dialyse, d. h. von Beginn der Dialyse an bis zum Tod des Patienten, gespeicherten Gesundheitsdaten, werden nicht einmal erwähnt. Im Datenflusskonzept ist auch kein Verfahren vorgesehen, das im Unterschied zum bisherigen Qualitätssicherungssystem den Patienten unkompliziert Auskunft über die über ihn gespeicherten Daten einschließlich Ausdrucke der medizinischen Daten erlaubt. Die Datenschutzbeauftragten von Bund und Ländern wollen alles daran setzen, dass in dieser ersten die Qualitätssicherung betreffenden Richtlinie des Gemeinsamen Bundesausschusses nach dem Gesundheitsmodernisierungsgesetz nicht nur ein hoher technischer Standard des Datenschutzes, sondern auch die Rechte der Patienten gesichert werden.

Beihilfe zur „Beihilfe“

Wir wurden darüber unterrichtet, dass die Bearbeitung von Beihilfeanträgen von Mitarbeitern der Beihilfestelle von „Kollege zu Kollege“ und manchmal auch vom fachvorgesetzten Gruppenleiter vorgenommen wird. Wir überprüften die Beihilfestelle und stellten Folgendes fest: Die Zuständigkeit für die Bearbeitung der Beihilfeanträge von Mitarbeitern der Beihilfestelle richtete sich unabhängig von der Stellung der Mitarbeiter zueinander nach dem Anfangsbuchstaben des Nachnamens. Im Vertretungsfall konnten auch die Fachvorgesetzten die Beihilfeabrechnungen vornehmen.

Wir regten an, diese Organisation zu überdenken, um den Anforderungen des § 56 a Landesbeamtengesetz (LBG) besser zu entsprechen und zu gewährleisten, dass *Beihilfeakten* nur für Beihilfezwecke verwendet werden können. Die Beihilfestelle wurde nach den gesetzlichen Erfordernissen umorganisiert.

Gegenüber der ursprünglichen Verfahrensweise ist diese Umorganisation eine Verbesserung, die sich in der Praxis allerdings bewähren muss. Beihilfevorgänge sollen nach § 56 a LBG in einer von den übrigen Personalverwaltungen getrennten Organisationseinheit bearbeitet werden. Diesem Schutzgedanken des Landesbeamtengesetzes muss auch in der internen Organisationsstruktur der Beihilfestelle Rechnung getragen werden. Die gesetzliche Anforderung, dass Beihilfedaten nur für Beihilfezwecke verwendet werden dürfen, schließt aus, dass Bedienstete, die Aufsicht über die Mitarbeiter ausüben, Kenntnis von Beihilfedaten nehmen können. Die neue Organisationsstruktur schließt zwar aus, dass Kollegen am Nachbartisch oder -zimmer oder unmittelbare Fachvorgesetzte die Beihilfevorgänge bearbeiten, es bleibt jedoch abzuwarten, ob die dadurch erreichte Vertraulichkeit auch den gesetzlichen Anforderungen in der Praxis entspricht.

Die vertrauensärztliche Begutachtung

Eine Beamtin trug vor, dass sie unter Vorlage eines fachärztlichen Attestes die Befreiung von der Teilnahme am Nachtdienst beantragt habe. Die Dienststelle habe sie daraufhin gebeten, sich beim Amts- und Vertrauensärztlichen Dienst des Bezirksamtes vorzustellen. Dieser habe nicht nur ihre Befreiung für ein Jahr, sondern darüber hinaus auch eine Behandlung zur Gewichtsreduktion empfohlen. Die Dienststelle habe daraufhin verfügt, dass sie dem nachzukommen habe. Sie habe jedoch widersprochen. Um die Angelegenheit zu klären, sei der Schriftwechsel zwischen dem Amts- und Vertrauensärztlichen Dienst und der Dienststelle durch den Amts- und Vertrauensärztlichen Dienst an die Personalabteilung übermittelt worden. Sie hatte einer Entbindung von der ärztlichen Schweigepflicht nicht zugestimmt.

Der *Amtsarzt* wird als Sachverständiger und Gutachter für die Dienstbehörde tätig. Nach § 77 Abs. 1 Satz 3 LBG sind Beamte verpflichtet, sich bei Zweifeln über ihre Dienstfähigkeit nach Weisung der Dienstbehörde ärztlich untersuchen und auch beobachten zu lassen, falls ein Amtsarzt dies für erforderlich hält. Entzieht sich dem der Beamte trotz wiederholter schriftlicher

[71] JB 2003, 4.5.1

Aufforderung ohne hinreichenden Grund, kann er so behandelt werden, als ob seine Dienstunfähigkeit ärztlich festgestellt worden wäre (§ 77 Abs. 1 Satz 4 LBG). Aufgrund der Bezugnahme in § 77 a LBG (begrenzte Dienstfähigkeit) ist diese Regelung auch auf eine strittige teilweise Dienstunfähigkeit anwendbar.

Eine Befugnis, an die Dienstbehörde medizinische Daten aus der Begutachtung zu übermitteln, ergibt sich aus dieser Vorschrift nicht. Vielmehr kann § 77 Abs. 1 Satz 4 LBG nur so verstanden werden, dass das Gesetz keine Übermittlungsbefugnis regeln wollte, denn sonst wäre Satz 4 sinnlos. Die Datenübermittlung konnte daher nicht auf § 77 Abs. 1 Satz 4 LBG gestützt werden.

Auch nach § 6 a Abs. 2 BlnDSG ist die Übermittlung von „Daten besonderer Kategorien“ nur zulässig, wenn der Betroffene ausdrücklich eingewilligt hat. Zwar hat das Gesundheitsamt in einem Aktenvermerk festgehalten, dass mit der Dienstkraft besprochen worden sei, dass dem Dienstherrn die Notwendigkeit der Gewichtsreduktion mitgeteilt wird: „Sie erklärt sich einverstanden und wolle sich umgehend um Gewichtsreduzierung bemühen.“ Dieser handschriftlich gefertigte Aktenvermerk genügte jedoch nicht den Anforderungen an eine Einwilligungserklärung nach § 6 a Abs. 2 BlnDSG. Nach § 6 Abs. 3 BlnDSG ist bei der Datenverarbeitung aufgrund einer Einwilligung des Betroffenen dieser in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten aufzuklären. Die Aufklärungspflicht umfasst bei beabsichtigten Übermittlungen auch den Empfänger der Daten sowie den Zweck der Übermittlung. Der Betroffene ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass er die Einwilligung verweigern kann. Nach § 6 Abs. 4 BlnDSG bedarf die Einwilligung der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Schriftform bedeutet, dass die Einwilligung vom Betroffenen unterschrieben sein muss, was hier erkennbar nicht der Fall war.

Die detaillierten medizinischen Feststellungen der gutachterlichen Untersuchung durften dem Dienstherrn nicht übermittelt werden. Der Dienstherr hätte jedoch eine gesundheitlich bedingte Dienstfähigkeit unterstellen können, bis die Beamtin der Übermittlung notwendiger medizinischer Daten zugestimmt hätte.

Krank und arbeitslos

Einer arbeitslosen Bürgerin wurde die Diagnose „Krebs“ gestellt. Sie teilt mit, dass ihre Krankenkasse beim Medizinischen Dienst der Krankenkassen (MDK) ein Gutachten in Auftrag gegeben und dieses an das Arbeitsamt weitergeleitet habe. Das Arbeitsamt schloss daraus, dass die Bürgerin der Arbeitsvermittlung nicht mehr zur Verfügung stehe. Eine Kopie des Gutachtens habe sie nicht vom MDK, sondern vom Arbeitsamt erhalten. Sie habe von der Übermittlung des Gutachtens an das Arbeitsamt durch den MDK nichts gewusst und fühlt sich entmündigt und in ihren Informationsrechten eingeschränkt. Dass sie angeblich zur Arbeitsvermittlung nicht zur Verfügung stehe, habe für sie schwerwiegende negative Folgen gehabt. Die vom MDK getroffenen Feststellungen zu ihrer Leistungsfähigkeit entbehrten jeglicher Grundlage. Sie sei vom MDK weder persönlich untersucht noch in Kenntnis gesetzt worden, dass ein Gutachten über sie erstellt werden solle. Auch im Nachhinein sei sie nicht informiert worden und habe keine Kopie des Gutachtens vom MDK erhalten.

Der *MDK* teilte dazu mit, dass die gutachterliche Stellungnahme im Auftrag der zuständigen Krankenkasse nach Aktenlage erfolgt sei. Die Übermittlung sei angesichts des § 125 Sozialgesetzbuch III (SGB III) erforderlich gewesen, der den Verbleib von arbeitsunfähigen arbeitslosen Personen im Leistungsbezug des Arbeitsamtes regele.

Der vom MDK erwähnte § 125 SGB III betraf nicht das Verfahren, das der MDK hier zu beachten hatte. Vielmehr war auf die Aufgaben des MDK nach § 275 ff. SGB V abzustellen, wonach der MDK die Aufgabe hat, Zweifel an der Arbeitsunfähigkeit eines Versicherten zu klären. Das datenschutzrechtliche Problem bestand darin, dass der MDK ein Gutachten nach Aktenlage gefertigt hatte, ohne den Versicherten von dieser Begutachtung zu informieren. Aus dem Grundsatz der Mitwirkungspflicht nach § 60 SGB I folgt, dass der Patient das Verfahren in jedem Moment steuern und beeinflussen können muss. Der MDK oder auch zuvor die Krankenkasse hätten daher die versicherten Personen von der Beauftragung des Gutachtens nach Aktenlage informieren müssen, auch dann, wenn eine persönliche Untersuchung tatsächlich nicht erforderlich gewesen wäre.

Die öffentliche Rüge

Eine Ärztin beschwerte sich darüber, dass auf einem zustellungsbedürftigen Schreiben der Ärztekammer Berlin auf dem Umschlag anstelle einer Geschäftsnummer der Vermerk „Rüge“ enthalten war. Die Überprüfung bei der Ärztekammer hat tatsächlich ergeben, dass dieser Vermerk beim Ausfüllen der Unterlagen für die Postzustellung erfolgte.

Für die *Zustellung* durch die Post ist die Angabe eines Zuordnungsmerkmals auf dem Umschlag zwingend erforderlich. Die Ärztekammer sicherte zu, anstelle eines inhaltlichen Vermerks künftig ein Aktenzeichen zuzüglich der Angabe der laufenden Nummer und des Jahres zu vermerken. Durch diese Angaben könne kein Rückschluss auf den Inhalt des im Umschlag befindlichen Schreibens gezogen werden.

Die Angabe des Inhaltes eines Schreibens auf dem Zustellungsumschlag ist eine Offenbarung der Daten an den Zusteller oder andere Personen und

widerspricht dem § 9 BlnDSG. Die Angabe des Inhaltes wird in jedem Fall dem Zusteller bekannt, ohne dass dafür eine Erforderlichkeit erkennbar ist.

Gruppentherapie und Arztgeheimnis

In einer Eingabe wurde berichtet, dass in einem Klinikum Gruppentherapien stattfinden, in denen mehrere Patienten zusammensitzen und von ihrer Krankengeschichte und von sich berichten. Wir sollten prüfen, ob es nach dem Datenschutzgesetz richtig ist, eine Therapie „dazu zu missbrauchen", Krankengeschichten unter den Patienten zu offenbaren; es könne nicht ausgeschlossen werden, dass andere Patienten mit dem in der Gruppentherapiesitzung erworbenen Wissen „Unfug trieben".

Die tagesklinische Behandlung beginnt in der Regel mit einem Vorgespräch vor der Aufnahme, in dem mit dem Patienten sein Behandlungsauftrag, der Schwerpunkt der angestrebten Veränderung und die Behandlungsmethoden des Krankenhauses besprochen werden. Als Ergebnis dieses Gespräches wird ein Behandlungsplan in der Krankengeschichte des jeweiligen Patienten dokumentiert. Zur Aufnahme des Patienten in eine *Gruppenpsychotherapie* gehört die Einladung, sich möglichst bald spontan offen in der Diskussion mit Patienten zu beteiligen, seine Gedanken und Gefühle, wie sie innerhalb der Behandlungsstunde aufsteigen, in Worte zu fassen und sich auch auf die Problemlösungsbemühungen seiner Mitpatientinnen/Mitpatienten einzustellen. Bei Suchtpatienten wird regelmäßig eine Darstellung ihrer Problematik in der Gruppe erwartet, da anderenfalls der therapeutische Prozess durch Verleugnung und Verdrängung der Suchtproblematik nicht in Gang kommen kann. Durch diese ausführliche Aufklärung ist sichergestellt, dass sich die Patienten in selbstbestimmter Weise in der Tagesklinik und in der Gruppentherapie einfinden und am gruppentherapeutischen Diskurs teilnehmen. Ein schriftlich erklärtes Schweigeversprechen gibt es nicht, denn es würde nach Auffassung des Klinikums den potenziellen therapeutischen Prozess konterkarieren und Misstrauen fördern. Daher beließe man es bei einem mündlich gegenüber dem Gruppentherapieleiter erklärten Schweigeversprechen durch die Mitpatientinnen/Mitpatienten in der Therapiegruppe. In den gruppentherapeutischen Sitzungen werden keine eigenständigen schriftlichen Gesprächsprotokolle angefertigt. In der Krankengeschichte des jeweiligen Patienten werden ausschließlich seine eigenen Daten nach denselben Regeln dokumentiert wie alle anderen therapierelevanten medizinischen Daten.

Die in der Eingabe erwähnte Missbrauchsabsicht bestätigte sich nicht. Die Offenbarung von Patientendaten durch die Therapieteilnehmer in der Gruppensitzung ist therapeutisch sogar Zweck der Veranstaltung. Nur der Therapeut, nicht aber die „Mitpatienten" stehen berufsrechtlich unter der Schweigepflicht. Hierauf kann sich der Patient auch ohne ausdrückliche Zusicherung verlassen; andererseits ist allen Patienten in einer Therapiegruppe

bekannt, dass sie als Patienten nicht einer gesetzlichen Schweigepflicht unterliegen und somit freiwillig die sie betreffenden Daten zu ihrer Erkrankung in das Gruppengespräch einbringen und den anderen Mitpatienten bekannt geben.

Vom gechipten Hund zum gechipten Menschen – was die RFID-Technologie alles ermöglicht

Die zahlreichen Berliner Hundebesitzer hat im vergangenen Jahr besonders erregt, dass im Rahmen des neuen Hundegesetzes allen Hunden künftig ein Chip implantiert werden soll, mit dessen Daten die Hunde identifizierbar sind. Das Gesetz wurde beschlossen. Dies ist allerdings nur ein Vorbote der Anwendung beim Menschen: Mitte Oktober gingen folgende Meldungen um die Welt: „US-Behörde genehmigt Implantieren von Datenchip" oder „Funk-Chip unter die Haut gespritzt".

Die Technologie, Tiere durch RFID-Chips eindeutig zu kennzeichnen, fand um das Jahr 1990 Einzug in die Arbeit der Tierärzte. Parallel dazu entstanden auf privatrechtlicher Basis drei große Registerstellen, die neben der Nummer des Chips die Daten zum Tier und zum Tierhalter speicherten und somit in der Lage waren, für vermisste Tiere Suchmeldungen insbesondere an die Tierärzteschaft herauszugeben und aufgefundene Tiere einem Tierhalter zuzuordnen. Die Anmeldung bei einem solchen Register ist selbstverständlich dem Tierhalter freigestellt.

Ende September beschloss das Abgeordnetenhaus das Gesetz über das Halten und Führen von Hunden in Berlin. In dieses Gesetz wurde eine Chippflicht für ab 2005 neu angeschaffte Hunde sowie ab 2010 für alle Hunde festgelegt. Parallel dazu besteht für Halter von bestimmten, als gefährlich eingestuften Rassehunden die Pflicht, die Chipnummer an die die Haltung genehmigende Behörde nachzumelden. Des Weiteren ist die Chippflicht als eine mögliche Maßnahme bei anderen durch ihre Gefährlichkeit auffällig gewordenen Hunden festgelegt. Die Chippflicht, so schrieben wir im Jahresbericht 2003[72] läuft jedoch gerade dadurch ins Leere, dass eine wie auch immer geartete zentrale Registratur nicht vorgesehen ist. Da die Chipnummer aber nunmehr nach Erlass des *Hundegesetzes* ein gesetzlich verankertes Kennzeichen ist, muss auch gesetzlich festgelegt werden, wie mit diesem Kennzeichen im Zusammenhang mit den Daten über den Halter und weiteren Daten über den Hund zu verfahren ist. Daher schlugen wir vor, im Hundegesetz festzulegen, wer bei welchen Anlässen die Chipnummer auslesen darf. Dies sind insbesondere: Zwecke der Strafverfolgung, Verfahren zur Erteilung einer Bescheinigung und Plakette für als besonders gefährlich eingestufte Hunde, Verfahren zum Nachweis der Sachkunde sowie die Prüfung von Maßnahmen, wie beispielsweise die angeordnete Tötung eines Tieres

[72] JB 2003, 4.4.2

und die Feststellung der Identität des Hundes bei Ordnungswidrigkeiten. Zu gleichen Zwecken dürfen die Informationen im Halsband über den Namen und die Anschrift des Hundehalters, die sich dort in einer kleinen Schraubkapsel auf einem Zettel zu befinden haben, ausgelesen werden.

Nunmehr steht aber auch die Anwendung der *RFID*-Chip-Technologie beim Menschen ins Haus. Die Food and Drug Administration (*FDA*), die amerikanische Zulassungsbehörde für Medizin und Medizinprodukte, hat die Anwendung derartiger Chips bei Patienten genehmigt. Medizinische Daten dürfen jedoch auf einem derartigen Chip nach der Zulassung der FDA nicht gespeichert werden. Der Code des Chips erlaubt es aber, durch den Arzt auf eine elektronische Patientenakte via Internet zuzugreifen.

In einer Diskothek in Barcelona können sich Stammgäste von einem Arzt einen Chip in den Arm implantieren lassen, der dann als unsichtbare Eintrittskarte und gleichzeitig bargeldloses Zahlungsmittel an der Bar genutzt wird.

In Großbritannien plant man, RFID mit GPS, der satellitengestützten Navigation, die den Aufenthaltsort bis auf wenige Meter genau ermitteln lässt, zu kombinieren, um so Auflagen an Sexualstraftäter zu kontrollieren. Die Anwendungsfelder dieser Kombination sind gegenwärtig kaum abschätzbar, es wurde aber beispielsweise die Idee vorgetragen, demenzkranke oder anderweitig verwirrte Menschen in Alters- bzw. Pflegeheimen mit Hilfe implantierter Chips auffinden zu können und sie somit vor den Folgen ihrer eigenen Verwirrtheit zu schützen. Dann jedoch dürfte der Weg nicht mehr weit sein, Mitarbeiter – sicherlich zunächst erst in sensiblen Bereichen – auf Schritt und Tritt zu kontrollieren oder Alarmfunktionen bei Schülern, die vom vorgegebenen Schulweg abweichen, auszulösen.

4.4.3 Sozial- und Jugendverwaltung

Sozialhilfe und Unterhaltsverzicht

Ein Bürger nahm Anstoß daran, dass das Sozialamt einen Unterhaltsverzicht nicht zur Kenntnis genommen, stattdessen seine geschiedene Ehefrau mit einer Rechtswahrungsanzeige angeschrieben und zugleich auch Sozialdaten von ihm offenbart habe. Er hätte den Unterhaltsverzicht durch Vorlage der entsprechenden Dokumente selbst belegen können; dies sei von ihm jedoch nicht verlangt worden.

Hierzu teilt uns das betroffene Sozialamt mit, dass die *Rechtswahrungsanzeige* nach dem Bundessozialhilfegesetz bereits dann zu versenden sei, wenn eine Unterhaltsverpflichtung nicht von vornherein ausgeschlossen sei (§ 91 Abs. 3 BSHG). Ein Ausschluss sei aber selbst bei einem behaupteten Unterhaltsverzicht nicht regelmäßig gegeben, da der Träger der Sozialhilfe

gehalten ist, die Wirksamkeit des Unterhaltsverzichtes zu prüfen, insbesondere ob der Unterhaltsverzicht wegen Sittenwidrigkeit nichtig sein könne. Hierfür seien die Angaben über die wirtschaftlichen und persönlichen Verhältnisse beider vertragschließenden Eheleute erforderlich. Bereits der Wunsch des durch den Unterhaltsverzicht benachteiligten Ehegatten, eine mögliche Prüfung der Unterhaltspflicht des geschiedenen Ehegatten solle von vornherein nicht stattfinden, könne Anlass für die Überprüfung einer möglichen Sittenwidrigkeit des Unterhaltverzichtes geben. Aus der Regelungssystematik des § 91 Abs. 3 BSHG ist ersichtlich, dass die damit verbundene Offenbarung von Sozialdaten des anderen Ehepartners in Kauf genommen wird. Deshalb war die Übermittlung der Sozialdaten nach § 69 Abs. 1 Nr. 1 Sozialgesetzbuch X (SGB X) i.V.m. § 91 Abs. 3 BSHG zulässig.

Der Streit ums Kindeswohl

Ein Petent sowie seine Frau werden wegen ihrer Kinder durch ein Jugendamt betreut und beraten. Beim Familiengericht ist ein Verfahren anhängig. Dorthin schickte die zuständige Sozialarbeiterin einen Bericht über die persönliche Beurteilung der Sachlage. Er wurde ohne vorherige Zustimmung des Petenten an das Gericht gesandt und diene – so der Petent – vom Inhalt her lediglich dazu, ein „schlechtes Licht" auf ihn zu werfen. Der Petent fragt, ob das Jugendamt befugt sei, anvertraute personenbezogene Daten ohne Einwilligung der Betroffenen an das Familiengericht zu übermitteln.

Die Datenübermittlung an das Gericht war auch ohne ausdrückliche Zustimmung des Betroffenen zulässig, da die Mitarbeiterin damit die gesetzlichen Aufgaben des Jugendamtes erfüllt. Leistungsträger wie das *Jugendamt* sind zwar an das Sozialgeheimnis nach § 35 SGB I gebunden. Eine Übermittlungsbefugnis liegt jedoch vor, wenn es zur Wahrung des Kindeswohls erforderlich ist, diese Daten zu übermitteln. So ist es Aufgabe des Jugendamtes, dem Familiengericht in rechtshängigen Verfahren eine sachverständige sozialpädagogische Stellungnahme abzugeben. Damit soll das Jugendamt dem Gericht ermöglichen, sich einen Einblick in die Familiensituation zu verschaffen. Das Jugendamt muss sich nicht auf bloße Mitteilungen von Tatsachen beschränken, zu denen auch zusammenfassende Berichterstattungen über betroffene Familienmitglieder gehören; es hat vielmehr die Tatsachen zu würdigen, dazu Stellung zu nehmen und einen bestimmten Vorschlag zu unterbreiten. Dabei können nach § 65 Abs. 1 SGB VIII auch in der Beratung anvertraute Sozialdaten weitergegeben werden – aber nur dem Vormundschafts- oder dem Familiengericht und nur wenn eine Gefährdung des Kindeswohls zu besorgen ist und ohne diese Mitteilung eine für die Gewährung von Leistungen notwendige gerichtliche Entscheidung nicht ermöglicht werden könnte, oder wenn eine der in § 203 StGB Abs. 1 oder 3 StGB genannten Personen dazu befugt wäre.

Ein fremder Besucher

Ein Bürger teilte mit, er habe Besuch von einer Person erhalten, die sich als Abgesandter des Sozialverbandes Deutschland (SoVD) ausgegeben habe; tatsächlich habe es sich jedoch um den Versicherungsvertreter eines großen Unternehmens gehandelt, dessen einziges Ziel der Abschluss von Versicherungsverträgen gewesen sei. Von dem Vertreter sei während des Gespräches eine Akquisitionskarte eingesetzt worden, auf der persönliche Daten des Petenten vermerkt waren (Name, Vorname, Anschrift, Geburtsdatum, SoVD-Mitgliedschaft, Tatsache, dass er Rentner sei). Der Petent fragt, von welcher Stelle des SoVD die Versicherung seine Daten erhalten habe, und bittet um Prüfung, ob weitere Angaben weitergegeben wurden.

Die Überprüfung beim Sozialverband ergab, dass der Petent eine Beitrittserklärung unterzeichnet hatte, in der es hieß:

„Der Sozialverband Deutschland hat für seine Mitglieder einen *Gruppenversicherungsvertrag* abgeschlossen. Um die Vergünstigungen des Gruppenversicherungsvertrages zu erhalten, bin ich damit einverstanden, dass hierfür mein Name und die Anschrift an den Versicherer weitergegeben werden."

Der Petent hatte dies mit „Ja" angekreuzt und somit sein Einverständnis zur Weiterleitung seiner Anschrift an „den Versicherer" erklärt. In § 7 Ziff. 2 der Satzung des Sozialverbandes Deutschland e. V. heißt es: „Die nicht geschützten personenbezogenen Daten der Mitglieder können vom RB an Dritte übermittelt werden, soweit es für Zwecke und Ziele dieser Satzung erforderlich ist und soweit das Mitglied nicht widerspricht."

Die Übermittlung personenbezogener Daten ist nach § 7 Ziff. 2 der Satzung zulässig, soweit es dem Satzungszweck dient oder zur Verfolgung der Ziele des Vereins erforderlich ist. Nach § 3 der Satzung des Sozialverbandes besteht sein Zweck darin, gemeinnützig tätig zu werden.

Bei der Weitergabe der Anschriften an den Gruppenversicherer kann es sich um eine gemeinnützige Maßnahme handeln, wenn die Gruppenverträge günstiger gestaltet werden. Dann ist die Datenübermittlung auch vom Vereinszweck gedeckt. Nach § 28 Abs. 3 Ziff. 3 BDSG können zum Zwecke der Werbung Daten, die sich auf die dort genannten Kriterien beschränken, übermittelt und genutzt werden, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat.

Schutzwürdig wäre ein Mitglied, das die Weitergabe der Daten an einen Gruppenversicherer ausdrücklich durch Ankreuzen mit „Nein" verboten hätte. Durch das Ankreuzen des Vermerks „Ja" kann jedoch hier davon ausgegangen werden, dass es im Interesse des Mitglieds liegt, die Vergünstigungen eines Gruppenversicherungsvertrages zu erhalten.

Der Petent trug vor, dass nicht nur die Anschrift, sondern auch sein Geburtsdatum und der Umstand, dass er Rentner sei, weitergeleitet worden

sei. Die Weitergabe dieser Daten war durch die vertragliche Einverständniserklärung nicht gedeckt. Der Sozialverband Deutschland musste deshalb dafür Sorge tragen, dass diese Daten zurückgeholt bzw. gelöscht werden und künftig solche Daten nicht ohne Zustimmung der Mitglieder weitergeleitet werden.

4.4.4 Bauen, Wohnen und Umwelt

Neufassung der Bauordnung für Berlin

Bereits in unserem Jahresbericht 1995[73] *haben wir darüber berichtet, dass der datenschutzgerechte Umgang mit personenbezogenen Daten in den Bauakten nach der bestehenden Rechtslage sehr problematisch ist. Insbesondere der Zugriff auf die Bauakten durch andere Behörden, aber auch durch private Dritte (z. B. Nachfolger des Bauherrn, Alteigentümer, Forscher), ist unzulänglich geregelt. Wir hatten bereits damals vorgeschlagen, die Bauordnung um normenklare gesetzliche Regelungen zur Verarbeitung personenbezogener Daten in Bauakten zu ergänzen.*

Der Gesetzentwurf für eine Neufassung der *Bauordnung* greift diese Empfehlung nunmehr auf und regelt in § 59 die Verarbeitung von personenbezogenen Daten im Bauaufsichtsverfahren.

Die Verarbeitung personenbezogener Daten der nach den §§ 54 – 57 am Bau verantwortlich Beteiligten, der Grundstückseigentümer, der Nachbarn, der Baustoffproduzenten, der Nutzungsberechtigten und der sonstigen am Verfahren zu Beteiligenden durch die Bauaufsichtsbehörden wird in § 59 Abs. 1 des Entwurfes umfassend und normenklar geregelt. Die zulässige Datenverarbeitung ist auf die Daten beschränkt, die zur Wahrnehmung der Aufgabenerfüllung der Bauaufsichtsbehörde (§ 58 des Entwurfes), zur Führung des Baulastenverzeichnisses (§ 82 des Entwurfes) sowie zur Verfolgung von Ordnungswidrigkeiten (§ 83 des Entwurfes) erforderlich sind. Darüber hinaus dürfen Daten nur mit Einwilligung des Betroffenen (§ 59 Abs. 1 Satz 2 des Entwurfes) verarbeitet werden.

Zum Schutz der Betroffenen ist in § 59 Abs. 2 des Entwurfes bestimmt, dass die Daten grundsätzlich nur bei diesen mit deren Kenntnis erhoben werden dürfen. Nur im Ausnahmefall dürfen die Daten bei Dritten ohne Kenntnis des Betroffenen erhoben werden, wenn eine Rechtsvorschrift dies erlaubt, der Betroffene in diese Form der Datenerhebung eingewilligt hat oder anderenfalls die Aufgabenerfüllung der Bauaufsichtsbehörde nach § 58 des Entwurfes gefährdet wäre.

[73] JB 1995, 5.2

Die Probleme, die nach der bestehenden Rechtslage bei der Übermittlung von personenbezogenen Daten aus den Bauakten an Dritte (z. B. Umweltschutz- oder Denkmalschutzbehörden, Nachfolger des Bauherrn, Alteigentümer usw.) bestehen, werden durch die neuen bereichsspezifischen Regelungen in § 59 Abs. 3 und 4 des Entwurfes ausgeräumt. Zukünftig ist normenklar geregelt, dass die Datenübermittlung an die am Bauaufsichtsverfahren beteiligten Behörden, öffentlichen und privaten Stellen und Personen zulässig ist. Darüber hinaus ist – unter den einschränkenden Voraussetzungen in § 59 Abs. 3 Satz 2 des Entwurfes (z. B. sofern es zur Erfüllung der gesetzlichen Aufgaben dieser Behörden oder Stellen erforderlich ist oder ein rechtliches Interesse dargelegt wird) – eine Übermittlung an andere Stellen ebenfalls zulässig. Für regelmäßige Datenübermittlungen im Bauaufsichtsverfahren kann die zuständige Senatsverwaltung eine Rechtsverordnung erlassen (§ 59 Abs. 4 Nr. 2 des Entwurfes).

Damit sind unsere datenschutzrechtlichen Empfehlungen zum großen Teil in den Entwurfstext eingegangen. Leider wurde jedoch unser Vorschlag, auch Regelungen zur Zulässigkeit der Einsichtnahme in die Bauakten durch private Dritte (z. B. die am Bau Beteiligten, Nachbarn, Nutzungsberechtigte, Forscher usw.) in den Entwurf zur Neufassung der Bauordnung aufzunehmen, bislang nicht umgesetzt, die Erörterungen dauern jedoch an.

Wohnungsbauförderung durch Investitionsbank Berlin

Ein Mieter beschwerte sich über seine Hausverwaltung. Diese habe ihn – im Auftrag der Investitionsbank Berlin (IBB) – aufgefordert, in die elektronische Verarbeitung seiner persönlichen Daten einzuwilligen. Der konkrete Zweck und Umfang der Datenverarbeitung seien ihm nicht mitgeteilt worden.

Die IBB begründete diese Maßnahme damit, dass Eigentümer von Wohnraum bei bestimmten Instandsetzungs- oder Modernisierungsmaßnahmen Fördergelder erhalten können. Um mögliche Mietpreiserhöhungen einzugrenzen, würden die Zuschüsse von der IBB nur gewährt, wenn die Eigentümer den modernisierten Wohnraum an Mieter mit WBS vermieten oder vermietet haben. Die WBS-Berechtigung der Mieter sei alle drei Jahre erneut nachzuweisen. Um die Zweckbindung der Fördermittel zu überprüfen, sei es erforderlich, die förderbezogenen Daten – darunter auch der Name des Mieters – zu erheben und zu speichern. Eine Weitergabe dieser Daten durch die IBB an Dritte würde nicht erfolgen.

Nach § 32 Abs. 2 *Wohnungsbauförderungsgesetz* (WoFG) ist die IBB befugt, Daten über die Wohnungen, ihre Nutzung, die Mieter und Vermieter, die Belegungsrechte und die höchstzulässigen Mieten zu erheben, zu verarbeiten und zu nutzen, soweit dies zur Sicherung der Zweckbestimmung der Wohnungen und der sonstigen Bestimmungen der Förderzusage im Rahmen der Wohnraumförderung nach dem WoFG erforderlich ist. Bei den von der

IBB geförderten Modernisierungsmaßnahmen handelt es sich um Maßnahmen zur Durchführung der sozialen Wohnraumförderung nach dem WoFG. Die Speicherung der Mieternamen und deren WBS-Berechtigung ist für die Abrechnung der Fördermittel mit dem Vermieter erforderlich. Diese Mieterdaten können – gestützt auf § 32 Abs. 2 WoFG – von der IBB erhoben und gespeichert werden. Eine Einwilligung der Betroffenen in die Datenerhebung und -speicherung ist nicht erforderlich. Diese sind der IBB nach § 32 Abs. 2 Satz 2 WoFG vielmehr zur Auskunft verpflichtet.

Wir haben der IBB empfohlen, die Betroffenen (Mieter) zukünftig in geeigneter Weise über den Zweck der Datenerhebung und -speicherung und den Umfang der gesetzlichen Auskunftspflicht (§ 32 Abs. 2 Satz 2 WoFG) zu informieren. Dabei sollten die Betroffenen auch ausdrücklich darauf hingewiesen werden, dass sie die beizubringenden Unterlagen und Angaben direkt der IBB – ohne Umweg über den Vermieter – zuleiten können.

Datenübermittlung durch Vermieter an das Sozialamt

Von der Senatsverwaltung für Gesundheit, Soziales und Verbraucherschutz wurden wir darüber informiert, dass eine Arbeitsgruppe zum Thema „Prävention in der Wohnungslosenhilfe“ gebildet worden sei. Diese würde sich mit der Frage beschäftigen, ob es datenschutzrechtlich zulässig sei, dass Vermieter das Sozialamt spontan und frühzeitig – z. B. durch Übersendung einer Kopie des Kündigungsschreibens – über bestehende Mietschulden eines Mieters informieren.

Es gibt keine Rechtsvorschrift, die diese Datenübermittlung erlaubt. Derartige Spontanübermittlungen von Kündigungsschreiben durch den *Vermieter* an das Sozialamt sind – ohne vorherige Anfrage des Sozialamtes – nur mit Einwilligung des Mieters zulässig.

Zu welchem Zeitpunkt diese Einwilligung eingeholt wird, ist – außer dass dies in jedem Fall im Vorfeld der Datenübermittlung zu erfolgen hat – nicht geregelt. Insofern ist es möglich, sie bereits zu einem Zeitpunkt einzuholen (z. B. zu Beginn des Vertragsverhältnisses), an dem die vertraglichen Beziehungen zwischen Mieter und Vermieter noch nicht durch Mietzahlungsrückstände belastet sind. Zu beachten ist dabei jedoch, dass die Einwilligung nach § 4 a Abs. 1 BDSG nur wirksam ist, wenn sie auf der freien Entscheidung des Betroffenen beruht. In keinem Fall darf die Abgabe einer derartigen Einwilligung des Wohnraumbewerbers daher als Voraussetzung für den Vertragsabschluss vom Vermieter verlangt werden. Dies würde die freie Entscheidung des Mietbewerbers beeinflussen und seine Erklärung wäre mangels Freiwilligkeit ungültig.

Viele der betroffenen Mieter sind – nach Auskunft der Wohnungswirtschaft – nicht bereit bzw. nicht in der Lage, sich konstruktiv an der Lösung ihres (Miet-)Schuldenproblems zu beteiligen. Eine Einwilligung in die

Datenübermittlung durch den Vermieter an das Sozialamt ist von diesen Mietern grundsätzlich nicht zu erwarten.

Um diesen Mietern – im Auftrag des Vermieters – eine private Schuldnerberatung anzubieten, kann die datenschutzrechtliche Möglichkeit der Datenverarbeitung im Auftrag nach § 11 BDSG genutzt werden. Werden bei der Auftragsdatenverarbeitung vom Auftraggeber (z. B. einem Wohnungsunternehmen) Daten an den Auftragnehmer (z. B. eine private Schuldnerberatung) weitergegeben, handelt es sich nicht um eine Datenübermittlung im Sinne des § 3 Abs. 4 Nr. 3 a) BDSG. Die Datenweitergabe an den Auftragnehmer kann daher – im engen Rahmen des Auftragsverhältnisses – ohne Einwilligung des Betroffenen erfolgen.

Für die Ansprache der betroffenen Mieter und die Unterbreitung eines Beratungsangebotes zur Entschuldung ist es ausreichend, dass der Auftraggeber (das Wohnungsunternehmen) dem Auftragnehmer (die private Schuldnerberatung) den Namen und die Anschrift des Betroffenen bekannt gibt. Nur diese Daten sind für die Angebotsunterbreitung erforderlich und dürfen im Rahmen der Auftragsdatenverarbeitung weitergegeben werden. Eine Weitergabe weiterer Mieterdaten (z. B. über die konkrete Mietkontensituation) ist für den genannten Zweck nicht erforderlich. Diese Daten dürfen vom Vermieter – z. B. zur Durchführung einer konkreten Einzelberatung – nur mit Einwilligung der betroffenen Mieter an Dritte übermittelt werden.

Einladung zur Kaffeefahrt

Bewohner eines Seniorenheimes hatten sich darüber beschwert, dass dort beschäftigte Mitarbeiterinnen eine „Bewohnerliste" mit Angaben zu Namen, Vornamen, genauem Wohnsitz und Telefonnummer der Bewohner ohne deren Einwilligung an einen außenstehenden Gewerbetreibenden für Zwecke der Werbung für Kaffeeveranstaltungen weitergegeben haben.

Bei der Übersendung der „Bewohnerliste" durch die Mitarbeiterinnen des *Seniorenheimes* an den Veranstalter von Kaffeefahrten ist von einem schutzwürdigen Interesse der Bewohner am Ausschluss der Übermittlung auszugehen. Diese waren bei der Erhebung der Daten zur Erstellung der „Bewohnerliste" vom Betreiber des Seniorenheimes nicht über die Kategorien von Empfängern dieser Daten informiert worden. Dies ist jedoch nach § 4 Abs. 3 Nr. 3 BDSG dann erforderlich, wenn der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an einen Empfänger rechnen muss. Die Bewohner eines Seniorenheimes müssen in keinem Fall damit rechnen, dass die in der „Bewohnerliste" enthaltenen Daten zu Werbezwecken an einen Gewerbetreibenden für die Durchführung von Kaffeefahrten übermittelt werden. Die Übermittlung der „Bewohnerliste" an den Veranstalter der Kaffeeveranstaltung war unzulässig.

Veröffentlichung der Auswertung von Mobilfunkmessungen

Von der Senatsverwaltung für Stadtentwicklung wurden wir gebeten zu prüfen, ob es datenschutzrechtlich zulässig ist, die Auswertungen von Mobilfunkmessungen, die im Auftrag von Mobilfunkbetreibern unter Beteiligung der Senatsverwaltung und in Abstimmung mit den Umweltämtern in den Bezirksämtern durchgeführt worden waren, im Internet zu veröffentlichen und an Dritte (z. B. nichtbeteiligte Umweltämter) zu übermitteln.

Zunächst stellten wir fest, dass die uns vorgelegte Dokumentation der Untersuchungsergebnisse des Messprojekts Daten (z. B. Namen, Adressen, Lagepläne und Fotografien von den Messpunkten) enthielt, bei denen – unter Verwendung von zugänglichem Zusatzwissen – die Identität der Betroffenen (z. B. des Mieters, Grundstücks- oder Wohnungseigentümers oder des Beschwerdeführers) feststellbar war. Als zugänglich ist dabei alles anzusehen, was rechtmäßig feststellbar ist (z. B. durch eine Grundbuchanfrage, Besichtigung des angegebenen (Adresse) Gebäudes) und nach sozialüblichen Maßnahmen nicht ausgeschlossen werden kann.

Um die personenbeziehbaren Untersuchungsergebnisse im Internet zu veröffentlichen, ist es erforderlich, die Daten auf einem Server zum Abruf bereitzuhalten. Dabei handelt es sich um eine Übermittlung von personenbezogenen Daten an Dritte nach § 4 Abs. 2 Nr. 4 BlnDSG. Diese Datenübermittlung kann im vorliegenden Fall auf keine Rechtsgrundlage gestützt werden.

Eine Veröffentlichung der Untersuchungsergebnisse im Internet kann aus datenschutzrechtlicher Sicht daher nur erfolgen, wenn die Betroffenen darin eingewilligt haben oder die personenbezogenen Daten zuvor anonymisiert werden.

Die datenschutzrechtliche Zulässigkeit einer Übermittlung der nichtanonymisierten Fassung der Untersuchungsergebnisse an öffentliche Stellen richtet sich nach § 12 BlnDSG. Werden die Ergebnisse der *Mobilfunkmessungen* mit den genannten personenbezogenen Daten z. B. von anderen Umweltämtern zur Erfüllung des gleichen Zweckes benötigt, zu dem die Daten von der Senatsverwaltung erhoben worden sind, kann die Senatsverwaltung die Daten an die Umweltämter (oder andere Behörden oder öffentliche Stellen) nach § 12 Abs. 1 Satz 2 BlnDSG übermitteln, wenn die Datenübermittlung zur rechtmäßigen Aufgabenerfüllung der Senatsverwaltung oder der Behörde oder der öffentlichen Stelle erforderlich ist.

Die Überwachung einer nicht vorhandenen Heizöltankanlage

Ein Petent beschwerte sich darüber, dass er von einem Umweltamt als Betreiber einer Heizöltankanlage geführt werde, obwohl diese Anlage überhaupt nicht mehr vorhanden sei.

Das Umweltamt bestätigte, dass der Petent in der elektronischen *Anlagenüberwachungsdatei* nach § 23 Berliner *Wassergesetz* (BWG) geführt wird. Das Bundesvermögensamt Berlin habe zwar bestätigt, dass das Haus, in dem der Petent lebt, bereits im Jahr 1981 von Ölfeuerung auf Gasheizung umgestellt worden sei. Einen Nachweis über die Verschrottung des *Heizöltanks* gebe es laut Mitteilung des Bundesamtes jedoch nicht. Insofern werde der das Grundstück betreffende Datenbestand auch zukünftig in der Datei mit der Anmerkung „Stilllegung" geführt.

Die Zulässigkeit der Verarbeitung personenbezogener Daten im Anzeigeverfahren nach § 23 BWG richtet sich nach § 113 c BWG. Danach ist die zuständige Behörde berechtigt, soweit dies für die Durchführung von Anzeigeverfahren nach dem Berliner Wassergesetz oder der Verordnung über Anlagen zum Umgang mit wassergefährdenden Stoffen und über Fachbetriebe (VAWS) erforderlich ist, personenbezogene Daten zu erheben und in sonstiger Weise zu verarbeiten (§ 113 c Abs. 1 Satz 5, 1 BWG). Zu den von der Erlaubnis erfassten personenbezogenen Daten zählen Name und Anschrift der zu beteiligenden Personen (§ 113 c Abs. 1 Nr. 5 BWG) sowie Lage, Größe und Nutzungsart des Grundstücks, auf dem sich die Anlage befindet (Nr. 3). Insofern ist die Behörde berechtigt, Daten zum Grundstück, Eigentümer und Betreiber der Anlage zu verarbeiten, da dies für die Anmeldeverfahren nach § 23 BWG und das Prüfverfahren nach § 23 VAWS erforderlich ist.

Unabhängig davon stieß die fortgesetzte Speicherung der Daten zur Person des Petenten im vorliegenden Fall auf datenschutzrechtliche Bedenken. Das Umweltamt hat ein berechtigtes Interesse daran festzustellen, dass der auf dem fraglichen Grundstück befindliche Tank rückstandslos beseitigt wurde. Dies hätte z. B. durch eine Ortsbesichtigung bestätigt werden können. Allein aus der Tatsache, dass das Bundesvermögensamt Berlin keinen Nachweis über die Verschrottung des Heizöltanks erbringen konnte, lässt sich jedoch kein dauerhaftes Speicherungsrecht des Umweltamtes ableiten.

Nachdem wir das Umweltamt über die Rechtslage informiert hatten, teilte dieses mit, dass der betreffende Datensatz nicht mehr gespeichert wird.

Der Kleingartenverein und seine Mitteilungen am „schwarzen Brett"

Ein ehemaliges Mitglied eines Kleingartenvereins beschwerte sich darüber, dass der Vorstand des Vereins die Öffentlichkeit durch Bekanntmachung am „schwarzen Brett" über die Umstände seines Vereinsaustritts informierte habe. Er und weitere Betroffene, die ebenfalls die Vereinsmitgliedschaft gekündigt hätten, seien namentlich benannt. In dem Aushang werde über die Motivation für die Vereinsaustritte öffentlich spekuliert. Insbesondere werde ausgeführt, dass zwei der Betroffenen damit offensichtlich der „ständigen Kritik des Vorstandes wegen des schlechten Gesamtzustandes ihrer Parzelle aus dem Wege gehen" wollten und dass für die ehemaligen Vereinsmitglieder ein Hausverbot für das Vereinshaus ausgesprochen worden sei.

Der Vorstand der *Kleingartenanlage* bestätigte den Sachverhalt und verwies darauf, dass er gegenüber seinen Mitgliedern nach dem Vereinsrecht eine Informationspflicht habe. Dieser Pflicht folgend habe er die Informationen über den Vereinsaustritt in die Info-Kästen des Vereins eingehängt. Diese Info-Kästen befänden sich auf dem Grundstück, das vom Verein verwaltet werde. Sie waren auch für Nichtvereinsmitglieder zugänglich. Insofern handelte es sich bei dem Aushang nicht nur um eine Übermittlung personenbezogener Daten der Betroffenen an Dritte innerhalb, sondern auch an Dritte außerhalb des Vereins.

Eine Einwilligung der Betroffenen in die Datenübermittlung lag nicht vor. Es bestand kein berechtigtes Interesse des Kleingartenvereins daran, personenbezogene Daten an Dritte, seien es Vereinsmitglieder oder -fremde, zu übermitteln. Insbesondere bestand für den Vereinsvorstand auch keine Informationspflicht nach dem Vereinsrecht. Die Bekanntgabe des Austritts der Betroffenen aus dem Verein war auch nicht zur Wahrung satzungsmäßiger Mitgliedsrechte erforderlich.

Unabhängig davon müssen es die Betroffenen nicht hinnehmen, dass vom Vereinsvorstand öffentlich über ihre Motivlage für den Vereinsaustritt und ihr Verhältnis zum Vorstand spekuliert wird. Die dadurch erzielte Prangerwirkung beeinträchtigte die schutzwürdigen Interessen des Betroffenen erheblich.

Der Vorstand des Kleingartenvereins wurde von uns aufgefordert, weitere Aushänge mit vergleichbarem Inhalt zukünftig zu unterlassen.

4.5 Wissen und Bildung

4.5.1 Wissenschaft und Forschung

Datenschutz im Berliner Hochschulgesetz neu gefasst

Mit der Anpassung des Berliner *Hochschulgesetzes* und des Landesbesoldungsgesetzes an das Bundesgesetz zur Reform der Professorenbesoldung wurden auch die Regelungen des Berliner Hochschulgesetzes zur Verarbeitung personenbezogener Daten neu gefasst[74]. Für bestimmte Zwecke, so die Organisation von Forschung und Studium, die Feststellung der Eignung und

[74] Gesetz zur Umsetzung des Professorenreformgesetzes und zur Änderung hochschulrechtlicher Vorschriften vom 2. Dezember 2004, GVBl., S. 484

Leistung von Hochschulmitgliedern durch Organe, Gremien und Kommissionen oder die Durchführung von Aufgaben der Akademischen Selbstverwaltung fehlten bislang datenschutzrechtliche Regelungen. Die nunmehr vom Abgeordnetenhaus beschlossene Regelung gliedert sich klar in die Erhebung, Speicherung und Nutzung der Daten durch die Hochschule, die Übermittlung und Löschung sowie die Ermächtigung zum Erlass einer Rechtsverordnung und die Satzungs- und Richtlinienkompetenz. Die Vorschriften sind so gefasst, dass sich für den Leser unmittelbar aus diesem Text alle Phasen der Datenverarbeitung erschließen. Damit ist die Neuregelung zwar länger, aber sicherlich für den Nutzer und Rechtsanwender praktikabler. In dieser Datenschutzvorschrift wurden die Erfahrungen der letzten zehn Jahre berücksichtigt. Beispielsweise ist nun explizit die Befugnis zum Datenaustausch zwischen Hochschulen und staatlichen Prüfungsämtern aufgenommen worden. Dies schließt auch ein, dass Prüfungsämter der Hochschule Mitteilungen über die Prüfungsbelastung von Hochschullehrerinnen und Hochschullehrern übermitteln dürfen. Bislang erfuhr die Hochschule nur wenig über die Prüfungsbelastung ihrer Mitglieder und konnte diesen Aspekt nicht bei der Leistungsbewertung und Mittelvergabe berücksichtigen.

Da die Hochschulen in verstärktem Umfang mit Wissenschafts- und Forschungseinrichtungen kooperieren, die privatrechtlich organisiert sind, war es auch erforderlich, eine Rechtsgrundlage zu schaffen, die die Übermittlung insbesondere auch von Mitarbeiterdaten an privatrechtlich organisierte Wissenschafts- und Forschungseinrichtungen erlaubt. Eine Beschränkung auf Ziele und Zwecke des Berliner Hochschulgesetzes regelt hier die Zweckbindung.

Datenschutzgerechte Forschung

Wie in jedem Jahresbericht wollen wir hier eine Auswahl von *Forschungsprojekten* kurz vorstellen, für die es mit zum Teil erheblichem Beratungsaufwand gelang, einen optimalen Datenzugang für die Forscher zu ermöglichen und zugleich die Rechte der Betroffenen auf informationelle Selbstbestimmung zu wahren.

Von Forschern befragt wurden:

- junge Frauen zu ihrem Sexualverhalten und möglichen Infektionen mit Chlamydia trachomatis sowie sich daraus ergebender möglicher Unfruchtbarkeit,
- Mitglieder von Mietervereinen zur Zufriedenheit über ihre Mieterorganisationen,
- Mieter in einem Milieuschutzgebiet in Friedrichshain-Kreuzberg zur Fortschreibung des Milieuschutzes,

- Schüler zu Suchtmittelkonsum und Mobbing,
- Sexualstraftäter zum soziokulturellen Hintergrund bei Gruppenvergewaltigungen,
- Muslime in europäischen Großstädten zu Lebensweise und Wertestruktur,
- Lehrer zur Neueinführung eines Sprachstandtestes nach Wegfall der Vorklassen in Berlin,
- Schüler, Lehrer und Schulleiter zu gesundheitsfördernden Maßnahmen der Schule,
- Strafgefangene zum Entwicklungsverlauf psychischer Störungen,
- Ärzte zur Effizienz eines elektronischen Arztbriefes unter Nutzung bildgebender Verfahren,
- Schüler in Schulen für Lernbehinderte und in Regelschulen zum Alkoholkonsum,
- Auszubildende und Eltern zur Durchführung einer internationalen Vergleichsstudie von Auszubildenden mit andersgeschlechtlichen Geschwistern und kompletten Eltern,
- Strafgefangene nach selbstschädigendem Verhalten im Strafvollzug, insbesondere Suizidversuchen,
- Pflegeeltern, die auf eine erfolgreiche Erziehung ihrer Pflegekinder verweisen können,
- Gesamtschüler in Schulen unterschiedlicher pädagogischer Ausrichtungen zum Zwecke der Evaluation.

Akteneinsicht nahmen Forscher in

- Auszüge aus dem polizeilichen ISVB zur Untersuchung eines möglichen Zusammenhangs von Intensivtätern mit Sexualverbrechen,
- kriminalpolizeiliche Akten zu Motiven bei Brandstiftung und dem Verhalten nach der Tat,
- Auswertungsbögen der Sprachstandsuntersuchungen „Bärenstark“ zur Erstellung anonymer Statistiken,
- Gefangenenpersonalakten von aus dem Strafvollzug entlassenen Jugendlichen für eine auf 15 Jahre angelegte Vergleichsstudie,
- Auszüge des Bundeszentralregisters, polizeiliche Datensammlungen u. Ä. zum Rückfallverhalten von vor zehn Jahren entlassenen Strafgefangenen (Ergänzungsprojekt der CRIME Studie),

– Daten des gemeinsamen Krebsregisters zur Klärung von Todesursachen infolge des Mannsfelder Kupferbergbaus,

– Unterlagen des Entschädigungsamtes zu den von den Nationalsozialisten selbst verfolgten homosexuellen ehemaligen SS-Mitgliedern,

– Gefangenenpersonalakten zur Evaluation von Vollzugsplänen.

Darüber hinaus wurden Forscher zu folgenden Themen beraten:

– zu einer anthropologischen Untersuchung bezüglich des Wissens und der Identitäten in Anbetracht der soziopolitischen Veränderungen in Deutschland seit der Vereinigung und der Nutzung von Video- und Audioaufnahmen,

– zur Erarbeitung von Verfahren zur flächendeckenden Qualitätssicherung in der Geriatrie,

– zu einer Befragung von 60- bis 105-Jährigen zu einem vermuteten Zusammenhang von Störungen des Gleichgewichtssinns und dem Auftreten von Demenz,

– zu einer Befragung Strafgefangener zu Möglichkeiten der Empathie und der Übernahme von Opferperspektiven,

– zu vergleichenden Untersuchungen des Lese- und Mathematikverständnisses in der ersten und zweiten Klassenstufe (Erweiterungsstudie von ELEMENT),

– zur Durchführung einer anonymisierten Studie unter Nutzung von Behandlungsdaten bei künstlicher Beatmung in Krankenhäusern,

– zur Evaluation eines Gebärdensprachtestes für Gehörlose durch Videoaufnahmen,

– zu einer Befragung von Lehrern über ihre Erfahrungen mit der Montessori-Pädagogik,

– zur Durchführung einer europaweiten Studie zur Auswirkung von Fluglärm auf unmittelbar Betroffene,

– zur Durchführung einer Längsschnitterhebung bei neuen HIV-Infektionen,

– zur Durchführung einer Evaluationsstudie über Verfahrensweise und Nutzen der Rasterfahndung,

– zur anonymisierten Nutzung von Unterlagen einer sozialtherapeutischen Anstalt im Justizvollzug zur anonymisierten Eigenevaluation der erstellten Prognosen.

4.5.2 Statistik

Berlin zählt seine Beamten

Unter dieser etwas grob geratenen Überschrift titelte ein Berliner Boulevardblatt einen Artikel zu dem Ende November unter dem etwas sperrigen Namen „*Personalstrukturstatistikgesetz*“ (PSSG) beschlossenen Statistikgesetz. In den Jahresberichten 2002 und 2003[75] hatten wir über die Grobstruktur des Gesetzentwurfs berichtet. Es war ein längerer Prozess, in dem die technische Machbarkeit, aber vor allem die Möglichkeit geprüft wurde, eine organisatorisch, personell und räumlich abgeschottete Statistikstelle bei der Senatsverwaltung für Finanzen zu bilden. Dabei war sicherzustellen, dass es keine Durchgriffsmöglichkeiten und -rechte auf Personaleinzeldaten durch andere Mitarbeiter der Senatsverwaltung einschließlich des Senators selbst gibt. In den deutschen Statistikgesetzen ist regelmäßig eine Strafvorschrift enthalten, die denjenigen bestraft, der statistische Einzelangaben zur Herstellung eines Personenbezuges nutzt oder sie mit anderen so zusammenführt, dass sich ein solcher ergibt. Wegen der Brisanz der Daten und der langen Speicherungsdauer schlugen wir vor, dass ebenso bestraft werden soll, wer solche Handlungen zur Deanonymisierung anweist oder anderweitig initiiert. Dies wurde im Gesetz berücksichtigt.

Neben diesen rechtlichen und organisatorischen Regelungen zur Abschottung der Statistikstelle wurde erstmals ein Konzept „Datenschutz durch Technik“ in einem Gesetz festgeschrieben. Wenn dieses Konzept umgesetzt ist, dürfte mit der Personalstrukturdatenbank in dieser Statistikstelle ein Niveau der statistischen Aufbereitung bei gleichzeitiger Sicherung der datenschutzrechtlichen Rahmenbedingen erreicht werden, das wenigstens in Deutschland einmalig ist. Auch wenn immer wieder zum Teil neidvoll von Statistikern auf die nordeuropäischen und niederländischen Registerstatistiken geschaut wird, kann die Personalstrukturdatenbank die Möglichkeiten derartiger Register, was die statistische Auswertung betrifft, weit übertreffen, insbesondere da jeder historische Strukturstand wieder erzeugt werden kann. Ausgliederungen aus dem öffentlichen Dienst, Umgruppierungen, Neuzuschnitte von Landesämtern, Senats- oder Bezirksverwaltungen, die in der Vergangenheit immer wieder zu Widersprüchlichkeiten in statistischen Aussagen geführt haben, können dieses System nicht beeinflussen. Gleichzeitig hat der Gesetzgeber beschlossen, dass dem Datenschutz durch ein mehrstufiges Verfahren der Pseudonymisierung und nachfolgend nur beschränkte Sichten auf die Einzeldaten bei der Plausibilisierung sowie durch inhaltliche Restriktionen, die einer beliebigen Kombinierbarkeit Grenzen setzen, Rechnung getragen wird. Die statistische Auswertbarkeit der

[75] Gesetz über die Statistik der Personalstruktur und der Personalkosten im unmittelbaren Landesdienst vom 2. Dezember 2004, BGBl. I, S. 490; JB 2002, 4.5.3; JB 2003, 4.5.2

Daten wird dadurch nicht beeinflusst, aber wollte man beispielsweise nach einzelnen Mitarbeitern suchen, die bestimmte Merkmalskombinationen aufweisen, lässt diese technische Lösung das nicht zu. Dies wird dadurch erreicht, dass jeweils nur zwei der sieben Teile des Datensatzes untereinander kombiniert werden dürfen.

Einer (oder einige) für alle – wirtschaftlichere Lösungen für die Bundesstatistik und Service für die Forschung

Im Jahresbericht 2003[76] informierten wir über unsere Rechtsauffassung, dass die Errichtung eines gemeinsamen *Forschungsdatenzentrums der statistischen Landesämter* eine explizite Befugnisnorm im Bundesstatistikgesetz voraussetzt. Rechtlich ist es nicht zulässig und schon gar nicht als Auftragsdatenverarbeitung zu fassen, wenn ein statistisches Landesamt die Daten der übrigen 15 Landesämter mit vorhält, auf Plausibilität prüft und nach den Wünschen von Wissenschaftlern für konkrete Forschungsvorhaben aufbereitet sowie dabei die statistische Geheimhaltung sichert. Dies sind hoheitliche Aufgaben der Statistik, die durch Auftragsdatenverarbeitung nicht übertragen werden können. Ein ähnlicher Ansatz wurde in einer Analyse der Rechnungshöfe des Bundes und der Länder zur Wirtschaftlichkeit des öffentlichen Statistikwesens in Deutschland vom November 2002 für die Organisation der gesamten Bundesstatistik gegeben. Die statistischen Landesämter nahmen diese Anregungen ernst und schlugen vor, eine Bündelung von Aufgaben für Information und Kommunikation nach dem Prinzip „Einer (oder einige) für alle“ anzustreben und dafür eine Rahmenvereinbarung zwischen den Landesämtern abzuschließen. Eine solche Rahmenvereinbarung stellt jedoch keine die Amtliche Statistik legitimierende Rechtsvorschrift dar, wie dies beispielsweise durch das Bundesstatistikgesetz oder Staatsverträge gegeben wäre. Nach dem energischen Widerspruch der Datenschutzbeauftragten in Bund und Ländern erarbeitete unsere Behörde gemeinsam mit dem Statistischen Landesamt einen Regelungsvorschlag, um zunächst die Arbeit von Forschungsdatenzentren rechtlich durch eine Änderung des Bundesstatistikgesetzes zu legitimieren. Diese Anregung wurde vom Bundesinnenministerium aufgegriffen, aber noch nicht in einen Gesetzentwurf der Bundesregierung zur Änderung des Statistikregistergesetzes und anderer Gesetze im Zusammenhang mit der Änderung der Handwerksordnung (Wegfall der Zulassungspflicht für 53 Gewerbe) mit aufgenommen. Der Vorschlag zur Änderung des Bundesstatistikgesetzes für diese Zwecke ist vom Bundesrat aufgegriffen und am 17. Dezember 2004 beschlossen worden[77].

[76] JB 2003, 4.5.2

[77] BR-Drs. 878/04

Vertiefte Kooperation oder Fusion der statistischen Landesämter Berlin und Brandenburg

Ende des Jahres 2003 war in der Presse eine nahezu unscheinbare Randnotiz zu finden, dass sowohl der Senat von Berlin als auch die Brandenburger Landesregierung beschlossen haben, eine vertiefte Kooperation der *statistischen Landesämter* oder möglicherweise sogar eine Fusion zu prüfen. Im Frühjahr nahm eine gemeinsame Projektgruppe der Innenverwaltungen und statistischen Landesämter mit fünf Untergruppen ihre Tätigkeit auf. Kontinuierlich wurden wir über den Fortgang der Arbeiten informiert und im September lag der erste Entwurf für einen Staatsvertrag mit dem Ziel der Fusion der Landesämter und der Bildung einer gemeinsamen Anstalt des öffentlichen Rechts vor. In der Tätigkeit der Projektgruppe wurde jedoch das ursprünglich mit anvisierte Ziel der vertieften Kooperation zunächst nicht in dem Umfang analysiert wie die Voraussetzungen und Konsequenzen einer Fusion. Anfang des Jahres 2005 soll der Abschlussbericht vorliegen, so dass wir dann detailliert prüfen können, ob die datenschutzrechtlichen Rahmenbedingungen im Entwurf des Staatsvertrages hinreichend Berücksichtigung gefunden haben.

4.5.3 Schule

Umsetzung des neuen Schulgesetzes

Nachdem im Januar vom Abgeordnetenhaus das neue Berliner *Schulgesetz*[78] beschlossen wurde, setzte die Senatsverwaltung für Bildung, Jugend und Sport sofort alles daran, die wichtigsten Regelungen durch Rechtsverordnungen und Ausführungsvorschriften umzusetzen, so dass eine Reihe von Veränderungen schon zum Beginn des Schuljahres 2004/2005 wirksam werden konnten. Dies sind insbesondere die Grundschulverordnung, die Verordnung über die Schularten und Bildungsgänge der Sekundarstufe I und die Sonderpädagogikverordnung. Die Überarbeitung der Schuldatenverordnung wurde zeitlich zurückgestellt, weil zunächst die inhaltlichen Veränderungen aufgrund des neuen Schulgesetzes in den einzelnen Rechtsverordnungen festgelegt werden müssen. Erst dann können entsprechende Präzisierungen und Ergänzungen in der Schuldatenverordnung vorgenommen werden.

Mit Beginn des Schuljahres 2004/2005 wurde eine Ausführungsvorschrift zur internen Evaluation an Schulen erlassen. Die interne Evaluation beinhaltet nach § 9 des Schulgesetzes schul- und schulartübergreifende Vergleiche sowie zentrale Schulleistungsuntersuchungen, aber auch Befragungen und

[78] GVBl. 2004, S. 26

Datenerhebungen nach den Methoden der empirischen Sozialforschung. Wir begrüßten es daher, dass die Senatsverwaltung für Bildung, Jugend und Sport in diesem Schuljahr für jede der Berliner Schulen zwei Lehrer als Schulevaluatoren fortbildet. An den Pilotschulungen haben wir uns beteiligt und auf Besonderheiten, insbesondere die datenschutzrechtlichen Rahmenbedingungen bei der Nutzung von Methoden der empirischen Sozialforschung (Lehrer-, Schüler-, Elternbefragungen), hingewiesen und klargelegt, dass nur ein hohes Maß an Anonymisierung bei den Befragungen Voraussetzung für richtige und ehrliche Ergebnisse sein kann.

Das Ende der Lernmittelfreiheit – der zweite Fehlversuch

Im Jahresbericht 2003 erläuterten wir die Endes des Schuljahres 2002/2003 aufgetretenen Probleme bei der Umsetzung der *Lernmittelverordnung*[79]. Wir regten ein Gutscheinsystem an, bei dem für die Schule weder die Art der Sozialleistung noch das leistungsgewährende Amt ersichtlich sein sollte und die Eltern vom Eigenanteil zur Finanzierung der Lernmittel befreit werden können. Der Vorschlag wurde von der Senatsverwaltung für Bildung, Jugend und Sport aufgegriffen, allerdings erst mit einem erheblichen Zeitverzug, so dass der Entwurf für diesen „Gutschein“ uns erst Anfang März 2004 vorgelegt wurde. Zunächst gingen wir davon aus, dass diese Bescheinigungen von den leistungsgewährenden Ämtern ausgegeben werden. Da der Druck der Bescheinigungen so spät erfolgte, wurden sie unmittelbar an die Schulen ausgeliefert. Dies führte zu erheblicher Verwirrung und zur Verärgerung auf Seiten der Schule und insbesondere auch der Eltern. Eine Reihe von Eltern hatte vor Auslieferung der Bescheinigungen Ende April/Anfang Mai bereits Unterlagen eingereicht, die ihre Befreiung dokumentieren. Nunmehr wurden sie von den Schulen aufgefordert, mit dem Vordruck nochmals zu den entsprechenden Ämtern zu gehen und diese stempeln zu lassen. Als wir davon erfuhren, teilten wir Ende Mai diesen Schulen mit, dass eine nochmalige Erhebung der Daten aufgrund der Vordrucke nicht erforderlich und damit nicht zulässig sei. Hinzu kam, dass insbesondere Wohngeldstellen sich weigerten, die entsprechenden Vordrucke zu stempeln. Die Ursache dafür war der Senatsverwaltung für Bildung, Jugend und Sport bereits seit Juni 2003 bekannt, wir erfuhren davon jedoch erst durch ein Berliner Bezirksamt. Die Ursache lag darin, dass die Wohngeldbescheide nicht mehr auf einer Papierakte basieren, sondern ausschließlich elektronisch erstellt werden. Aufgrund der vielen Anrufe und Anfragen, die bei uns eingingen, konnten wir den Eltern lediglich empfehlen, wie im Vorjahr wieder die Originale der Wohngeldbescheide bei den Schulen vorzulegen. Zum Ende des alten Schuljahres und zum Beginn des Schuljahres 2004/2005 versandten wir an ca. 300 Schulen Informationsschreiben. Dabei mussten wir auch feststellen, dass die Senatsverwaltung für Bildung, Jugend

[79] JB 2003, 4.5.3

und Sport über keinen aktuellen Fax- oder E-Mail-Verteiler der Berliner Schulen verfügt, der eine unmittelbare, schnelle und weitgehend automatisierte Information der einzelnen Schulen erlaubt. Nur dank der Flexibilität der Berliner Schulleiter konnten bis Ende September die Daten für die Befreiungen vom Eigenanteil erhoben und entsprechend gehändelt werden.

4.6 Wirtschaft

4.6.1 Banken

Girokonto für Jedermann

Der Zentrale Kreditausschuss (ZKA) hat sich in einer Empfehlung im Jahr 1995 dafür ausgesprochen, dass jedem Bürger – unabhängig von seiner wirtschaftlichen Situation – ein Girokonto auf Guthabenbasis zur Verfügung gestellt wird. Von diesem Grundsatz sollte nur abgewichen werden, wenn dem Betroffenen bestimmte Verfehlungen zur Last gelegt werden, wie etwa Betrug, Geldwäsche, Belästigung oder Gefährdung von Kunden und Mitarbeitern. Demgegenüber ist ein Negativeintrag bei der SCHUFA kein Grund, das „Girokonto für Jedermann“ nicht zu gewähren. Trotzdem holen die Banken beim Antrag auf Eröffnung eines „Girokontos für Jedermann“ eine SCHUFA-Auskunft über den Betroffenen ein.

Die Gewährung von *Guthabenkonten* für sozial Schwache ist für die Banken wirtschaftlich unattraktiv. Durch die SCHUFA-Auskunft können sie feststellen, ob der Antragsteller tatsächlich über kein Girokonto verfügt und somit Anspruchsberechtigter der Selbstverpflichtung des ZKA ist. Da Banken beim Guthabenkonto kein Ausfallrisiko tragen und der von der SCHUFA zur Verfügung gestellte Datensatz neben der Information, ob der Betroffene ein Girokonto besitzt oder nicht, noch zahlreiche andere (Bonitäts-) Daten enthält, fehlt den Banken für die SCHUFA-Abfrage das berechtigte Interesse.

Dieses Problem umgehen die Banken dadurch, dass sie kein Produkt „Guthabenkonto für Jedermann“ zur Verfügung stellen. Sie würden nach einer Analyse der SCHUFA-Auskunft in jedem Einzelfall prüfen, ob dem Betroffenen ein normales Girokonto zur Verfügung gestellt werden kann, dies auch dann, wenn der Betroffene ausdrücklich ein Girokonto unter Hinweis auf die ZKA-Empfehlung beantragt hat.

Die Einlassung der Banken kann nur dann überzeugen, wenn die Banken tatsächlich nach der Analyse der SCHUFA-Auskunft Personen mit Negativeintrag unter bestimmten Bedingungen ein normales Girokonto gewähren. Ob dies tatsächlich der Fall ist, wird zu untersuchen sein.

Zusendung des Bankmagazins

Eine Bank versandte ihr Kundenmagazin in einer Klarsichtfolie. Auf der Außenseite des Magazins befand sich nicht nur der Name und die Anschrift des Kunden, sondern auch seine um die letzte Ziffer reduzierte Kontonummer. Diese Zahl konnte bei einer Kundin nicht nur der Postbote, sondern auch die Nachbarn sehen, da das Magazin aus dem Briefkastenschlitz herausragte.

Die Bank hat eingeräumt, dass die um eine Ziffer reduzierte Kontonummer versehentlich auf das Adressfeld gelangt ist. Die Bank hat den Adressaufdruck und den Vertrieb des Magazins durch einen Dienstleister erledigen lassen; ihm hat die Bank versehentlich nicht nur die Adressdaten, sondern auch die reduzierte Kontonummer zugeleitet. Der Dienstleister ging dann davon aus, dass die Nummer auch in das Adressfeld des Magazins aufgenommen werden sollte. Die Bank hat zugesagt, dass sich zukünftig ein derartiger Fehler nicht wiederholt.

Die Versendung von *Magazinen* in einer Klarsichthülle ist in der Bankenbranche üblich. Aus der Zusendung eines Magazins ergibt sich, dass der Adressat Kunde einer bestimmten Bank ist. Diese Information erhält nicht nur der Postbote, sondern auch die Nachbarn, wenn das Magazin wie im vorliegenden Fall aus dem Briefkastenschlitz herausragt. Datenschutzfreundlicher wäre deshalb die verschlossene Versendung von Bankmagazinen, entsprechende Empfehlungen wurden aber bisher von den Banken aus Kostengründen abgelehnt.

Drohung mit der SCHUFA

Ein Kreditkarteninhaber weigerte sich, sein Kreditkartenkonto auszugleichen, da die spanische Akzeptanzstelle seine Unterschrift durch die Verabreichung von Drogen erschlichen habe. Dies habe er der Bank umgehend mitgeteilt. Trotzdem forderte die Bank ihren Kunden auf, den Fehlbetrag umgehend zu überweisen. Für den Fall der Nicht-Überweisung drohte sie: „Ferner wird die Kündigung der SCHUFA gemeldet. Dies kann für Sie zur Folge haben, dass Sie für einen längeren Zeitraum bei den der SCHUFA angeschlossenen deutschen Kreditinstituten keine Kredite erhalten und möglicherweise sogar keine neuen Konten eröffnen können. Bitte bedenken Sie diese Folgewirkungen."

Als Unternehmer hätte für den Kreditkarteninhaber die Einmeldung eines Negativdatums bei der SCHUFA das wirtschaftliche Aus bedeutet. Dabei wollte er die Forderung im Fall einer gerichtlichen Niederlage sofort begleichen.

Es kommt nicht selten vor, dass die Einmeldung von Negativdaten an die *SCHUFA* als Druckmittel verwendet wird, um den (vermeintlichen) Schuldner zur sofortigen Zahlung zu bewegen und ein möglicherweise langwieriges Gerichtsverfahren zu vermeiden. An die SCHUFA dürfen aber nur solche Forderungen als Negativdaten eingemeldet werden, bei denen die Nichtzahlung entweder auf Zahlungsunwilligkeit oder -unfähigkeit beruht. Danach wäre die Einmeldung der Kreditkartenforderung rechtswidrig gewesen. Die unberechtigte Drohung mit der SCHUFA-Einmeldung kann als versuchte Nötigung (§§ 240, 22 StGB) oder sogar als versuchte Erpressung (§§ 253, 22 StGB) gewertet werden.

Die Bank hat ihre Drohung zurückgezogen.

4.6.2 Auskunfteien

Überprüfungsergebnisse

Bei der Überprüfung von zwei Auskunfteien wurden verschiedene Datenschutzverstöße festgestellt.

Die Auskunfteien verwendeten nicht gekennzeichnete *Schätzdaten*[80]. Inzwischen sind sie auf Druck der Aufsichtsbehörden dazu übergegangen, bei Auskünften, die Schätzdaten enthalten, einen allgemeinen Hinweis hierauf zu geben. Auch wenn die Einzelkennzeichnung der Schätzdaten aus datenschutzrechtlicher Sicht vorzuziehen gewesen wäre, ist der jetzt vereinbarte allgemeine Hinweis noch vertretbar. Die Auskunfteien haben anscheinend die Einzelkennzeichnung abgelehnt, da sie die Kunden über den Umfang der Schätzdatenverwendung im Unklaren lassen möchten.

Auskunftsersuchen der Betroffenen über die Empfänger der Daten wurden in der Regel verweigert, da grundsätzlich die Namen ihrer Kunden ein überwiegendes Geschäftsgeheimnis darstellten[81]. Ab September 2004 haben die Auskunfteien ihr Verfahren umgestellt und gewähren nun grundsätzlich Auskunft über den Empfänger der Daten, nur in Ausnahmefällen werden sie sich – entsprechend den Vorgaben des § 34 Abs. 1 Satz 3 BDSG – auf das Vorliegen eines Betriebsgeheimnisses berufen.

Die Auskunfteien haben auch Ärzte und Zahnärzte als Kunden. Gerade bei umfangreichen Behandlungen haben die Angehörigen von Heilberufen ein Interesse daran, bei Privatpatienten eine Bonitätsanfrage zu stellen. Durch die Anfrage bei einer Auskunftei übermittelt der Arzt nicht nur ein sensitives Datum im Sinne des § 3 Abs. 9 BDSG, nämlich die Tatsache, dass ein Betroffener einen bestimmten Arzt aufgesucht hat, die Anfrage stellt auch eine nach § 203 Abs. 1 Nr. 1 StGB strafbewehrte Verletzung von Privatgeheimnissen dar. Wir haben den Auskunfteien empfohlen, die Verpflichteten nach § 203 StGB darauf hinzuweisen, dass sie vor einer Bonitätsabfrage die Einwilligung des Patienten einholen müssen.

[80] JB 2000, 4.6.2

[81] JB 2001, 4.6.3

Im Jahresbericht 2002[82] hatten wir kritisiert, dass die Auskunfteien der Verpflichtung, bei zwei Promille der Auskunftsbegehren das berechtigte Interesse ihrer Kunden zu überprüfen, nur unzureichend nachgekommen sind. Dieser Mangel ist von den Auskunfteien inzwischen behoben worden, die vereinbarte Prüfung findet in ausreichend substanziierter Form statt. In zwei Fällen hätte die Auskunftei allerdings auf eine genauere Begründung des berechtigten Interesses ihres Kunden drängen müssen. Ein Kunde verweigerte unter Berufung auf das Bundesdatenschutzgesetz Informationen, in einem anderen Fall wurde die Informationsverweigerung damit begründet, die Unterlagen seien bereits archiviert, der Aufwand für eine Auskunft sei deshalb zu groß.

Die Kunden der Auskunfteien erhalten auch Bonitätsdaten im Rahmen eines Auswahlverfahrens für neue Mitarbeiter. Hier fehlt dem Arbeitgeber in der Regel das für die Datenermittlung nach § 29 Abs. 2 Nr. 1 a BDSG erforderliche berechtigte Interesse an der Kenntnis der Daten. Ein berechtigtes Interesse besteht für den Arbeitgeber nur dann, wenn eine ausreichende Bonität für den konkreten Arbeitsplatz ausnahmsweise erforderlich ist (z. B. Vermögensverwalter).

Auch Vermieter erhalten von den Auskunfteien unbeschränkte Bonitätsauskünfte. Dies ist bei der Vermietung von Gewerberäumen nicht zu beanstanden. Demgegenüber haben Mieter von privatem Wohnraum ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung von Negativdaten, die aufgrund ihrer Geringfügigkeit keine ausreichende Indizwirkung dafür haben, dass der Mieter seine Mietschuld nicht begleicht (§ 29 Abs. 2 Satz 1 Nr. 2 BDSG).

Ein berechtigtes Interesse an Bonitätsdaten setzt auch voraus, dass es zu einer Verdichtung der Wahrscheinlichkeit von Geschäftskontakten zwischen dem Anfragenden und dem Betroffenen gekommen ist. Bei einer Anfrage über einen potenziellen Geschäftspartner, mit dem bisher noch keine Verhandlungen geführt wurden und der selbst auch kein Interesse an einer Geschäftsbeziehung geäußert hat, fehlt es an einem berechtigten Interesse zur Abfrage von Bonitätsdaten. Dies mussten wir einer der überprüften Auskunfteien aus gegebenem Anlass mitteilen.

SCHUFA-Score

Das *Scoring-Verfahren* der SCHUFA ist schon seit mehreren Jahren in der datenschutzrechtlichen Diskussion[83]. Bisher liegt kein Gerichtsurteil vor, welches sich mit der Frage befasst, ob das Scoring-Verfahren der SCHUFA rechtmäßig ist oder nicht. Das SCHUFA-Verfahren unterscheidet zwischen A- und B-Vertragspartnern. Während A-Vertragspartner sowohl positive als

[82] JB 2002, 4.6.2

[83] JB 1998, 4.6.1; JB 2000, 4.6.2; JB 2002, 4.6.2

auch negative Daten erhalten und liefern, beschränken sich die Datenflüsse zwischen der SCHUFA und den B-Vertragspartnern auf Negativdaten. Da B-Vertragspartner ohne Einwilligungserklärung arbeiten, wäre die Übermittlung von *Positivdaten* mangels Rechtsgrundlage rechtswidrig (§ 4 Abs. 1 BDSG). Bei dem SCHUFA-Score wird mit Hilfe von Positivdaten die Wahrscheinlichkeit eines Negativdatums berechnet. Da der Scoring-Wert auch den B-Vertragpartnern zur Verfügung gestellt wird, erhalten diese über den Umweg des Scoring-Wertes Positivdaten des Betroffenen. Es wäre empfehlenswert, wenn die SCHUFA den Scoring-Wert nur noch an A-Vertragspartner übermitteln würde.

Auch bei der Verwendung des Scoring-Wertes kann es zu datenschutzrechtlichen Problemen kommen. Häufig verwenden Banken den Scoring-Wert der SCHUFA, betreiben aber gleichzeitig ein bankeigenes Scoring-Verfahren, um später anhand beider Werte eine Kreditentscheidung zu treffen oder beide Scoring-Werte zu einem einheitlichen Gesamtscoring-Wert zusammenzuführen. Hierbei besteht die Gefahr, dass ein „statistischer Negativwert“ doppelt negativ berücksichtigt wird. Hierdurch könnten Kreditentscheidungen der Banken negativ beeinflusst werden.

4.6.3 Was wir sonst noch geprüft haben …

Cold call im Call-Center

Die Anzahl der Beschwerden über telefonische Werbung ist im letzten Jahr deutlich gestiegen. Bei der Überprüfung von drei Call-Centern haben wir festgestellt, dass Bürger telefonisch beworben wurden, ohne dass diese darin eingewilligt hatten. Die Werbung erfolgte sowohl durch Call-Center-Mitarbeiter als auch durch Bandansagen. Zwei der drei überprüften Unternehmen hatten sich auf Werbung für die Süddeutsche und Norddeutsche Klassenlotterie bzw. deren Lotterieeinnahmen spezialisiert.

Nach der Novellierung des Gesetzes gegen den unlauteren Wettbewerb (UWG) vom 3. Juli 2004[84] ist die *Telefonwerbung* nunmehr ausdrücklich geregelt. Nach § 7 Abs. 2 Nr. 2 UWG ist eine unzumutbare Belästigung insbesondere anzunehmen bei einer Werbung mit Telefonanrufen gegenüber Verbrauchern ohne deren Einwilligung oder gegenüber sonstigen Marktteilnehmern (wie z. B. Unternehmen) ohne deren zumindest mutmaßliche Einwilligung. Eine Datennutzung unter Verstoß gegen § 7 Abs. 2 Nr. 3 BDSG stellt, sofern eine natürliche Person betroffen ist, gleichzeitig eine rechtswidrige Datennutzung nach Bundesdatenschutzgesetz dar, da die verantwortliche Stelle sich bei der Datennutzung nicht auf ein Gesetz oder eine andere Rechtsvorschrift berufen kann (§ 4 Abs. 1 BDSG). Aufgrund der ein-

[84] BGBl. I, S. 1414

deutigen Rechtslage ist eine Tendenz zu beobachten, dass „seriöse verantwortliche Stellen“ die Telefonwerbung an *Call-Center* outsourcen; sie lassen sich von den Call-Centern zwar bestätigen, dass diese das UWG beachten, dies ist jedoch bei den von den Call-Centern geforderten und gelieferten Fallzahlen nicht möglich.

Die Call-Center beriefen sich darauf, sie würden über Adresslisten von Betroffenen verfügen, die in Telefonwerbung eingewilligt haben. Bei Nachprüfungen hat sich dies allerdings nie bestätigt. Es erscheint auch fraglich, ob die teilweise gegebene Einwilligung in Telefonwerbung im Rahmen von Preisausschreiben oder Konsumentenbefragungen nicht zu unbestimmt ist, um die Vorgaben des § 7 Abs. 2 Nr. 2 UWG zu erfüllen. Gerichtsurteile zu dieser Frage stehen noch aus.

Feindliche Übernahme

Einer Schweizer Aktiengesellschaft, die ihren Aktionären als Dividende Urlaub in unternehmenseigenen Ferienwohnungen gewährt, drohte eine feindliche Übernahme. Eine Berliner „Interessengemeinschaft der Aktionäre“ versuchte, bei der nächsten Hauptversammlung die Mehrheit der Aktionäre hinter sich zu bringen und einen neuen Verwaltungsrat zu installieren. Um dieses Ziel zu erreichen, schrieb die Interessenvereinigung Hunderttausend Aktionäre in Deutschland, Holland und der Schweiz an, um sie davon zu überzeugen, der Interessenvereinigung das Stimmrecht für die Hauptversammlung zu übertragen. Durch eine Neubesetzung des Verwaltungsrates hätte die Interessenvereinigung die vollständige Exekutivgewalt über die Aktiengesellschaft erlangen können. Sie hätte auch die Möglichkeit gehabt, den sehr wertvollen Immobilienbesitz der Aktiengesellschaft zu verkaufen. Der Versuch der feindlichen Übernahme scheiterte.

Anfragen von Aktionären bezüglich der Herkunft der gespeicherten Daten beantwortete die Interessengemeinschaft ebenso wenig wie Löschungsbegehren. Da es nach Schweizer Recht kein allgemein zugängliches Aktionärsverzeichnis gibt, bestand von Anfang an der Verdacht, dass die Interessenvereinigung die *Aktionärsdaten* rechtswidrig erhoben hat. Da die Interessenvereinigung uns gegenüber keine Aussage zur Herkunft der Daten machte, waren wir auf die Ermittlungen der Schweizer Behörden angewiesen. Die Ermittlungen dort sind zwar noch nicht abgeschlossen, man geht aber davon aus, dass ein ehemaliger Mitarbeiter der Aktiengesellschaft die Aktionärsdaten an die Interessenvereinigung verkauft hat. Dies stellt nach deutschem Recht nach § 44 Abs. 1 i.V.m. § 43 Abs. 2 Nr. 3 BDSG einen Straftatbestand dar.

Für die Verarbeitung und Nutzung der durch einen Datendiebstahl erhobenen personenbezogenen Daten der Aktionäre kann sich die Interessenvereinigung auf keine Rechtsvorschrift berufen, die Verarbeitung und Nutzung

dieser Daten ist somit unzulässig (§ 4 Abs. 1 BDSG). Den Aktionären steht gegen die Interessenvereinigung ein Anspruch auf Auskunft über die gespeicherten Daten zu, auch soweit sie sich auf die Herkunft dieser Daten beziehen (§ 34 Abs. 1 Satz 1 Nr. 1 BDSG), sowie ein Löschungsanspruch nach § 35 Abs. 2 Satz 2 Nr. 1 und 3 BDSG. Eine Gruppe von Aktionären hat diese Ansprüche zivilrechtlich eingeklagt, eine Vollstreckung dieser Ansprüche ist allerdings noch nicht erfolgt.

Gegen die Interessenvereinigung wird in der Schweiz und Berlin strafrechtlich ermittelt. Da die Interessenvereinigung und der sie vertretende Rechtsanwalt uns gegenüber bisher keine zur Aufklärung des Sachverhalts dienlichen Auskünfte erteilt haben, haben wir gegen die Interessenvereinigung nach § 43 Abs. 1 Nr. 10 BDSG ein Ordnungswidrigkeitenverfahren eingeleitet.

Glücksspiel im Internet

In einer Mailingaktion hat ein angeblich unabhängiges Magazin für Casinos Werbung für ein bestimmtes Internet-Casino verschickt. Auskunftsansprüche der Betroffenen über die zu ihrer Person gespeicherten Daten sowie die Herkunft der Daten wurden abgelehnt. Auf die Möglichkeit eines Werbewiderspruchs nach § 28 Abs. 4 Satz 2 BDSG wurde nicht hingewiesen, das Unternehmen war auch nicht bereit, einen Werbewiderspruch zu beachten. Das Unternehmen sei für gekaufte Adresslisten aus dem Ausland nicht verantwortlich. Da sich der Sitz des Unternehmens im außereuropäischen Ausland befinde, seien juristische Schritte wegen der Nutzung allgemein verfügbaren Adressenmaterials gegen ihr Unternehmen zwecklos. Im Zeitalter der Globalisierung sei es für grenzüberschreitend werbende Unternehmen unzumutbar, sich den unterschiedlichen Datenschutzgesetzen einzelner Länder zu beugen. Das Unternehmen hat als Hauptsitz einen Karibikstaat angegeben, gleichzeitig wurde aber auch eine Berliner Adresse benannt.

Die Auffassung des Unternehmens, das Bundesdatenschutzgesetz sei für die Werbeaktion des Unternehmens nicht einschlägig, ist unrichtig. Nach § 1 Abs. 5 Satz 2 BDSG findet es Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Das Bundesdatenschutzgesetz ist somit anwendbar, weil das Bewerben der Betroffenen eine Datennutzung darstellt und diese im Geltungsbereich des Bundesdatenschutzgesetzes stattfindet (unabhängig hiervon ist die Einlassung, man habe mit Adresslisten ausländischer *Adresshändler* gearbeitet, nicht sehr glaubhaft).

Das *Werbeprivileg* nach § 28 Abs. 3 Satz 1 Nr. 3 BDSG ist insoweit beschränkt, als kein Grund zu der Annahme bestehen darf, dass der Betrof-

fene ein schutzwürdiges Interesse an dem Ausschluss der Nutzung hat. In dem Anschreiben wurden die Betroffenen für die Beteiligung an einem unerlaubten Glücksspiel beworben, die Teilnahme an diesem *Glücksspiel* ist nach § 285 StGB strafbar. Die Betroffenen haben ein schutzwürdiges Interesse daran, nicht zu Handlungen beworben zu werden, die zu einem strafgerichtlichen Verfahren führen können. Danach kann sich das Unternehmen nicht auf das Werbeprivileg berufen[85]. Auch die Erhebung und Speicherung von Daten zur Durchführung rechtswidriger Mailingaktionen und die Nichterteilung von Auskünften nach § 34 BDSG sind rechtswidrig.

Bei einer Überprüfung haben wir festgestellt, dass es sich bei der von dem Unternehmen angegebenen Berliner Adresse um eine Scheinanschrift handelte. Wo das Unternehmen tatsächlich seinen Sitz hat, konnte nicht ermittelt werden. Wir haben den Betroffenen empfohlen, Strafantrag und Strafanzeige zu erstatten. Neben der unerlaubten Veranstaltung eines Glücksspiels nach § 284 StGB und der Anstiftung zur Beteiligung an einem unerlaubten Glücksspiel nach §§ 285, 26 StGB haben sich die Verantwortlichen außerdem nach § 44 Abs. 1 i.V.m. § 43 Abs. 2 Nr. 1 BDSG strafbar gemacht, indem sie unbefugt personenbezogene Daten in der Absicht verarbeitet haben, sich oder einen anderen zu bereichern.

Datenschutz contra Chiffre-Geheimnis

Ein Bürger hat sich darüber beschwert, dass eine Zeitung nicht bereit ist, ihm die Auftraggeber von Chiffre-Nummern zu benennen, bei denen er sich beworben hat und die seine Bewerbungsunterlagen nicht zurückgesandt haben. Die Zeitung berief sich anfangs uns gegenüber auf das Chiffre-Geheimnis, hierdurch sei die Zeitung gehindert, die Namen von Chiffre-Kunden offen zu legen.

Nach § 4 Abs. 3 Nr. 1 BDSG ist der Betroffene bei der Datenerhebung über die Identität der verantwortlichen Stelle zu unterrichten. Diese Norm scheint auf den ersten Blick *Chiffre-Anzeigen*, bei deren Beantwortung personenbezogene Daten übermittelt werden müssen, unmöglich zu machen. Allerdings wird man davon ausgehen können, dass Chiffre-Anzeigen auch nach der jetzigen Fassung des Bundesdatenschutzgesetzes noch rechtlich möglich sind, da der Betroffene bei einer Antwort auf die Chiffre-Anzeige selbst darauf verzichtet, Kenntnis von der Identität der verantwortlichen Stelle zu erhalten. Insoweit mag noch der Grundsatz „volenti non fit iniuria“ gelten.

Es kann allerdings nicht angenommen werden, dass jemand, der auf eine Chiffre-Anzeige antwortet, vollständig auf sein informationelles Selbstbestimmungsrecht verzichten will. Eine derartige Einwilligungserklärung wäre

[85] vgl. Ratgeber zum Datenschutz Nr. 2 „Adressenhandel und Umgang mit unerwünschter Werbung“. BlnBDI, 2004

im Übrigen auch sittenwidrig und damit unwirksam. Der Betroffene kann somit damit rechnen, dass Unternehmen, die mit Chiffre-Anzeigen arbeiten, die Vorgaben des Bundesdatenschutzgesetzes beachten. Nur unter dieser Prämisse haben die Chiffre-Anzeigen-Interessenten darauf verzichtet, die Identität der verantwortlichen Stelle zu erfahren. Chiffre-Anzeigen, bei denen personenbezogene Daten an den Anzeigenden übermittelt werden, sind somit nur rechtmäßig, wenn ein geordnetes Verfahren vorhanden ist, das die Verfahrensweise regelt, wenn der Anzeigende das informationelle Selbstbestimmungsrecht derjenigen, die ihm personenbezogene Daten zuleiten, verletzt.

Die Zeitung hat sich inzwischen bereit erklärt, die Anschrift der Anzeigenkunden, die Bewerbungsunterlagen nicht zurücksenden, gegenüber dem Betroffenen zu nennen. Die Zeitung informiert die Anzeigenkunden vorab hierüber und gibt ihnen Gelegenheit, ihre Pflicht zur Zurücksendung der Bewerbungsunterlagen zu erfüllen. Falls der Anzeigenkunde dies nicht macht oder überhaupt nicht reagiert, ist die von der Zeitung vorgenommene Datenübermittlung nach § 28 Abs. 3 Satz 1 Nr. 1 BDSG rechtmäßig.

Nachweis der Sportunfähigkeit

Eine Bürgerin hat von ihrem Recht nach § 626 BGB Gebrauch gemacht, den Vertrag mit einem Fitnessstudio aufgrund der bei ihr eingetretenen Sportunfähigkeit mit sofortiger Wirkung zu kündigen. Zum Nachweis ihrer Sportunfähigkeit legte sie ein ärztliches Attest vor. Die Bestätigung der Sportunfähigkeit durch einen Arzt reichte dem Fitnessstudio zur Gewährung des außerordentlichen Kündigungsrechts nicht. Es forderte ein detailliertes Attest mit genauen Angaben zur Erkrankung, eine Darstellung der Umstände, die zur Gesundheitsbeeinträchtigung geführt haben, und der dadurch entstandenen Folgen.

Eine zur Sportunfähigkeit führende Erkrankung gibt dem Mitglied eines *Fitnessstudios* das Recht, früher zu kündigen, als dies bei einer ordentlichen Kündigung der Fall gewesen wäre. Es ist verständlich, dass das Fitnessstudio sichergehen will, dass seine Kunden die vertraglich vereinbarten Kündigungsfristen nicht dadurch umgehen, dass sie behaupten, sie seien aufgrund einer Erkrankung nicht in der Lage, die Leistungen des Fitnessstudios in Anspruch zu nehmen. Nach § 28 Abs. 6 Nr. 3 BDSG ist das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (wie hier Krankheitsdaten) für eigene Geschäftszwecke zulässig, wenn dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt. Erforderlich ist das Attest eines Arztes, aus dem hervorgeht, dass der Petent aufgrund seiner Erkrankung sportunfähig geworden ist und deshalb nicht mehr die von dem Fitnessstudio zur Verfügung gestellten Anlagen benutzen kann.

Wir haben dem Fitnessstudio empfohlen, zukünftig bei Kündigungen wegen Sportunfähigkeit auf detaillierte Atteste zu verzichten.

Wir haben allerdings festgestellt, dass die Amtsgerichte, die sich bisher mit Klagen von Fitnessstudios gegen sportunfähig gewordene Kunden befasst haben, die von dem Fitnessstudio geforderte Substanziierung der Sportunfähigkeit bestätigt haben.

Auskunftsersuchen nach Gewerbeabmeldung

Die Senatsverwaltung für Wirtschaft, Arbeit und Frauen regte an, Daten aus dem Gewerbeanzeigenverfahren bei erfolgter Gewerbeabmeldung nach spätestens zwölf Monaten zu löschen. An die Auskunftsersuchen, die in diesem Zeitraum eingingen, wären erhöhte Anforderungen hinsichtlich des Zusammenhangs mit der aufgegebenen gewerblichen Tätigkeit zu stellen.

Wir haben der Senatsverwaltung Folgendes mitgeteilt:

Nach § 14 Abs. 8 Gewerbeordnung (GewO) dürfen nicht-öffentliche Stellen Grunddaten aus der *Gewerbeanzeige* des Gewerbetreibenden an Dritte übermitteln, wenn der Auskunftsbegehrende ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft macht. Berechtigt ist jedes wirtschaftliche und ideelle Interesse, das auf sachlichen Erwägungen beruht und mit der Rechtsordnung im Einklang steht.

Nach einer Gewerbeabmeldung ist § 14 Abs. 11 GewO i.V.m. § 17 Abs. 2 Satz 2 Berliner Datenschutzgesetz (BlnDSG) zu beachten, wonach personenbezogene Daten zu sperren sind, wenn ihre Kenntnis für die Daten verarbeitende Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

Der Sinn und Zweck der Vorschrift ist einerseits die Wahrung geschäftlicher bzw. finanzieller Interessen des Auskunftsersuchenden, andererseits handelt es sich bei den Daten nach Abs. 8 Satz 1 lediglich um Grunddaten. Daher bestehen keine datenschutzrechtlichen Bedenken gegen eine Übermittlung, wenn das Gewerbe kurze Zeit vorher abgemeldet wurde. Eine Auskunftserteilung ist maximal zwölf Monate nach Betriebsaufgabe rechtmäßig, wenn der Auskunftsbegehrende das berechtigte Interesse nicht nur glaubhaft, sondern anhand von schriftlichen Nachweisen darlegt.

Dasselbe gilt, wenn die Übermittlung weiterer Daten aus der Gewerbeanzeige nach § 14 Abs. 8 Satz 2 GewO gewünscht wird. Auch hier ist die Geltendmachung von Rechtsansprüchen nachweisbar darzulegen.

Daten von Kammerzugehörigen an politische Parteien

Der Landesbeauftragte für den Datenschutz Baden-Württemberg schilderte folgenden Sachverhalt:

Vom Büro eines Abgeordneten wurden für den Kreisverband der Partei bei einer IHK für eine geplante Veranstaltung zum Thema „Familien- und Bildungspolitik“ Adressdaten nach bestimmten Selektionskriterien ausgewählter Kammerzugehöriger angefordert. Die daraufhin übermittelten Datensätze enthielten auch Daten (Name und Anschrift des Unternehmens, Rechtsform und Branche) der Gesellschaft eines Petenten. Die IHK vertrat die Auffassung, dass ein anderer dem Wirtschaftsverkehr dienender Zweck vorgelegen habe. Sie begründete dies mit dem Bezug der Familien- und Bildungspolitik zur und ihren Auswirkungen auf die Wirtschaft und nannte als Beispiele dafür unter anderem Betriebskindergärten sowie die schulische und berufliche Ausbildung.

Da der *Deutsche Industrie- und Handelskammertag* seinen Sitz in Berlin hat, haben wir die weiteren Verhandlungen geführt. Rechtsgrundlage für die Übermittlung von Daten der Kammerzugehörigen an nicht-öffentliche Stellen durch die IHK war wegen der Subsidiarität des Landesdatenschutzgesetzes (LDSG) in diesem Fall § 9 Abs. 4 Satz 1 des Gesetzes zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern (IHK-G). Danach dürfen die Industrie- und Handelskammern Namen, Firma, Anschrift und Wirtschaftszweig ihrer Kammerzugehörigen zur Förderung von Geschäftsabschlüssen und zu anderen dem Wirtschaftsverkehr dienenden Zwecken an nicht-öffentliche Stellen übermitteln. Diese Vorschrift bezieht sich mangels einer entsprechenden Einschränkung auch auf die Weitergabe personenbezogener Daten.

Insbesondere verwies der DIHK auf den Wortlaut des § 9 Abs. 4 IHK-G, aus dem sich die seiner Meinung nach geringe Schutzwürdigkeit der Daten ergebe, die nicht auf Umwegen wieder infrage gestellt werden könne.

Der Gesetzgeber unterscheidet allerdings in Abs. 4 zwischen Daten, zu deren Weitergabe die Kammern in jedem Fall berechtigt sind (Name, Anschrift und Wirtschaftszweig des Kammerzugehörigen), soweit dieses dem Wirtschaftsverkehr dient, und Daten, die zu diesem Zweck nur dann weitergegeben werden dürfen, wenn der Betroffene nicht widerspricht. Im ersten Fall handelt es sich um Daten, die aus der Sicht des Betroffenen relativ unsensibel sind, weil er sich mit ihnen zur Verwirklichung seines Geschäftszwecks ohnehin freiwillig in die Öffentlichkeit begibt. Die Weitergabe ist an enge Bedingungen geknüpft.

Für den konkreten Fall bedeutet dies, dass Fragen der Familien- und Bildungspolitik für Unternehmen zwar von Interesse sein mögen, jedoch nicht dem in § 9 Abs. 4 IHK-G geforderten Wirtschaftzweck dienen. Zwar haben die Kammern einen gewissen Ermessensspielraum, dieser entbindet sie allerdings nicht von ihrer Verantwortung, auf die Zulässigkeit der Übermitt-

lung streng zu achten. Bei Veranstaltungen von politischen Parteien und anderen außerhalb der Wirtschaft stehenden Interessenverbänden (Religionsgemeinschaften etc.) ist daher in jedem Einzelfall die Zweckbestimmung zu prüfen.

4.7 Europäischer und internationaler Datenschutz

4.7.1 Europäische Union

Die Europäische Union ist am 1. Mai um zehn Länder erweitert worden: Estland, Lettland, Litauen, Malta, Polen, Slowakei, Slowenien, Tschechien, Ungarn und Zypern. Datenübermittlungen in alle nunmehr 25 Mitgliedstaaten der Europäischen Union und in die übrigen Mitgliedstaaten des EWR (Island, Norwegen, Liechtenstein) sind nun unter vereinfachten Voraussetzungen möglich (§ 4 b Abs. 2 BSDG).

Angemessenheitsentscheidungen

Die Europäische Kommission hat eine weitere Entscheidung zur Angemessenheit des Datenschutzniveaus in *Drittländern* nach Art. 25 Abs. 6 Europäische Datenschutzrichtlinie getroffen, und zwar zur Isle of Man[86]. Die Kanalinseln Guernsey und Jersey sowie die Isle of Man gelten als Drittländer, da sie volle Unabhängigkeit genießen und nicht zum Vereinigten Königreich gehören. Feststellungen über die Angemessenheit des Datenschutzniveaus existieren bereits zu Drittländern wie der Schweiz, Kanada, Argentinien und die Kanalinsel Guernsey[87].

Die Gewährleistung eines angemessenen Datenschutzniveaus in den USA wird seit der Entscheidung der Europäischen Kommission vom 26. Juli 2000[88] durch die *Safe-Harbor-Prinzipien* sichergestellt. Art. 4 der Kommissionsentscheidung bestimmt, dass die Kommission nach drei Jahren die Umsetzung der Entscheidung überprüfen muss. Vorbereitungen hierzu begannen bereits 2002[89]. Am 20. Oktober hat die Kommission den Safe-Harbor-Bericht formal als „Arbeitspapier der Kommissionsdienststellen" angenommen[90]. Der Bericht basiert maßgeblich auf einer Studie über die Erfahrungen der Mitgliedstaaten mit den Safe-Harbor-Prinzipien. Sie wurde von der Europäischen Kommission bei der Universität Namur in Belgien

86 ABl. EG vom 30. April 2004, L 151/51

87 ABl. EG vom 25. August 2000, L 215/1; ABl. EG vom 4. Januar 2002, L 2/13; ABl. EG vom 5. Juli 2003, L 168/19; ABl. EG vom 25. November 2003, L 308/27

88 ABl. EG L 215/7, vgl. Anlagenband „Dokumente zum Datenschutz 2000", S. 23

89 JB 2002, 4.7.1

90 SEC (2004) 1323

in Auftrag gegeben und am 19. April fertig gestellt. Der Bericht beinhaltet die Überprüfung von US-Unternehmen auf Einhaltung der Safe-Harbor-Prinzipien und die Überprüfung des US-Department of Commerce als verantwortliche Stelle für die Zertifizierung von Unternehmen in Safe Harbor. Die Art. 29-Datenschutzgruppe hatte bei der Kommission erfolglos beantragt, vor Verabschiedung des Berichts gehört zu werden. Die Datenschutzgruppe hat nunmehr beschlossen, den Bericht kritisch insbesondere auf die Kompatibilität der Safe-Harbor-Prinzipien mit der Antiterrorgesetzgebung der USA, dem US PATRIOT Act, zu prüfen, da diese Gesetzgebung nach den Terroranschlägen auf Einrichtungen der USA am 11. September 2001 die Herausgabe von Daten durch US-Unternehmen an US-Sicherheitsbehörden verlangt. Dieser Umstand konnte durch die Safe-Harbor-Prinzipien selbst nicht berücksichtigt werden und ist im Arbeitspapier der Kommissionsdienststellen vom 20. Oktober nicht enthalten. Zwischenzeitlich sind in der Liste des US Department of Commerce 637 Unternehmen, die sich den Grundsätzen des sicheren Hafens verschrieben haben, enthalten.

Übermittlung von Flugpassagierdaten in die USA

Auf die Antiterrorgesetzgebung der USA geht auch die Forderung nach Übermittlung der *Flugpassagierdaten* zurück, die zum rechtzeitigen Aufspüren von potenziellen Terroristen von den fünf größten europäischen Fluggesellschaften (Air France, British Airways, Iberia, KLM und Lufthansa) seit März 2003 den US-Sicherheitsbehörden zur Verfügung gestellt werden[91]. Die USA verlangen von den Fluggesellschaften die Reservierungsdaten (Passenger Name Records – PNR) ihrer Passagiere, anderenfalls hätten sie mit Sanktionen bis hin zum Entzug der Landerechte zu rechnen. Nicht nur aus deutscher Sicht war die Datenübermittlung in die USA mangels freiwilliger Einwilligung und Rechtsgrundlage nicht zulässig. Deshalb hat die Europäische Kommission im Mai eine Feststellung nach Art. 25 Abs. 6 Europäische Datenschutzrichtlinie im Hinblick auf die Angemessenheit des Schutzes der personenbezogenen Daten in den Passenger Name Records (PNR) getroffen[92]. Zusätzlich hat der Ministerrat beschlossen, mit den USA ein bilaterales Abkommen nach Art. 300 EG-Vertrag zu schließen[93]. Damit wurde für die Fluggesellschaften die notwendige Rechtsgrundlage für die Datenübermittlung in die USA geschaffen. Die Kommission hat sich über Bedenken hinweggesetzt, die das Europäische Parlament gegen die Datenübermittlung in die USA geäußert hatte. Es hatte den Verstoß gegen die Europäische Datenschutzrichtlinie gerügt und gefordert, dass Passagiere ihre in die USA übermittelten Daten kontrollieren und falls nötig korrigieren

91 JB 2003, 4.7.1

92 ABl. EG vom 6. Juni 2004, L 235/11

93 Ratsbeschluss vom 17. Mai 2004 über den Abschluss des Abkommens sowie das Abkommen selbst, ABl. EG vom 20. Mai 2004, L 183/83, 84

können sowie im Streitfall ein neutrales Schiedsgericht anrufen dürfen. Das Europäische Parlament hat den Europäischen Gerichtshof zur Überprüfung der Entscheidung der Kommission und des bilateralen Abkommens angerufen. Mit einer Entscheidung des EuGH wird von der Kommission nicht vor Mitte 2005 gerechnet, wahrscheinlich sogar erst 2006 oder 2007. Die Art. 29-Datenschutzgruppe hat in ihrer Stellungnahme[94] zur Angemessenheitsentscheidung der EU-Kommission und zum Abkommen mit den USA praktische Maßnahmen für dringend erforderlich gehalten, um die Eingriffe in die Rechte der Passagiere so gering wie möglich zu halten. Dazu gehört die Forderung, dass die Fluggesellschaften die Datenübermittlung so schnell wie möglich vom Pull-Verfahren auf ein Push-Verfahren umstellen. Bei dem bisher praktizierten Pull-Verfahren können die USA auf sämtliche Daten zugreifen, wobei sie allerdings nur die vereinbarten 34 Datensätze weiterverarbeiten dürfen. Dieses System soll dergestalt verändert werden, dass die Fluggesellschaften die vereinbarten Daten aktiv übermitteln.

Eine weitere Forderung der Art. 29-Datenschutzgruppe bestand darin, dass die Fluggäste über den Datentransfer angemessen informiert werden. Hierzu hat sie zwei Informationstexte erarbeitet[95], die europaweit verwendet werden sollen. Einen kurzen Informationstext erhalten diejenigen Passagiere, die ihren Flugschein in einer Reiseagentur oder per Telefon buchen. Die Langfassung gibt ein umfassendes Bild über den Zweck der Datenübermittlung, den Empfänger der Daten und die Speicherdauer und informiert eingehend über die Rechte der Fluggäste. Wir haben beim Deutschen Reisebüro- und Reiseveranstalter Verband (DRV), für den wir zuständig sind, angefragt, welche Maßnahmen getroffen worden sind, damit in Reisebüros und bei Reiseveranstaltern die Unterrichtungstexte der Art. 29-Datenschutzgruppe verwendet werden. Der DRV hat mitgeteilt, dass die Mitglieder in einem Rundschreiben über die Informationspflichten in Bezug auf die Übermittlung von PNR-Daten in die USA aufgeklärt werden. Wir haben darüber hinaus empfohlen, für den Fall, dass Reiseveranstalter in ihren Katalogen oder Fluggesellschaften die Informationstexte noch nicht vorhalten, die Reisebüros anzuhalten, die Informationstexte für die Passagiere bereitzuhalten.

Die Datensammelwut der USA aufgrund der Antiterrorgesetze zieht weite Kreise. Der Datenschutzbeauftragte von British Columbia/Kanada wies unlängst darauf hin, dass beim Outsourcing öffentlicher Dienstleistungen an US-Firmen mit Sitz in Kanada die dort befindlichen Daten dem Zugriff der US-Sicherheitsbehörden ausgeliefert sind. In seinem Bericht[96] gibt er Empfehlungen, wie die Daten geschützt werden können. Das Thema wird auch in Europa diskutiert werden müssen.

94 vom 21. Juni 2004, WP 95

95 Stellungnahme 8/2004 zur Unterrichtung von Fluggästen anlässlich der Übermittlung persönlicher Daten bei Flügen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika vom 30. September 2004, WP 97

96 Bericht von David Loukidelis

Neue Standardvertragsklauseln

Datenübermittlungen in Drittländer, zu denen die Europäische Kommission die Angemessenheit des Datenschutzniveaus noch nicht festgestellt hat, können gleichwohl unter den Voraussetzungen von § 4 c Abs. 1 BDSG erfolgen oder wenn beim Empfänger ausreichende Datenschutzgarantien vorhanden sind (§ 4 c Abs. 2 BDSG). Derartige Garantien können sich insbesondere aus Vertragsklauseln oder *verbindlichen Unternehmensregelungen* ergeben. Die Europäische Kommission hat bereits im Jahr 2001 Entscheidungen hinsichtlich *Standardvertragsklauseln* für die Übermittlung personenbezogener Daten in Drittländer getroffen[97]. Sie hat nun die Entscheidung vom 15. Juni 2001 dahingehend geändert, dass zu den im Anhang 1 enthaltenen, nach wie vor gültigen Standardvertragsklauseln der Kommission in einem Anhang 2 alternative Standardvertragsklauseln enthalten sind[98]. Auch wird klargestellt, dass die Klauseln aus den beiden Standardverträgen weder geändert noch kombiniert werden können. Die alternativen Standardvertragsklauseln gelten ab 1. April 2005. Die Mitgliedstaaten können aber Datenübermittlungen auf dieser Grundlage bereits vorher genehmigen.

Die neuen Klauseln waren von Wirtschaftsverbänden wie der Internationalen Handelskammer/ICC, der Confederation of British Industry/CBI und dem Europäischen Direktmarketingverband/FEDMA entworfen worden mit der Intention, die Wirtschaftsteilnehmer zur intensiveren Nutzung von Vertragsklauseln zu veranlassen. Die Standardvertragsklauseln der Europäischen Kommission waren von der Wirtschaft als für ihre geschäftlichen Bedürfnisse zu unflexibel empfunden worden. Die Art. 29-Datenschutzgruppe hatte in ihrer Stellungnahme[99] Nachbesserungen insbesondere in Bezug auf die Haftungsregelung und erweiterte Befugnisse der Aufsichtsbehörden gefordert. Die Pflicht zur Zusammenarbeit mit der Datenschutzaufsichtsbehörde wird nun gestärkt: Sie kann Datenübermittlungen verbieten oder aussetzen, wenn der Datenimporteur sich weigert, mit ihr zusammenzuarbeiten, oder der Datenexporteur es ablehnt, nach ihrer Aufforderung binnen der Regelfrist von einem Monat Maßnahmen zur Durchsetzung der Vertragspflichten gegenüber dem Datenimporteur zu ergreifen. Bei Verstößen durch den Datenimporteur kann nun auch direkt gegen den Datenexporteur geklagt werden, wenn er sich nicht von der Fähigkeit des Importeurs zur Einhaltung der Klauseln überzeugt hat. Wie bei den Standardvertragsklauseln der Kommission wird bei Verwendung der neuen alternativen Klauseln die Genehmigungspflicht für die Datenübermittlungen nach § 4 c Abs. 2 BDSG entfallen.

97 ABl. EG vom 4. Juli 2001, L 181/19; Auftragsdatenverarbeitung, ABl. EG vom 10. Januar 2002, L 006/52; vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2001“, S. 37 ff.

98 ABl. EG vom 29. Dezember 2004, L 385/74

99 zu dem von mehreren Wirtschaftsverbänden eingereichten Entwurf von Standardvertragsklauseln („alternative Standardvertragsklauseln“) 8/2003 vom 17. Dezember 2003, WP 84

Zusammenarbeit der Aufsichtsbehörden in Europa

Wir haben in der Vergangenheit ausführlich über die Bedeutung und den Inhalt von *Unternehmensregelungen* als Garantie für den Datenschutz in Drittstaaten und die Diskussionen auf europäischer Ebene berichtet[100], die nicht nur den wesentlichen Inhalt von verbindlichen Unternehmensregelungen, sondern auch die Zusammenarbeit der nationalen Aufsichtsbehörden betrafen. Das im Arbeitspapier der Art. 29-Datenschutzgruppe WP 74[101] genannte koordinierte Verfahren der Aufsichtsbehörden sieht vor, dass Unternehmen, die an einer Genehmigung für ähnliche Arten des Datenexports aus verschiedenen Mitgliedstaaten interessiert sind, sich eines koordinierten Genehmigungsverfahrens bedienen können.

Die zugrunde liegende Hauptidee, dass Unternehmen nur *einen* Antrag auf Genehmigung bei einer Datenschutzbehörde eines Mitgliedstaats stellen können, die zur Erteilung von Genehmigungen durch alle Datenschutzbehörden der Mitgliedstaaten führt, in denen das Unternehmen tätig ist, wird allerdings vorerst eine Wunschvorstellung bleiben, da dies in den nationalen Verfahrensordnungen nicht vorgesehen ist. Zweckmäßigerweise sollte hierfür eine Rechtsgrundlage in die Europäische Datenschutzrichtlinie aufgenommen werden. Das gilt auch für die (bis dahin freiwillige) Teilnahme der Aufsichtsbehörden in Europa an einem koordinierten Verfahren zur gegenseitigen Anerkennung von einzelnen Unternehmensregelungen. Immerhin konnten hierzu Fortschritte erzielt werden, nachdem sich bei Aufsichtsbehörden in Europa und den europa- und weltweit agierenden Unternehmen die Erkenntnis durchgesetzt hatte, dass ein nationaler „Alleingang“ nicht im Sinne des Europäischen Binnenmarkts sein kann.

Als erste hatten DaimlerChrysler und General Electric Company, deren Unternehmensregelungen von den deutschen Aufsichtsbehörden unter unserem Vorsitz in der AG „Internationaler Datenverkehr“ als ausreichende Datenschutzgarantien anerkannt worden sind[102], die europaweite Koordinierung bezüglich der Anerkennung ihrer Unternehmensregelungen beantragt. Hieran interessierte Aufsichtsbehörden in Europa haben sich im Mai in Berlin zu einem Workshop zusammengefunden, der unter dem Dach der Europäischen Akademie für Informationsfreiheit und Datenschutz[103] unter unserem Vorsitz stattgefunden hat. Im Workshop vertreten waren die Aufsichtsbehörden Frankreichs, Großbritanniens, der Niederlande, Österreichs, Polens, Ungarns sowie von den deutschen Aufsichtsbehörden außer uns die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen. Die Beteiligten waren sich einig, dass in Bezug auf Unternehmensregelungen zwei Stufen voneinander getrennt betrachtet werden müssen. Zunächst müssen die beteiligten Aufsichtsbehörden eine gemeinsame Stellungnahme erarbeiten und beurteilen, ob die vorgelegte Unternehmensregelung angemessene Datenschutzgarantien (Art. 26 Abs. 2 Europäische Datenschutzrichtlinie) beinhaltet. In einem zweiten Schritt genehmigt die jeweilige Aufsichtsbehörde die Datenübermittlung auf der Grundlage der anerkannten Unternehmensregelung, wobei hier Besonderheiten des nationalen Rechts berücksichtigt werden können.

Einigkeit bestand auch darüber, dass zunächst nur eine Aufsichtsbehörde in Europa federführend die Überprüfung der Unternehmensregelung betreibt und Verhandlungen mit dem Unternehmen hierüber führt. Die übrigen beteiligten Aufsichtsbehörden erhalten erst einen diskutablen „ersten endgültigen Entwurf“, zu dem sie sich kritisch äußern dürfen. Aufgabe der federführenden Aufsichtsbehörde ist es, die Kritikpunkte zu sammeln und dem Unternehmen zu unterbreiten. Dieses Verfahren hat sich in Deutschland bereits bewährt[104], wo die föderale Struktur und die Vielzahl der Aufsichtsbehörden diese zu einem arbeitsökonomischen Vorgehen gezwungen haben.

Wie in Deutschland muss bei einer europaweiten Koordinierung im Einzelfall zunächst entschieden werden, welche Aufsichtsbehörde die Federführung bei den Verhandlungen mit dem Unternehmen übernimmt. Dies ist nicht notwendigerweise diejenige Aufsichtsbehörde, an die sich das Unternehmen zuerst wendet. Vielmehr müssen sachliche Kriterien gefunden werden, die die Zuständigkeit einer bestimmten Aufsichtsbehörde begründen. Diese Kriterien müssen so gewählt sein, dass sie zugleich Rechtssicherheit bei den Aufsichtsbehörden und den beteiligten Unternehmen schaffen und ein „forum shopping“ vermeiden. Ein Unternehmen, das eine Anerkennung seiner Unternehmensregelung in mehreren Mitgliedstaaten der Europäischen Union betreiben will, soll sich nämlich nicht primär an die aus Sicht des Unternehmens günstigste Aufsichtsbehörde wenden und später deren positive Entscheidung den anderen Aufsichtsbehörden in Europa entgegenhalten dürfen. Mehrere Anfragen bei uns von weltweit tätigen Unternehmen mit Niederlassungen in Deutschland deuteten darauf hin, dass Deutschland als „Einstiegsland“ für die europaweite Anerkennung der Unternehmensregelung gewählt werden soll mit der (zweifellos widerlegbaren) Begründung, die deutschen Aufsichtsbehörden hätten die strengsten Anforderungen an Unternehmensregelungen, so dass eine Anerkennung durch sie fast zwingend die Anerkennung durch andere Aufsichtsbehörden in Europa zur Folge hätte. In dem von den Workshop-Teilnehmern beschlossenen Kooperationsmodell wurden einzelne Kriterien genannt, nach denen die federführende Aufsichtsbehörde bestimmt wird. Maßgeblich hierfür ist ein vorhandener europäischer Hauptsitz des Unternehmens. Aber auch die größte Niederlassung in Europa (gemessen an den Arbeitnehmern), die größte Anzahl der Niederlassungen in einem Mitgliedstaat, der Sitz der Hauptdatenbank mit

[100] JB 2002, 3.2 und 4.7.3; JB 2003, 4.7.1

[101] Arbeitsdokument vom 3. Juni 2003: Übermittlung personenbezogener Daten in Drittländer: Anwendung von Art. 26 Abs. 2 Europäische Datenschutzrichtlinie auf verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer; vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2003“, S. 65

[102] JB 2002, 4.7.3; JB 2003, 4.7.2

[103] JB 2002, 6.5

[104] JB 2003, 4.7.2

den international zu übermittelnden Daten oder der Ort, an dem Datenschutzfragen des Unternehmens entschieden werden, wurden als Anknüpfungspunkte diskutiert.

Im Workshop wurden fünf „Testfälle“ im Hinblick auf die Federführung bei der Erarbeitung einer gemeinsamen Stellungnahme zur Unternehmensregelung besprochen: DaimlerChrysler, General Electric (GE), Philips, KPMG International und British Petrol BP. In Bezug auf die Unternehmensregelung von DaimlerChrysler für Kunden-/Lieferantendaten[105] und die Unternehmensregelung von General Electric Company für Mitarbeiterdaten[106] wurde beschlossen, dass Deutschland die Federführung in Europa nicht übernehmen kann, da die Unternehmensregelungen hier bereits formal anerkannt worden waren und auf ihrer Grundlage Genehmigungen für Datenübermittlungen (§ 4 c Abs. 2 BDSG) erteilt worden sind. Da zum Zeitpunkt des Workshops bereits Verhandlungen von DaimlerChrysler mit der französischen Aufsichtsbehörde CNIL anstanden, hat die CNIL zugleich die Federführung bei der europaweiten Koordinierung der Anerkennung übernommen. Bei der Unternehmensregelung von General Electric für Mitarbeiterdaten konnte trotz des europäischen Hauptsitzes in Brüssel die belgische Aufsichtsbehörde die Federführung nicht übernehmen, da auch in Belgien die Unternehmensregelung bereits anerkannt war. Angesichts von 20 % der in Europa tätigen Mitarbeiter von General Electric in Ungarn lag es nahe, dass die Aufsichtsbehörde in Ungarn die Federführung bei der Koordinierung übernimmt. Diese übergab die Federführung jedoch an die britische Aufsichtsbehörde, die sich angesichts der Anzahl der Niederlassungen von GE und des Hauptsitzes eines der größten Unternehmen von GE in Großbritannien für die geeignetere Aufsichtsbehörde im Hinblick auf die Federführung hielt. Das Beispiel zeigt, dass den Unternehmen, aber auch den Aufsichtsbehörden nicht zuviel Ermessen bei dieser Entscheidung eingeräumt werden darf.

Die Federführung für die Unternehmensregelung von Philips liegt angesichts des Hauptsitzes des Konzerns bei der niederländischen Aufsichtsbehörde. Die Unternehmensregelung von KMPG International mit Hauptsitz in Amsterdam war von einem deutschen Mitglied des Unternehmens uns zur Überprüfung vorgelegt worden und ist an die für den Hauptsitz zuständige Aufsichtsbehörde in den Niederlanden übergeben worden. Die Unternehmensregelung für den Konzern British Petrol war von der deutschen Niederlassung bei der Aufsichtsbehörde in Hamburg zur Überprüfung eingereicht worden und wurde von ihr angesichts des Hauptsitzes des Konzerns in Großbritannien an die britische Aufsichtsbehörde geleitet.

Leider hat sich bei Folgeveranstaltungen gezeigt, dass einige Aufsichtsbehörden in Europa von der Idee der Federführung abrücken und Stellungnahmen der übrigen Aufsichtsbehörden zu einzelnen Fragestellungen einholen,

[105] JB 2002, 4.7.3, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2002“, S. 38

[106] JB 2003, 4.7.2

anstatt zunächst selbst die Verhandlungen mit dem Unternehmen zu führen und auftretende Fragen mit diesem zu klären. Zwischenzeitlich hat sich auch die Art. 29-Datenschutzgruppe der Thematik angenommen. Bei Konferenzen in Brüssel und Den Haag, wo im Rahmen einer Anhörung zu den Erfahrungen mit dem WP 74 sowohl Aufsichtsbehörden – auch wir – als auch Unternehmensvertreter zu Wort gekommen sind, wurde die Erarbeitung von Arbeitspapieren in Aussicht genommen, die sowohl die Koordinierung des Verfahrens der europaweiten Anerkennung von Unternehmensregelungen als auch die inhaltlichen Anforderungen an Unternehmensregelungen konkretisieren. Grundlage hierfür ist eine Checkliste, die von der britischen Aufsichtsbehörde für die Beratung von Unternehmen entworfen worden ist. Die Entwürfe der Arbeitspapiere sollen in einer Unterarbeitsgruppe weiterentwickelt werden, in die wir die Vorstellungen und Erfahrungen in Deutschland einbringen werden.

4.7.2 AG „Internationaler Datenverkehr“

Die Arbeit der AG „*Internationaler Datenverkehr*“ des Düsseldorfer Kreises war in diesem Jahr maßgeblich von den Entwicklungen auf europäischer Ebene geprägt. Daneben ist es gelungen, nach den Erfolgen in den vergangenen Jahren[107] eine weitere Unternehmensregelung auf den Weg zu bringen: Die Schering AG hat den Entwurf einer „Unternehmensrichtlinie zum Umgang mit personenbezogenen Daten innerhalb des Schering-Konzerns“ vorgelegt. Sie gilt für die Verarbeitung sämtlicher personenbezogener Daten über Mitarbeiter und Vertragspartner, Probanden und Patienten in klinischen Prüfungen, Medizinpersonal und Kunden und soll für ausreichende Datenschutzgarantien nach Übermittlung dieser Daten in Konzernteile sorgen, die in Drittländern ohne angemessenes Datenschutzniveau ansässig sind (§ 4 c Abs. 2 BDSG). Von den weltweit tätigen 26.000 Mitarbeitern sind nur 10.000 in Deutschland beschäftigt.

Da der Konzernhauptsitz in Berlin ist, haben wir als zuständige Aufsichtsbehörde die Verhandlungen mit dem Konzern über die unabdingbaren Inhalte der Unternehmensregelung geführt. Der Entwurf wurde sodann in der AG „Internationaler Datenverkehr“ behandelt, in der letzte offene Fragen der übrigen Aufsichtsbehörden mit den Vertretern des Konzerns geklärt wurden. Nach Übernahme der letzten Änderungen in die Unternehmensrichtlinie und Mitteilung durch die Schering AG, aus welchen anderen EU-Mitgliedstaaten internationale Datentransfers auf der Grundlage der Unternehmensrichtlinie erfolgen, werden wir die Koordinierung der Anerkennung dieser Unternehmensrichtlinie durch die beteiligten Aufsichtsbehörden in Europa betreiben. Am Ende des Koordinierungsverfahrens steht die Genehmigung der Datenübermittlung durch uns, denn internationale Datentrans-

[107] JB 2003, 4.7.2; JB 2002, 4.7.3

fers aus Deutschland auf der Basis der Unternehmensrichtlinie sollen nur vom Konzernhauptsitz in Berlin erfolgen. Der europäische Binnenmarkt zollt also seinen Tribut: Einen deutschen „Alleingang“ in Bezug auf die Anerkennung von Unternehmensregelungen und die Genehmigung von Datenübermittlungen wird es angesichts der – hoffentlich unumkehrbaren – Bestrebungen zur Verfahrenskoordinierung und europaweiten Anerkennung nicht mehr geben.

4.8 Organisation und Technik

4.8.1 Behördliche Datenschutzbeauftragte

Gesprächskreis der behördlichen Datenschutzbeauftragten der Bezirke

Im Berichtszeitraum fanden erneut drei Treffen der *behördlichen Datenschutzbeauftragten* der Bezirke statt.

Am Beispiel des neuen IT-Verfahrens EvASta (Einbürgerung von Ausländern und Staatsangehörigkeitsangelegenheiten) wurde die Durchführung der mit der Novellierung des Berliner Datenschutzgesetzes im Jahre 2001 neu eingeführten Vorabkontrolle durch die behördlichen Datenschutzbeauftragten der Bezirke erörtert.

Die *Vorabkontrolle* ist nach § 5 Abs. 3 Satz 2 BlnDSG geboten, wenn in einem Verfahren Daten verarbeitet werden, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen oder zur Verfolgung von Straftaten oder Ordnungswidrigkeiten erhoben werden. § 19 a Abs. 1 Satz 3 Nr. 1 BlnDSG bestimmt als eine Aufgabe der behördlichen Datenschutzbeauftragten die Durchführung solcher Vorabkontrollen bei den mit besonderen Risiken für Rechte und Freiheiten von Betroffenen verbundenen Verarbeitungen. Das Einbürgerungsverfahren fällt nicht unter § 5 Abs.3 Satz 2 BlnDSG, jedoch werden Angaben zur Volkszugehörigkeit (im Unterschied zur Staatsangehörigkeit) verarbeitet, die als personenbezogene Daten über die rassische und ethnische Herkunft zu den besonderen Kategorien personenbezogener Daten gehören, die nach § 6 a BlnDSG nur unter sehr eingeschränkten und strengen rechtlichen Voraussetzungen verarbeitet werden dürfen. Dies rechtfertigt auch die Durchführung der Vorabkontrolle.

Die Verarbeitung solcher Daten verlangt angemessene Garantien zum Schutze des Rechts auf informationelle Selbstbestimmung und konkret eine besondere Rechtsvorschrift, die den Zweck der Verarbeitung bestimmt. Für das Einbürgerungsverfahren gibt es keine solche Rechtsvorschrift, so dass die Verarbeitung der sensitiven Daten nur zulässig ist, wenn der Betroffene ausdrücklich eingewilligt hat.

Moderne Arbeitsplatzrechner und Notebooks sind mit USB-Schnittstellen (Universal Serial Bus) ausgestattet. Diese Schnittstellen dienen dem Anschluss verschiedener Hardwarekomponenten wie Drucker, Laufwerke für externe Speichermedien (Disketten, CD oder DVD), Festspeichermedien oder Netzwerkhardware bis hin zu digitalen Kameras. Da die modernen Betriebssysteme die neu angeschlossenen Geräte automatisch erkennen und einbinden, entfallen aufwändige Installationsprozeduren für Hard- und Software.

Dadurch sinkt die Hemmschwelle in den Dienststellen, nicht freigegebene oder auch private Technik zu nutzen. Die bisher eingerichteten Nutzungsbeschränkungen für CD- und Floppy-Laufwerke sind bei *USB-Anschlüssen* nicht mehr ausreichend wirksam. Folglich müssen Mechanismen gefunden werden, mit denen der Zugriff auf den USB eines bestimmten, zugelassenen Geräts beschränkt werden kann.

Lösungen hängen im Wesentlichen von dem zum Einsatz kommenden Betriebssystem ab. Mit Windows kann der Zugriff auf USB-Geräte derzeit noch nicht auf einfache Weise verhindert werden. Mit moderatem zusätzlichem Aufwand kann die Installation nicht zugelassener Gerätetypen jedoch erkannt und blockiert werden. Unter Linux ist es ebenfalls mit geringem bis moderatem Aufwand möglich, den Zugriff auf ausdrücklich benannte Geräteklassen oder -typen zu beschränken.

Details zum Schutz vor Missbrauch von USB-Schnittstellen sind der Orientierungshilfe „Datensicherheit bei USB-Geräten“ des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu entnehmen.

Workshop der behördlichen Datenschutzbeauftragten der Amtsgerichte

Beim Erfahrungsaustausch der Datenschutzbeauftragten der Amtsgerichte nahm die Erstellung einer Checkliste breiten Raum ein, die für die Kontrollen nach § 5 BlnDSG zur Anwendung kommen soll. Hierfür wurde eine Arbeitsgruppe eingesetzt, die – auf die Verhältnisse und die technisch-organisatorische Umgebung in den Amtsgerichten zugeschnitten – die wichtigsten Prüfkriterien zusammenstellte. Das Spektrum reicht von der Kontrolle der Zugangsbedingungen, der Berechtigungen für einen Zugriff auf personenbezogene Daten bis hin zu Fragen der Protokollierungen und der Dokumentation, unter anderem auch behördlichen und verfahrensspezifischen Sicherheitskonzepten.

Zwei Datenschutzbeauftragte erklärten sich bereit, die Checkliste probeweise in ihren *Gerichten* anzuwenden. Bei der nächsten Sitzung berichteten sie von ihren Erfahrungen: Dabei stellte sich heraus, dass es bei den meisten Verantwortlichen an Datenschutzbewusstsein mangelt. Da die Hauptanwendung – das IT-Verfahren *AULAK* (Automatische Verfahren Land-, Amts-,

Kammergericht) – vom LIT betreut wird, verwiesen die meisten Befragten beim überwiegenden Teil der Fragen auf die Zuständigkeit des IT-Dienstleisters. Offensichtlich fehlt das Bewusstsein, dass die Gewährleistung des Datenschutzes bei der Daten verarbeitenden Stelle – also bei ihnen selbst – liegt. Daten verarbeitende Stelle ist nach § 4 Abs. 3 Nr. 1 BlnDSG jede Behörde oder sonstige öffentliche Stelle, die Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt.

Auffällig war insbesondere die fehlende Zugangssicherung in vielen Räumen, in denen personenbezogene Unterlagen aufbewahrt werden, aber auch in sicherheitsrelevanten Serverräumen. Mangelfeststellungen der behördlichen Datenschutzbeauftragten der Gerichte betrafen hier vorwiegend fehlende Sicherheitsschlösser und nicht abschließbare Schränke. Die Verteidigung der Befragten war in diesen Fällen stets die gleiche, nämlich dass für besondere Sicherheits- und Schutzmaßnahmen kein Geld vorhanden sei und dass man im Übrigen schon immer so verfahren habe.

Diese Reaktion offenbart Gleichgültigkeit gegenüber den gesetzlichen Forderungen. Die sichere Unterbringung personenbezogener Daten sollte mittlerweile eine Selbstverständlichkeit sein und entsprechend – durch Prioritätsverlagerung bei den Haushaltsmitteln – finanziert werden.

> *Aus einem Amtsgericht wurde berichtet, dass der Fachpostverkehr sehr nachlässig gehandhabt wird. Hier wird eine Fremdfirma für den Aktentransport eingesetzt und es wurde mehrmals beobachtet, dass der Aktenwagen samt Aktenmappen und Transportkisten längere Zeit unbeaufsichtigt – z. T. auch in Bereichen mit regem Publikumsverkehr – herumstand.*

Der behördliche Datenschutzbeauftragte hatte als Anschauungsobjekt eine leere *Transportkiste* mitgebracht, die sogar vorschriftsmäßig mit einer Plombe versehen war; er demonstrierte jedoch anschaulich, wie er aus der Kiste durch einfaches Öffnen der Plombe (leichtes Herausziehen und Zurückstecken des Haltedrahts) leicht an Unterlagen gelangen konnte, ohne dass der Zugriff bemerkt werden konnte.

Bei solchen Transportvorkehrungen – die offensichtlich nicht ausreichend getestet wurden – liegt ein Verstoß nach § 5 Abs. 4 i.V.m. § 5 Abs. 2 Nr. 1 und 3 BlnDSG vor (mangelnder Schutz der Vertraulichkeit und der Verfügbarkeit der nicht automatisiert verarbeiteten Daten).

> *Ein Teilnehmer fragte, ob es auch in anderen Amtsgerichten zulässig sei, dass Hilfskräfte von außerhalb des Hauses bei den Geschäftsstellen der Amtsgerichte mitarbeiten dürfen. Bei diesen Kräften handelt es sich meist um Sozialhilfeempfänger und Resozialisierungsfälle, manchmal aber auch Praktikanten. Sie bekommen im Rahmen ihrer Tätigkeit Einblicke in Sachakten, wobei es sich mitunter auch um Unterlagen mit sehr sensiblen Inhalt handelt, z. B. zu Zwangsvollstreckungen und Auszüge aus dem Schuldnerverzeichnis. In einem Fall wurde ein Straftäter als Hilfskraft eingesetzt, der bei seiner Tätigkeit sogar Einsicht in Strafakten nehmen konnte.*

Gegen den Einsatz von Hilfskräften ist nichts einzuwenden, sofern darauf geachtet wird, dass diese Mitarbeiter keine personenbezogenen Daten zur Kenntnis nehmen können. Durch geeignete Maßnahmen (z. B. Vergabe von Aufgaben, bei denen man nicht mit personenbezogenen Daten in Berührung kommt; strengere Aufsicht) ist zu gewährleisten, dass die erforderliche Vertraulichkeit beim Umgang mit diesen Daten gewahrt bleibt.

Behördliche Datenschutzbeauftragte in den Stellenpool!

> *Der Datenschutzbeauftragte eines Bezirksamtes war der erste, der uns alarmierte, weil seine Personalstelle ihm die Versetzung in den Stellenpool angekündigt hatte. In diese bei der Senatsverwaltung für Finanzen angesiedelte Behörde für das Personalüberhangmanagement werden Beamte und Angestellte auf Lebenszeit abgeordnet, deren Aufgabengebiet im Rahmen der Straffung öffentlicher Aufgaben entfallen ist. Der Stellenpool hat die Aufgabe, diese Bediensteten wieder in andere Aufgabengebiete oder auf Arbeitsplätze in der Privatwirtschaft zu vermitteln.*

Der Datenschutzbeauftragte des Bezirks konnte offensichtlich seine Behörde von der Rechtswidrigkeit ihres Handelns überzeugen und verblieb im Amt, ohne dass wir intervenieren mussten.

Anders war die Lage im Landesverwaltungsamt, einer nachgeordneten Behörde der für die Datenschutzgesetzgebung zuständigen Senatsverwaltung für Inneres. Das *Landesverwaltungsamt* ist verantwortlich für das zentrale IT-Großverfahren IPV (Integrierte Personalverwaltung), in dem die Personaldaten fast aller im öffentlichen Dienst des Landes Beschäftigten verarbeitet werden. Das Amt ist zentrale Beihilfestelle des Landes Berlin und verarbeitet automatisiert und manuell Personaldaten, die auch medizinische Daten enthalten. Es hat noch viele weitere Aufgaben im Zusammenhang mit personenbezogen Daten: als Pensionsstelle für die Versorgung der Pensionäre, als Gehalts-, Vergütungs- und Lohnstelle für diverse Behörden und als Entschädigungsbehörde zur Entschädigung der Opfer des Nationalsozialismus.

Dem *behördlichen Datenschutzbeauftragten* und seinem Vertreter wurde kurzerhand mitgeteilt, dass sie in den Stellenpool versetzt werden, weil das Aufgabengebiet des behördlichen Datenschutzes gestrichen worden sei und in Zukunft nur noch als Funktion erhalten bliebe. Diese Funktion könne man auch aus dem Stellenpool aus erfüllen, so dass man noch nicht einmal die als rechtswidrig erkannte Abbestellung des Datenschutzbeauftragten durchführen müsse. Wenn er von dort aus auf andere Arbeitsplätze vermittelt würde, könne er die Funktion nicht mehr wahrnehmen und es läge dann ein wichtiger Grund vor, ihn nach § 626 BGB außerordentlich zu kündigen.

Wir haben das Landesverwaltungsamt nachhaltig auf die Rechtswidrigkeit seines Vorhabens aufmerksam gemacht und die aufsichtführende Senatsverwaltung für Inneres darüber unterrichtet.

Mit der Abschaffung des geschäftsplanmäßigen Aufgabengebietes „Behördlicher Datenschutz“ und der Beibehaltung des behördlichen Datenschutzbeauftragten als reine institutionelle Funktion wird der Stellenwert des Datenschutzes im Landesverwaltungsamtes eklatant und in demonstrativer Weise verringert. Dies ist angesichts der datenschutzrechtlichen Bedeutung des Amtes nicht hinnehmbar. Auch ohne Würdigung der besonderen Bedeutung des Datenschutzes im Landesverwaltungsamt wird dem Datenschutzbeauftragten durch Gesetz (§ 19 a Abs. 1 BlnDSG) eine Vielzahl von Aufgaben zugewiesen, die selbstverständlich ein Arbeitsgebiet darstellen, die eine Alibibestellung ausschließen.

Angesichts der datenschutzrechtlichen Relevanz des Landesverwaltungsamtes kann die Funktion des Datenschutzbeauftragten nur mit einem ausgewiesenen Aufgabengebiet verbunden sein. Ganz sicher würde eine den gesetzlichen Aufgaben des behördlichen Datenschutzbeauftragten entsprechende Aufgabenwahrnehmung auch eine volle Stelle ausfüllen.

Durch die Bestellung zum behördlichen Datenschutzbeauftragten ist das Amt persönlich übertragen worden. Voraussetzung für eine korrekte Amtsführung ist seine Unabhängigkeit, die es ihm ermöglichen muss, ohne Furcht vor Sanktionen auch Konflikte mit der Amtsleitung durchzustehen. Seine Unabhängigkeit wird gesetzlich geschützt durch seine Weisungsfreiheit in Angelegenheiten des Datenschutzes, den unmittelbaren Zugang zur Behördenleitung, das Benachteiligungsverbot und in erster Linie den Schutz vor willkürlicher Abberufung.

Da der Amtsinhaber weiterhin die Aufgaben des behördlichen Datenschutzbeauftragten wahrnehmen soll, kann er nicht in den Stellenpool versetzt werden, denn es ist untersagt, dass Mitarbeiter, die in den Stellenpool versetzt wurden, weiter ihren früheren Aufgaben nachgehen dürfen. Dies stünde im Widerspruch zum Zwecke des Stellenpools.

Voraussetzung dafür, den Amtsinhaber in den Stellenpool zu versetzen, wäre die vorherige Abberufung aus dem Amt des Datenschutzbeauftragten und die Neubestellung eines Datenschutzbeauftragten. Da er das Amt jedoch nicht freiwillig freigeben wollte, setzt die Abberufung die Anwendung von § 626 BGB voraus.

Die formelle Bestellung eines Stellvertreters des behördlichen Datenschutzbeauftragten ist im neuen Berliner Datenschutzgesetz vorgesehen worden, um eine Abwesenheitsvertretung zu gewährleisten. Er erfüllt in Abwesenheit des behördlichen Datenschutzbeauftragten dessen Aufgaben und benötigt dafür die gleiche Unabhängigkeit wie dieser. Aus diesem Grunde gilt für den Stellvertreter nichts anderes als für den primären Amtsinhaber.

Inzwischen ist der behördliche Datenschutzbeauftragte freiwillig in den vorzeitigen Ruhestand gegangen. Das Amt wurde der Leiterin des Steuerungsdienstes übertragen, die hoffentlich über die für die Aufgabe des Datenschutzes nötigen Zeitreserven verfügt. Das Problem des Stellvertreters wurde noch nicht beseitigt.

4.8.2 Mehr IT-Sicherheit durch Server Based Computing?

Im Jahresbericht 2003[108] wurde die Renaissance der *zentralen Datenverarbeitung* als ein wesentlicher Trend der Entwicklung informationstechnischer Systeme herausgestellt. Ein Jahr später hat der Trend längst die IT-Landschaft der Berliner Verwaltung erfasst und nährt die Hoffnung nach höherer Verfahrenssicherheit. Auf dem Konzept des *Server Based Computing* hat die Senatsverwaltung für Inneres ihre Datenverarbeitung modernisiert, auf dem gleichen Konzept sollen auch die hohen Sicherheitsrisiken des Sozialhilfeverfahrens BASIS eingedämmt werden.

Server Based Computing (SBC) ermöglicht die Durchführung der Datenverarbeitungsprozesse für die Anwendungen und Dienste auf zentralen Rechnern (Servern). Die Bildschirmausgabe wird jedoch auf einen entfernten Arbeitsplatz umgeleitet. Ein Server kann dabei eine Vielzahl von graphischen Arbeitsplätzen (Clients) gleichzeitig bedienen. Die Betreuung der Applikationen erfolgt zentral durch den Administrator des Servers. Dort erfolgt auch die Steuerung der Zugriffe auf die Applikationen, Programme und Daten, also die Zugriffskontrolle. Andererseits können von einem Arbeitsplatz aus Verbindungen zu mehreren Servern aufgebaut werden, sofern der Benutzer dazu berechtigt ist.

Die Clients agieren lediglich als Ein- bzw. Ausgabegeräte. Ihre Rechnerleistung dient vor allem der ergonomischen und graphisch anspruchsvollen Präsentation der Verarbeitungsdialoge. Dabei spielt es keine Rolle, über welches Leistungsvermögen die eingesetzten Rechner verfügen. Die Funktionalität entspricht prinzipiell der von Terminals, die über keine eigene Verarbeitungskapazität verfügen. Im Gegensatz zu den einfachen Terminals, die noch aus der Zeit vor den Client-Server-Konfigurationen bekannt sind, kann der „Terminal-Client“ seine Ressourcen, wie z. B. seine Schnittstellen, den daran angeschlossenen lokalen Drucker und seine Soundkarte weiterhin nutzen. Er ist sogar weiterhin in der Lage, die Aufgaben eines vollwertigen PC wahrzunehmen, beispielsweise als Stand-Alone-PC für lokale Anwendungen (z. B. Textverarbeitung) oder als Client in einem Client-Server-Netz einer anderen Anwendung.

Der Ansatz, Funktionen von in lokalen Netzen organisierten Personal Computern zu zentralisieren, ist unter den Stichwörtern „Netzwerk-Computer“, „Medialess PC“ oder „Thin-Client“ schon früher verfolgt worden.

[108] JB 2003, 2.1

Diese Netzwerk-Computer sind Clients, deren lokale Ausstattungen stark reduziert werden: Interne Massenspeicher werden nicht mehr gebraucht, denn alle Programme und Daten, die für die Verarbeitung benötigt werden, werden aus dem Netz bezogen, denn irgendwo steht ein Server, der den jeweils gewünschten Dienst leisten kann. Der Netzwerkcomputer ist auf die Bedienung und die Benutzeroberfläche spezialisiert. Im Unterschied zum Server Based Computing verarbeitet der „Thin-Client" seine Prozesse selbst und lagert lediglich seine Datenhaltung auf einen Server aus.

Der bereits 1997[109] diskutierte Ansatz des Netzwerk-Computers scheiterte aus mehreren Gründen. Einerseits stieß die damals durchschnittlich verfügbare Netzwerkleistung von 10 Megabit/Sekunde schnell an ihre Kapazitätsgrenzen, was durch die Verbreitung graphischer Benutzeroberflächen (z. B. Windows) besonders schnell deutlich wurde. Diese benötigen einen virtuellen Arbeitsspeicher, der standardmäßig auf Festplatten abgelegt wird und eine sehr hohe Anzahl von Zugriffen erzeugt. Nur wenige Netzwerk-Computer reichten aus, um ein Netz zu überlasten. Andererseits war die damals zur Verfügung stehende Hardware nicht leistungsfähig genug, um dieses Problem durch beispielsweise entsprechend hohen Arbeitsspeicher zu kompensieren.

Das Server Based Computing bietet eine Reihe von Vorteilen, die sich auch auf die Sicherheit der Datenverarbeitung auswirken:

– Auftretende Probleme müssen nur einmal am Server behoben werden und nicht an jedem einzelnen Client. Die Benutzerunterstützung kann effizienter und schneller arbeiten. Für die Clients ergibt sich eine „Zero-Administration", einen gegen Null tendierenden Administrationsaufwand. Das verbessert die Verfügbarkeit der Systeme.

– Die Verfügbarkeit wird auch verbessert durch die Erhöhung der Ausfallsicherheit – sowohl beim Anwender als auch auf dem Server. Fällt ein Endgerät aus, kann der Anwender ein anderes nutzen – alle wichtigen Daten oder Anwendungen sind zentral auf dem Server gespeichert. Server-Parks können so ausgelegt sein, dass im Falle eines Ausfalls ein anderer Server die Arbeit übernimmt.

– Ein weiterer Vorteil ist die Kapselung der Arbeitsumgebung: Wenn keine Anwendungen aufgespielt werden können, ist auch keine Gefahr gegeben, dass Viren eingeschleust oder Daten kopiert und entwendet werden können. Der Schutz von Vertraulichkeit, Verfügbarkeit und Integrität wird weiter deutlich erhöht.

– Auch umgekehrt gelingt eine Schutzverbesserung, wenn ein Server Based Computing System für den Zugang zum Internet genutzt wird. Wird der Server erfolgreich angegriffen, so bleiben die Clients geschützt und für die lokalen Aufgaben einsatzfähig.

[109] JB 1997, 2.1

Auch auf die Kostenseite kann sich Server Based Computing positiv auswirken. Statt einer Lizenz für jeden einzelnen Mitarbeiter benötigt man nur einen Pool von Lizenzen zur simultanen Nutzung. Da in der Regel nicht alle Mitarbeiter gleichzeitig eine Anwendung nutzen, können hier ebenfalls erhebliche Kosten eingespart werden. Auch auf der Hardwareseite kann gespart werden, da auch veraltete PC weiter als Client nutzbar sind, weil die Kapazitäten moderner Rechner gar nicht ausgenutzt werden können.

Als Nachteile werden oft die anfangs hohen Beschaffungskosten für die Serverhardware angesehen, an die wegen der hohen Aufgabenlast sehr hohe Leistungsmaßstäbe gesetzt werden müssen. Kritisch wird auch die zu erwartende Erhöhung der Netzwerklast gesehen. Eine Machbarkeitsstudie des LIT für die Server-Based-Computing-Lösung in der Sozialverwaltung (BASIS) kam jedoch zu dem Ergebnis, dass die bestehende Netzinfrastruktur den Anforderungen gerecht werde.

4.8.3 Verschlüsselte Viren – die unerkannte Gefahr?

Viren und *Würmern* wird bereits beim Eintreten in das Berliner Landesnetz durch eine zentrale Virenkontrolle im *LIT* Angst gemacht; und trotzdem treten hier und da Schädlinge auf. Bei neuen Schädlingen ist das klar. Abhilfe schafft hier das schnelle Einspielen der aktuellen Vireninformationen. Es treten aber auch häufig welche auf, die schon lange bekannt sind und durch Virenscanner eigentlich entdeckt werden müssten. Ursache hierfür ist oftmals die Nutzung des aus Datenschutzsicht sehr zu begrüßenden verschlüsselten WWW-Dienstes (*HTTPS* – Hypertext Transfer Protocol Secure). Die Verschlüsselung der Kommunikation und der Daten führt jedoch dazu, dass der zentrale Virenscanner die Viren nicht erkennt und so die ansonsten gewünschte Vertraulichkeit der Kommunikation bzw. der Daten zu erheblichen Gefahren für die an das Berliner Landesnetz angeschlossenen Systeme führt. Aus diesem Grund hat der LIT ein Verfahren eingeführt (HTTPS-Scan), das die Kontrolle auf schädliche Inhalte beim verschlüsselten Webverkehr ermöglicht. Dazu werden die verschlüsselten Daten entschlüsselt, auf Viren geprüft, wieder verschlüsselt und anschließend an den Empfänger weitergeleitet. Dieses hat zu mehreren Beschwerden geführt und den LIT veranlasst, das HTTPS-Scan-Verfahren vorerst wieder einzustellen.

Durch die Nutzung von HTTPS wird die Vertraulichkeit der übertragenen Daten gewährleistet. Ein „Aufbrechen" der Verschlüsselung zum Schutz des gesamten Berliner Landesnetzes gegen Viren steht diesem entgegen. Wir bewegen uns also im Spannungsfeld zwischen Datenschutz und Systemschutz, wobei der Systemschutz ein wesentlicher technischer Eckpfeiler zur Umsetzung der datenschutzrechtlichen Anforderungen ist. Wir haben daher das HTTPS-Scan-Verfahren im LIT einer Kontrolle nach § 24 Abs. 1 Berliner Datenschutzgesetz unterzogen, um zu einer eigenen Position in diesem Spannungsfeld zu gelangen.

Wird aus dem Berliner Landesnetz heraus eine HTTPS-Verbindung in das Internet aufgebaut, wird diese automatisch über einen HTTPS-Scanserver geleitet. Dieser bleibt während der gesamten Verbindung zwischen dem anfragenden Client und dem eigentlichen Server aktiv. Der HTTPS-Scanserver nimmt den Wunsch des Clients für den Verbindungsaufbau entgegen und sendet diesen an den eigentlichen Server weiter. Der Server sendet sein Zertifikat an den HTTPS-Scanserver. Dieser überprüft das Zertifikat und baut nach erfolgreicher Prüfung eine HTTPS-Verbindung zum eigentlichen Server auf und ist damit im Besitz des Verbindungsschlüssels zur Serverseite hin. Auf der anderen Seite generiert er ein Serverzertifikat und sendet es dem anfragenden Client zu. Akzeptiert dieser das Zertifikat, wird auch an dieser Seite eine HTTPS-Verbindung aufgebaut und der HTTPS-Scanserver ist im Besitz des Verbindungsschlüssels zur Clientseite hin. Nun kann der HTTPS-Scanserver den Inhalt der HTTPS-Verbindung auf Viren überprüfen, indem er die vom Server kommenden Daten entschlüsselt, auf Viren prüft, wieder verschlüsselt und dem Client sendet. Dieser Vorgang findet gekapselt auf einem Server statt. Somit ist gewährleistet, dass außerhalb des Scanvorgangs die Daten immer verschlüsselt sind.

Insgesamt konnte festgestellt werden, dass

- auf Client-Seite ausschließlich die an das MAN angeschlossenen Nutzer betroffen sind,
- die Nutzung dieser Clients nach § 1 Abs. 4 der Dienstvereinbarung über die Nutzung des Internets und anderer elektronischer Informations- und Kommunikationsdienste in der Berliner Verwaltung – abgeschlossen zwischen der Senatsverwaltung für Inneres und dem Hauptpersonalrat für die Behörden, Gerichte und nichtrechtsfähigen Anstalten – grundsätzlich zu dienstlichen Zwecken gestattet ist,
- der Datenverkehr nur auf Viren geprüft wird und keiner weiteren Filterung unterliegt,
- mit dieser Maßnahme verhindert werden kann, dass Viren in das Berliner Landesnetz eindringen, insbesondere beim Herunterladen von E-Mails bzw. Attachments über HTTPS-Webmail von externen Servern im Internet,
- das „Aufbrechen“ der Verschlüsselung, das Scannen auf Viren und das erneute Verschlüsseln der jeweiligen Verbindung auf demselben Server stattfindet,
- durch das Verfahren gewährleistet ist, dass die Inhaltsdaten nur von der Anti-Viren-Software überprüft, nicht jedoch von den Administratoren oder sonstigen Nutzern zur Kenntnis genommen werden können, und
- den Nutzern durch Hinweise beim Einlesen der Server-Zertifikate verdeutlicht wird, dass der HTTPS-Datenverkehr nicht direkt mit dem angewählten Server stattfindet.

Vor diesem Hintergrund musste die Abwägung zwischen den zur Gewährleistung der IT-Sicherheit getroffenen Maßnahmen und den berechtigten Interessen der Nutzer an der Vertraulichkeit des Datenverkehrs zugunsten des Schutzes des gesamten Berliner Landesnetzes vor Viren ausfallen, da innerhalb des Berliner Landesnetzes die ordnungsgemäße Datenverarbeitung zu gewährleisten ist und die Vertraulichkeitsrisiken vernachlässigt werden können. Wir haben dem LIT daher empfohlen, das HTTPS-Scan-Verfahren wieder einzusetzen.

4.8.4 Videoüberwachung in einer Berliner Magistrale

Durch zahlreiche Eingaben von Bürgern, Foren im Internet und Meldungen in den Medien veranlasst, haben wir eine Hauptgeschäftsstraße Berlins, konkret die Friedrichstraße zwischen dem gleichnamigen S-Bahnhof im Norden und dem Mehringplatz im Süden, hinsichtlich der dort zu erwartenden Videoüberwachungsmaßnahmen datenschutzrechtlich überprüft. Von besonderem Interesse waren für uns dabei solche Überwachungsanlagen, bei denen die Außenbereiche der Gebäude mit Hilfe von mehr oder weniger offensichtlich angebrachten Kameras beobachtet werden.

Nach § 6 Abs. 1 Nr. 2 BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen zulässig, soweit dies zur Wahrung des Hausrechts erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Da es den Kameras äußerlich nicht in jedem Fall anzusehen ist, ob sich der jeweils von ihnen erfasste Bildausschnitt auf den zulässigen Hausrechtsbereich beschränkt, haben wir in Zweifelsfällen vor Ort Kontrollen bei den verantwortlichen Betreibern der Überwachungsanlagen durchgeführt. Dabei haben wir mehrfach festgestellt, dass sich die Beobachtung über die Grundstücksgrenzen der verantwortlichen Stellen hinaus auch auf öffentliches Straßenland erstreckt. Begründet wurde dies mit der Erforderlichkeit zur Verhinderung bzw. Aufklärung von Straftaten und Vandalismusschäden (z. B. Graffitti, Scratching auf oder die totale Zerstörung von Schaufensterscheiben). Eine Ausrichtung der Kameras allein auf die Fassade sei dafür nicht ausreichend.

Diese Ausweitung des beobachteten Bereichs ist im privatwirtschaftlichen Bereich dann hinnehmbar, wenn es sich um hoch frequentiertes öffentliches Straßenland (z. B. Gehwege, Straßen und Plätze) handelt und das Terrain des Hausrechts nicht mehr als ca. einen Meter überschritten wird. Das Amtsgericht Berlin-Mitte hat sich dieser Auffassung in einem Urteil vom 18. Dezember 2003[110] angeschlossen. Das Gericht hat in seinem Urteil klar-

[110] JB 2002, 4.6.5; JB 2003, 4.6.4

gestellt, dass sich ein Grundstückseigentümer auch dann an diese Einschränkung zu halten hat, wenn sein Grundstück mit einer Widmung für die öffentliche Nutzung belastet ist.

Insgesamt konnten wir feststellen, dass sich das mutmaßliche Szenario einer flächendeckenden *Videoüberwachung* – jedenfalls in der Friedrichstraße – noch nicht bestätigt.

Im südlichen Teilbereich der *Friedrichstraße* ist – im Gegensatz zu den großen Stadtquartieren im Norden – eine kleinteilige Gebäudestruktur vorherrschend. An den einzelnen Gebäuden konnten wir hier – insbesondere südlich der Leipziger Straße – nur vereinzelt Videokameras an den Außenfassaden feststellen. Sofern diese auch auf Teile des öffentlichen Straßenlandes gerichtet waren, ergab die Überprüfung, dass sie sich ohne großen (materiellen und technischen) Aufwand so positionieren lassen, dass die Erfassung des Straßenlandes nach den oben genannten Kriterien gesetzeskonform erfolgt.

Das nördliche Teilstück der Friedrichstraße wird nahezu ausschließlich von großen Gebäudeblöcken in Form von Stadtquartieren dominiert. Die Gebäudeverwaltung und -sicherheit in diesen Quartieren wird zumeist zentral durch damit betraute Fachfirmen wahrgenommen. Sie setzen zur Überwachung des Gebäudes und der Außenanlagen, aber auch zur Kommunikation mit Besuchern von Mietern, Lieferanten usw., verstärkt Videokameras ein. Da sich diese Quartiere in der Regel von einer Querstraße der Friedrichstraße zur nächsten erstrecken, erfassen die an den Außenfassaden angebrachten Videoüberwachungsanlagen einen besonders großen Straßenabschnitt. Insbesondere auch diesem Umstand ist es geschuldet, dass sich Personen, die sich auf dem Weg von der Leipziger Straße bis zum S-Bahnhof befinden, wesentlich häufiger und länger im Blickfeld der Videokameras aufhalten müssen.

Wir haben die von uns festgestellten Videoüberwachungsmaßnahmen – je nach der mit ihnen verbundenen Eingriffsintensität in datenschutzrechtlich geschützte Bereiche – klassifiziert. Das Ergebnis ist anschaulich der nachfolgenden graphischen Darstellung der Friedrichstraße und der sie kreuzenden Querstraßen zu entnehmen.

0 keine Videoüberwachungsmaßnahmen

1 Videokameras in Klingeltableaus mit einer „Blickrichtung“ parallel zum Gehweg, wobei sich die Klingeltableaus in fast allen Fällen in Eingangsnischen befinden und somit die Beobachtung öffentlichen Straßenlandes nahezu ausgeschlossen ist

2 Videokameras in Klingeltableaus mit einer „Blickrichtung“ im rechten Winkel zum Gehweg, wodurch Passanten kurzzeitig in das Blickfeld der Kamera geraten können. Da bei diesen Anlagen die Kamera zumeist erst mit dem Betätigen der Klingel aktiviert wird, der Einlass Begehrende in der Regel das Bild ausfüllt und Aufzeichnungen nicht gefertigt werden, ist hier allenfalls die Einhaltung der Hinweispflicht nach § 6 b Abs. 2 BDSG zu fordern

3 Videokameras, mit denen die unmittelbaren Eingangsbereiche und gegebenenfalls der bereits erwähnte 1-m-Streifen öffentlichen Straßenlandes bzw. der Öffentlichkeit gewidmeten Grundstücks (fast ausschließlich Arkaden) erfasst werden, unabhängig davon, ob aufgezeichnet wird oder nicht

4 Videokameras, die bei unserer Kontrolle so ausgerichtet waren, dass öffentliches Straßenland bzw. ein der Öffentlichkeit gewidmetes Grundstück in unzulässiger Weise erfasst wurde

4.9 Informationsfreiheit

4.9.1 Endlich in Aussicht: ein Informationsfreiheitsgesetz des Bundes

Das in den vergangenen Jahren mehrmals ins Stocken geratene[111] Vorhaben für ein *Informationsfreiheitsgesetz des Bundes* hat wieder Fahrt aufgenommen. Diese erfreuliche Entwicklung geht auf eine Initiative der Regierungsfraktionen im Bundestag zurück, die zumindest den grundsätzlichen Widerstand einiger Bundesministerien gegen den Anspruch auf Informationszugang überwunden hat. Zugleich haben verschiedene Institutionen die öffentliche Debatte durch die Vorlage eines eigenen Gesetzentwurfs wiederbelebt und gemeinsam die Kampagne pro-information gestartet. Unvermittelt hatte auch das Bundesinnenministerium seinen eigenen Entwurf parat, der dem Entwurf der Regierungsfraktionen den Rang abzulaufen drohte. Diese Situation konnte innerparteilich nicht zuletzt mit dem Argument abgewendet werden, dass die Bundesregierung über geraume Zeit die Einführung von Informationsrechten für die Bürgerinnen und Bürger nicht betrieben hatte, so dass der Entwurf der Regierungsfraktionen zum Zug gekommen ist.

Die erste Lesung des Gesetzentwurfs[112] hat im Bundestag am Jahresende stattgefunden. Ohne Zweifel ist ein derartiges Gesetz auch für die Bundesebene sehr zu begrüßen. Allerdings bietet der Katalog von Ausnahmen ein viel zu breites Einfallstor, um Informationen zu verweigern.

4.9.2 Informationen als Nutzen für die Privatwirtschaft

Der öffentliche Sektor verfügt über Informationen, die häufig wirtschaftlich gut verwertbar sind. Auch um dem Interesse der Privatwirtschaft an der kommerziellen Nutzung entgegenzukommen, wurde bereits 2003 die Europäische Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors erlassen[113]. Sie schafft keine neuen Informationsrechte, sondern vereinheitlicht den Rechtsrahmen für die Umnutzung vorhandener Informationen durch Private für kommerzielle und nichtkommerzielle Zwecke. Die Mitgliedstaaten sind bis zum 1. Juli 2005 zur Angleichung ihrer Rechtsvorschriften verpflichtet. Insbesondere die Übernahme der Tarifgrundsätze der Richtlinie, nach denen die Gebühr kostenbasiert zuzüglich einer angemessenen Gewinnspanne berechnet wird, eröffnet den Mitgliedstaaten neue Einnahmequellen. Aus diesem Anlass hat die Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland (AGID), der außer uns die Informationsfreiheitsbeauftragten Brandenburgs, Nordrhein-Westfalens und Schleswig-Holsteins angehören, eine Entschließung verabschiedet[114].

111 JB 2003, 4.9.2

112 BT-Drs. 15/4493

113 2003/98/EG vom 17. November 2003

114 vom 3. Juni 2004: Kommerzielle Nutzung öffentlicher Informationen – keine Nachteile für Bürgerinnen und Bürger

Darin wird auch gefordert, dass bei der Umsetzung der Richtlinie nicht nur die Vorteile der Kommerzialisierung, sondern auch die Belange der Bürger berücksichtigt werden, indem die Kosten für den Informationszugang nicht abschreckend sein dürfen.

4.9.3 Weitere Entwicklungen für mehr Transparenz

Der Bundestag hat das Gesetz zur Neugestaltung des *Umweltinformationsgesetzes*[115] verabschiedet, das am 14. Februar 2005 in Kraft tritt. Damit wird die Richtlinie 2003/4/EG der Europäischen Gemeinschaft über den Zugang der Öffentlichkeit zu Umweltinformationen auf Bundesebene rechtzeitig umgesetzt. Vorgesehen ist ein voraussetzungsloser Anspruch auf freien Zugang zu Umweltinformationen, den die informationspflichtige Stelle in der Regel innerhalb eines Monats nach Antragstellung zu erfüllen hat. Abgesehen von den Bundesbehörden gehören zu den informationspflichtigen Stellen auch natürliche und juristische Personen des Privatrechts, soweit sie öffentliche Aufgaben wahrnehmen bzw. öffentliche Dienstleistungen erbringen und dabei vom Bund kontrolliert und beaufsichtigt werden. Ein weiteres Anliegen des Gesetzes ist die Verbreitung vorhandener Umweltinformationen durch die Nutzung von elektronischer Datenverarbeitung, die mittels elektronischer Kommunikation für die Öffentlichkeit auch abrufbar sind.

Auch die Bundesländer sind im Rahmen ihrer Zuständigkeit in der Umsetzungspflicht. Hierzu regt die Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland (AGID) in einer Entschließung[116] an, die Umweltinformationsgesetze der Länder mit den allgemeinen Informationsfreiheitsgesetzen zusammenzuführen. Übersichtliche Informationsrechte, die sich aus ein und demselben Gesetz ergeben, tragen zur Umsetzung transparenter Teilhaberechte der Bürgerinnen und Bürger bei.

Mit einer weiteren Entschließung forderte die AGID, dass der Grundsatz der *Öffentlichkeit von Sitzungen* für Entscheidungsgremien eingeführt wird[117]. Für die Transparenz staatlicher Entscheidungsfindung ist die Möglichkeit der Teilnahme an Sitzungen von Gremien, die oftmals mit erheblichen Entscheidungsbefugnissen ausgestattet sind, unverzichtbar. Dies schließt nicht aus, dass für bestimmte Bereiche oder im Einzelfall die Vertraulichkeit gewahrt wird. Als Vorbild dient der „Government in the Sunshine Act“ in den USA, wonach der Meinungsaustausch in behördlichen Kollegialsitzungen im Lichte der Öffentlichkeit durchzuführen ist.

115 BGBl. I 2004, S. 3704

116 vom 3. Juni 2004: „Verbesserter Zugang zu den Umweltinformationen durch die neue Richtlinie der Europäischen Union“, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2004“, S. 93

117 vom 22. November 2004, vgl. a.a.O., S. 94

Für die Vorstände von öffentlich-rechtlichen Anstalten und Trägern, wie z. B. der Deutschen Bundesbank oder der Krankenkassen, ist die *Offenlegung von Vorstandseinkommen* längst zur Normalität geworden. Wenn sich die Betätigung aus Pflichtbeiträgen oder Steuern speist, erscheint es selbstverständlich, dass auch über diesen Posten Rechenschaftspflichten der Vorstandsmitglieder bestehen. Diese Transparenz wird zunehmend für Gesellschaftsformen mit Anteilseignern diskutiert. Bei einer Anzahl von Unternehmen gehört der offene Umgang mit den Gehältern bereits zur Unternehmensphilosophie. In diese Richtung zielt auch die Empfehlung der von der Bundesregierung eingesetzten Regierungskommission Deutscher Corporate Governance Kodex, die Bezüge der einzelnen Vorstandsmitglieder im Jahresbericht offen zu legen. Mit dem auf börsennotierte Aktiengesellschaften zugeschnittenen Verhaltenskodex[118] wird für einen Bewusstseinswandel geworben. Dass nunmehr etwa die Hälfte der 30 im Deutschen Aktienindex (DAX) notierten Unternehmen ihre Vorstandsbezüge im Jahresbericht ausweisen wollen, ist nicht zuletzt dem Umstand geschuldet, dass sich die Bundesregierung eine gesetzliche Regelung vorbehalten hatte. Das Bundesjustizministerium hatte zwar stets auf das Prinzip der Freiwilligkeit gesetzt, andererseits aber ein Gesetz nicht ausgeschlossen, um ein Ende der Geheimhaltung zu erzwingen.

4.9.4 Informationsfreiheit im Land Berlin

In Berlin wird die Offenlegung von Bezügen der Spitzenmanager von landeseigenen Unternehmen gefordert. Die Fraktionen der SPD und der PDS fordern in ihrem Antrag „Transparenz im Umgang mit den landeseigenen Unternehmen“[119], dass der Senat die Empfehlungen des Deutschen Corporate Governance Kodex übernimmt und dass künftig die Höhe der Vergütung für Geschäftsführung, Vorstände und Aufsichtsgremien veröffentlicht wird. Wir haben gegen eine Offenlegungsklausel in den Verträgen mit den Führungskräften keine Bedenken.

Seit 2003 verfügt Berlin über ein *Verbraucherinformationsgesetz*[120]. Danach ist die Senatsverwaltung für Gesundheit, Soziales und Verbraucherschutz ermächtigt, die Öffentlichkeit über Rechtsverstöße bei Lebensmitteln und Bedarfsgegenständen aufzuklären. Allerdings steht den Verbraucherinnen und Verbrauchern kein eigener Informationsanspruch zu. Deshalb hat das Abgeordnetenhaus den Senat aufgefordert, einen Entwurf zur Fortentwicklung des Gesetzes vorzulegen, der den Verbraucherinnen und Verbrauchern selbst ein Recht auf Zugang zu den Informationen einräumt, die bei den Behörden über Produkte im Geltungsbereich des Gesetzes vorliegen[121].

118 in der Fassung vom 21. Mai 2003

119 Abghs.-Drs. 15/2846

120 Gesetz zur Information der Verbraucherinnen und Verbraucher im Lebensmittelverkehr im Land Berlin, GVBl., S. 174

121 vgl. Beschluss des Abgeordnetenhauses, Anhang 1, Abghs.-Drs. 15/2784

Für Amtshandlungen nach dem Berliner Informationsfreiheitsgesetz (IFG) können nach § 16 IFG *Gebühren* zwischen 10,23 € und 511,29 € erhoben werden[122]. Ausnahmsweise sind einfache mündliche Auskünfte gebührenfrei. Auch für die Ablehnung des Informationszugangs werden keine Gebühren erhoben. Nach wie vor bereitet den öffentlichen Stellen die Ermittlung der Gebühren Schwierigkeiten[123]. Unser beharrliches Bestreben, den Rahmengebührentatbestand nach bestimmten Kriterien zu staffeln, wird nunmehr auf der Basis eines konkreten Entwurfs fortgesetzt, der mit den Senatsverwaltungen für Inneres sowie Finanzen beraten wird. Die Gebührenstaffelung hat sich in den übrigen Bundesländern mit Informationsfreiheitsgesetzen und auch nach dem Umweltinformationsgesetz des Bundes bewährt.

Informationsanspruch gegenüber Berliner Klinikum

Eine Petentin begehrte den Informationszugang zu statistischen Angaben über den Krankenstand von Ärzten in einem Berliner Klinikum für das vergangene Jahr. Von dort wurde nach dem Grund der Anfrage zurückgefragt. Später wurde der Informationszugang mit der Begründung verweigert, das IFG beziehe sich hauptsächlich auf die persönlichen Daten der Petentin.

Darin lag bereits eine Verkennung des Geltungsbereichs des IFG, das der Allgemeinheit ein umfassendes Informationsrecht einräumt (§ 1 IFG). Nach § 3 Abs. 1 IFG hat jeder Mensch gegenüber den in § 2 genannten Stellen, zu denen auch *Krankenhausbetriebe* zählen, ein Recht auf Einsicht in oder Auskunft über den Inhalt der von der öffentlichen Stellen geführten Akten. Das Informationsrecht kann ohne Begründung geltend gemacht werden (§ 13 Abs. 1 IFG). Das Berliner Klinikum kann den Informationszugang nur bei Vorliegen eines der Tatbestände nach §§ 5 bis 12 IFG zulässig beschränken. Inzwischen wurde zugestanden, dass ein Einsichts- und Auskunftsrecht nach dem IFG grundsätzlich nicht infrage gestellt wird.

Einsicht in Protokoll über Polizeieinsatz

Ein Petent hatte die Einsichtnahme in das Protokoll über einen nächtlichen Polizeieinsatz in einer bestimmten Gaststätte beim Polizeipräsidenten in Berlin beantragt. Dem Antrag auf Akteneinsicht wurde zunächst nicht stattgegeben, da sich weder aus dem Antrag noch aus dem Zusammenhang das allgemeine Informationsinteresse ergab. Ohne konkreten Rückschluss, ob der Informationszugang zu diesem polizei-

122 Fünfundzwanzigste Verordnung zur Änderung der Verwaltungsgebührenordnung vom 7. Dezember 2001, GVBl., S. 632

123 JB 2001, 4.9

lichen Einsatzprotokoll vorrangig der Verfolgung des Gesetzeszwecks diene, könne die Zulässigkeit des Antrags nach § 14 Abs. 1 IFG nicht geprüft werden. Diese Auffassung wurde maßgeblich auf die „Ersten Hinweise" der Senatsverwaltung für Inneres zur Anwendung des IFG gestützt.

Das Informationsrecht wurde in § 3 Abs. 1 IFG als voraussetzungsloser Anspruch eines jeden Menschen ausgestaltet. Soweit in § 14 Abs. 1 Satz 2 IFG eine Prüfung des Antrags auf Zulässigkeit vorgesehen ist, kann in deren Rahmen ein Antrag in Verfolgung des Gesetzeszwecks zwanglos vermutet werden. Nach § 1 IFG ist es der Zweck des Gesetzes, durch ein umfassendes Informationsrecht die demokratische Meinungs- und Willensbildung zu fördern und eine Kontrolle des staatlichen Handelns zu ermöglichen. Dabei handelt der Einzelne, auch wenn er individuelle Motive verfolgt, grundsätzlich als Sachwalter der Allgemeinheit[124]. Der Antrag auf Akteneinsicht bedarf insgesamt keiner besonderen Begründung. Da die „Ersten Hinweise" zur Anwendung des IFG offenbar auch von der Senatsverwaltung für Inneres diesbezüglich als überholt angesehen wurden, hat der Petent schließlich eine Kopie des Einsatzprotokolls erhalten.

Einsicht in Erwerbsunterlagen zum Gemälde in einem städtischen Museum

Ein Petent hat bei einem Museum die Einsicht in die Erwerbsunterlagen zu einem bestimmten Gemälde beantragt, von dem er annahm, dass es vor 1965 zum Familieneigentum gehörte. Das Museum teilte mit, dass sich aus den vorliegenden Unterlagen keine Rückschlüsse auf Herkunft und Eigentumsverhältnisse ziehen lassen. Der Petent begehrte weiterhin die Akteneinsicht. Ihm wurde für diesen Fall eine Gebühr von 150,– bis 200,– € in Aussicht gestellt.

Nach § 3 Abs. 1 IFG ist das Informationsrecht als Wahlrecht zwischen Akteneinsicht und Aktenauskunft ausgestaltet. Dieses Wahlrecht wird missachtet, wenn die öffentliche Stelle die Akten selbst sichtet und die Relevanz für das Interesse des Antragstellers bestimmt. Daran ändert auch der Umstand nichts, dass sich aus dem Zusammenhang die konkrete Fragestellung des Antragstellers ergab. Die Ankündigung der voraussichtlich für die Akteneinsicht oder Aktenauskunft anfallenden Gebühr soll zum frühestmöglichen Zeitpunkt erfolgen, wobei die Gebühren nach einem Urteil des EuGH[125] nicht prohibitiv, also für den Bürger abschreckend, wirken dürfen. Aufgrund unserer Intervention wurde dem Petenten die Einsicht gewährt. Die am Ende tatsächlich geforderten Gebühren betrugen nur 43,47 €, also nur ein Viertel der ursprünglich in Aussicht gestellten Gebühr.

[124] JB 2001, 4.9

[125] vom 9. September 1999, in: NVwZ 1999, S. 1209, 1211

Einsichtsbegehren eines Strafgefangenen

Die Senatsverwaltung für Gesundheit, Soziales und Verbraucherschutz hat mit der Medienanstalt Berlin-Brandenburg (MABB) eine Rahmenvereinbarung über die sozialverträgliche Umstellung der analogen Fernsehübertragung auf die digitale geschlossen. Ein Strafgefangener beantragte bei der Senatsverwaltung erfolglos die Einsicht in die Rahmenvereinbarung. Sie verwies ihn an die zuständige Senatsverwaltung für Justiz, da man sein Gesamtanliegen für aussichtslos hielt. Die MABB hatte sein bei ihr gestelltes Akteneinsichtsbegehren direkt an die Senatsverwaltung für Justiz weitergeleitet.

Im Unterschied zu den im letzten Jahr dargestellten Fällen[126], bei denen die Anwendung des IFG im *Strafvollzug* von der Senatsverwaltung für Justiz unter Hinweis auf den allein maßgeblichen § 185 StVollzG verneint worden war, wurde hier dem Einsichtsbegehren durch die Senatsverwaltung für Gesundheit, Soziales und Verbraucherschutz stattgegeben. Allerdings war die Weiterverweisung an die „zuständige" Senatsverwaltung für Justiz nicht sachgerecht. Grundsätzlich darf die öffentliche Stelle, bei der die Unterlagen vorliegen, nicht an ein anderes Fachressort verweisen (§ 13 Abs. 1 IFG). Selbst wenn das Gesamtanliegen den Umständen nach keinen Erfolg verspricht und es bereits in anderer Zuständigkeit bearbeitet wird, kann das Akteneinsichtsbegehren nicht mit dieser Begründung abgeschlossen werden.

Mit unserer Hilfe konnte das Akteneinsichtsbegehren des Petenten durchgesetzt werden.

Das Asbestgutachten: Etappensieger durch Weiterleitung

Eine Petentin bemüht sich seit März 2002 um die Akteneinsicht in ein Gutachten zur Asbestbelastung für ein Institutsgebäude einer Berliner Universität. Nach einem Jahr wurde ihr mitgeteilt, dass die Universität nicht über dieses Gutachten verfügt. Die Petentin wurde an die auftraggebende Senatsverwaltung für Stadtentwicklung verwiesen. Die Senatsverwaltung hat den daraufhin bei ihr gestellten Antrag an das betreffende Institut der Universität weitergeleitet, dem die Unterlagen auch nicht vorlagen. Nach zweieinhalb Jahren war wieder die Abteilung befasst, die schon den Ausgangsantrag bearbeitet hatte. In der Zwischenzeit war das Gutachten von der Senatsverwaltung an die Universität übermittelt worden. Dort entschloss man sich zur Übergabe an die Unfallkasse Berlin.

Die Verpflichtung einer unzuständigen Stelle zur Weiterleitung an die zuständige Stelle nach § 13 I IFG wird oft übersehen. Die Zuständigkeit richtet sich danach, bei welcher Behörde die Akten geführt werden. Hier bestand

[126] JB 2003, 4.9.3

die Besonderheit, dass die Weiterleitung mehrfach gerade nicht an die zuständige Stelle erfolgte. Erschwerend trat hinzu, dass keine Stelle der Petentin eine verbindliche Information über das Vorhandensein des *Gutachtens* gegeben hat. Schließlich verstieß die Weitergabe des Gutachtens an die Unfallkasse dann gegen das IFG, wenn der Akteneinsichtsantrag bereits vorlag und diese Maßnahme gerade deswegen ergriffen wurde. Die Petentin beabsichtigt nun, den Informationszugang bei der Unfallkasse zu beantragen.

Informationszugang zum Terminkalender des Regierenden Bürgermeisters

Ein Petent beantragte nach dem IFG Einsicht in den Terminkalender des Regierenden Bürgermeisters für einen in der Vergangenheit liegenden Zeitraum von drei Monaten. Diesen Antrag hat er ausdrücklich auf solche Termine beschränkt, die in seiner Eigenschaft als Amtsträger als Regierender Bürgermeister wahrgenommen wurden. Die Senatskanzlei hat den Antrag im Wesentlichen mit der Begründung abgelehnt, dass der Terminkalender keine Akte im Sinne von § 3 Abs. 2 IFG sei. Der Petent hat hiergegen Klage beim Verwaltungsgericht erhoben.

Die Aktenqualität des amtlichen *Terminkalenders* ergibt sich ohne weiteres aus § 3 Abs. 2 IFG, denn es handelt sich um eine schriftliche Gedankenverkörperung, die amtlichen Zwecken dient. Insbesondere wird der Terminkalender zu dem amtlichen Zweck geführt, den Tagesablauf des *Regierenden Bürgermeisters* für die Wahrnehmung amtlicher Termine zu koordinieren. Der eindeutige Gesetzeswortlaut steht einer auf die Wahrnehmung von Verwaltungsaufgaben einschränkenden Auslegung des Aktenbegriffs entgegen. Im Übrigen ist nach dem in § 1 IFG statuierten Gesetzeszweck ein umfassendes Informationsrecht über das in Akten festgehaltene Wissen und Handeln öffentlicher Stellen vorgesehen. Dieses Recht kann nur aufgrund der in §§ 6 bis 11 IFG normierten Ausnahmen eingeschränkt werden. Das Informationszugangsbegehren war von vornherein auf amtliche Termine in der Funktion als Regierender Bürgermeister beschränkt. Für die Einschränkung des Informationszugangs zum Schutz personenbezogener Daten sieht § 6 Abs. 1 IFG eine Abwägung zwischen dem Informationsinteresse (§ 1 IFG) und dem Interesse der Betroffenen an der Geheimhaltung vor. Bei einem überwiegenden Informationsinteresse hindert die Offenbarung personenbezogener Daten nicht den Informationszugang. Nach § 6 Abs. 2 Satz 1 Nr. 2 IFG stellt die Mitwirkung eines bestimmten Amtsträgers an einem Verwaltungsvorgang ohnehin einen Regelfall für die zulässige Offenbarung personenbezogener Daten dar. Daraus folgt zugleich, dass über im Kalender genannte Termine dann nicht informiert werden muss, wenn sie keinem Verwaltungsvorgang zuzuordnen sind.

5. Telekommunikation und Medien

5.1 Telekommunikationsdienste

Neuer Telekommunikationsdatenschutz in Kraft

Bereits in unserem letzten Jahresbericht hatten wir uns ausführlich mit dem umstrittenen Gesetzentwurf der Bundesregierung für ein neues *Telekommunikationsgesetz* (TKG) befasst[127]. Nach Abschluss der Beratungen im parlamentarischen Verfahren und der Einigung im Vermittlungsausschuss konnte das TKG nunmehr am 26. Juni 2004 in Kraft treten[128]. Im Zuge der durch den neuen europäischen Rechtsrahmen[129] ausgelösten Novelle wurde ein eigener, abschließender Datenschutzteil im TKG geschaffen. Durch dieses Konzept einer einheitlichen gesetzlichen Regelung im TKG (§§ 91 – 107) konnte die bislang parallel geltende Telekommunikations-Datenschutzverordnung (TDSV) aufgehoben werden.

Die Datenschutzvorschriften des TKG dienen dem Schutz personenbezogener Daten der Teilnehmer und Nutzer von Telekommunikation bei der Erhebung und Verwendung dieser Daten durch Personen und Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an deren Erbringung mitwirken. Die §§ 91 ff. TKG gelten grundsätzlich auch für geschlossene Benutzergruppen öffentlicher Stellen (Behördennetze). Soweit diese von öffentlichen Stellen der Länder betrieben werden, finden ergänzend die jeweiligen Landesdatenschutzgesetze, in Berlin also das Berliner Datenschutzgesetz, Anwendung.

Direktmarketing ohne vorherige Einwilligung

Eine Neuregelung hat der zulässige Umgang mit Kundendaten zu Werbezwecken erfahren. Telekommunikationsanbieter dürfen Bestandsdaten, d. h. im Rahmen der Vertragsverhältnisse anfallende Daten ihrer Kunden, wie bisher zur Beratung, zur Werbung für eigene Angebote und zur Marktforschung grundsätzlich nur verwenden, soweit dies für diese Zwecke erforderlich ist und der Kunde eingewilligt hat (Opt-in-Lösung). Diese Regelung gilt zunächst für sämtliche Übermittlungsformen, wie Telefon, Telefax, E-Mail, SMS oder MMS. Der Grundsatz wird aber entscheidend eingeschränkt, soweit es sich nicht um Telefonwerbung handelt und der Diensteanbieter im

127 JB 2003, 5.1

128 BGBl. I, S. 1190

129 vgl. die für den Datenschutz relevante Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. EG L 201/37; auch JB 2002, 5.1

Rahmen einer bestehenden Kundenbeziehung rechtmäßig Kenntnis von der Rufnummer oder der (elektronischen) Postadresse des Teilnehmers (Kunden) erhalten hat. Insoweit gilt nur das kundenunfreundlichere Opt-out-Prinzip. Das bedeutet, die Werbung ist so lange zulässig, bis der Teilnehmer der Verwendung seiner Daten zu diesen Zwecken widersprochen hat. Der Teilnehmer muss außerdem bei der Erhebung oder der erstmaligen Speicherung der Rufnummer oder (elektronischen) Adresse und bei jeder Versendung einer Nachricht an diese deutlich sichtbar und gut lesbar auf die Möglichkeit hingewiesen werden, dass er der Versendung weiterer Werbenachrichten jederzeit schriftlich oder elektronisch widersprechen kann[130].

Die neuen erweiterten Zulässigkeitsgrenzen in § 95 Abs. 2 stellen – trotz Abweichungen im Wortlaut – inhaltlich das datenschutzrechtliche Pendant zu den Regelungen in § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG) dar, welche seit dem 4. Juli 2004 in Kraft sind[131]. Das neue Wettbewerbsrecht hatten wir bereits im letzten Jahresbericht im Rahmen des Schwerpunktthemas zur elektronischen Werbung vorgestellt[132].

Im Gegensatz zum Telekommunikationsrecht hat der Bereich der Teledienste im Zuge der Umsetzung der Vorgaben aus Art. 13 der EG-Datenschutzrichtlinie für elektronische Kommunikation keine Neuregelung erfahren. Im einschlägigen Teledienstedatenschutzgesetz (TDDSG) ist deshalb nach wie vor keine Privilegierung für die Direktwerbung gegenüber den eigenen Kunden vorgesehen. Da die werbliche Nutzung der Vertragsdaten auch nicht durch den zugrunde liegenden Vertrag legitimiert wird, bedarf es wie bisher einer ausdrücklichen Erlaubnis in Form einer Einwilligung durch den Nutzer. Auf das UWG können sich die Anbieter von Telediensten insoweit nicht berufen, da das Wettbewerbsrecht keine datenschutzrechtlichen Erlaubnistatbestände enthält, sondern allein festlegt, in welchen Fällen eine unlautere Wettbewerbshandlung durch eine unzumutbare Belästigung anzunehmen ist oder nicht.

Verarbeitung von Standortdaten nur mit Einwilligung

Eine wesentliche Neuerung im TKG stellt die Vorschrift über *Standortdaten* in § 98 dar. Die Regelung setzt die europarechtlichen Vorgaben aus Art. 9 der Datenschutzrichtlinie für elektronische Kommunikation in deutsches Recht um und schafft die datenschutzrechtlichen Voraussetzungen für das Angebot standortbezogener Dienste (*„Location Based Services“*). Solche Dienste, die dem Nutzer in Abhängigkeit von seinem aktuellen Aufenthaltsort zur Verfügung gestellt werden, zählen zu den erfolgversprechendsten Applikationen im Mobilfunk. Ein zentraler Anwendungsbereich

130 ein Musterschreiben zur Ausübung des Widerspruchsrechts findet sich in unserem Internet-Angebot „Das Datenscheckheft online“ unter http://www.datenschutz-berlin.de/infomat/datensch/inhalt.htm

131 BGBl. I, S. 1414

132 JB 2003, 3.3

sind Informations- und Unterhaltungsdienste. Sie reichen von Hinweisen auf nächstgelegene Restaurants, Einkaufsmöglichkeiten, Kinos, Geldautomaten, Tankstellen oder freie Parkplätzen über standortbezogene Verkehrsinformationen und Fahrplanauskünfte bis hin zu lokalen Wettervorhersagen. Neuere Anwendungen dienen der Ortung und Verfolgung von Personen, insbesondere von Kindern durch ihre Eltern. Aus Sicht des Datenschutzes ergeben sich hierbei erhebliche neue Risiken, etwa die Gefahr der Erstellung von umfassenden Bewegungsprofilen.

Nach dem jetzt geltenden Recht dürfen die Standortdaten nur in dem für die Bereitstellung dieser Dienste erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden. Zudem muss die Verarbeitung entweder anonym erfolgen oder der Teilnehmer muss zuvor über die Datenverarbeitung informiert werden und seine Einwilligung erteilt haben. Die Einwilligung ist dabei nicht vor jeder Inanspruchnahme eines Dienstes erforderlich, sondern kann auch im Rahmen des Vertrags über die Erbringung der Dienste oder einer Dienstegruppe mit dem Anbieter erfolgen. Wird das Mobilfunkgerät noch von weiteren Personen genutzt, muss der Teilnehmer diese von der erteilten Einwilligung in Kenntnis setzen. Dadurch soll die ungewollte Preisgabe von Standortdaten durch den jeweiligen Nutzer verhindert werden. Die neue Vorschrift sieht ferner vor, dass Teilnehmern, die ihre Einwilligung zur Verarbeitung von Standortdaten einmal erteilt haben, auch weiterhin die Möglichkeit eingeräumt werden muss, die Verarbeitung solcher Daten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise und unentgeltlich zeitweise zu untersagen. Die Datenschutzaufsichtsbehörden werden künftig verstärkt darauf achten, wie die neuen datenschutzrechtlichen Vorgaben von den Diensteanbietern technisch umgesetzt werden.

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation/International Working Group on Data Protection in Telecommunications (IWGDPT) hatte bereits auf ihrer 29. Sitzung am 15./16. Februar 2001 einen gemeinsamen Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten verabschiedet, in dem Forderungen für eine datenschutzgerechte Gestaltung solcher Dienstleistungen formuliert wurden[133]. Auf ihrer 36. Sitzung am 18./19. November 2004 hat die Arbeitsgruppe diese Stellungnahme ergänzt. In der überarbeiteten Fassung wird nunmehr eine Unterscheidung zwischen Teilnehmern, d. h. den Personen, die mit dem Anbieter einen Vertrag über die Erbringung der standortbezogenen Dienste geschlossen haben, und sonstigen Nutzern vorgenommen und für beide die jederzeitige Möglichkeit zur Unterdrückung der Verarbeitung von Standortinformationen auch nach bereits erteilter Einwilligung gefordert[134].

133 JB 2001, 5.1

134 Gemeinsamer Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten in der Fassung vom 18./19. November 2004, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2004“, S. 84

Rufnummer verrät Namen – die Inverssuche

Bisher erhielt man von der Telefonauskunft nur die Telefonnummer und die Adresse von Teilnehmern, wenn man diese namentlich kannte. Seit In-Kraft-Treten des neuen TKG geht es auch andersherum: Die Auskunft über Namen oder Namen und Anschrift eines Teilnehmers, von dem nur die Rufnummer bekannt ist. Eine solche *Inverssuche* ist allerdings nur erlaubt, wenn der Kunde im Telefonbuch oder einem öffentlichen elektronischen Kundenverzeichnis eingetragen ist und gegen die Inverssuche keinen Widerspruch eingelegt hat[135]. Auf dieses Widerspruchsrecht muss ihn sein Diensteanbieter hinweisen. Der Widerspruch kann jederzeit per Telefon, Brief oder Fax gegenüber dem Telekommunikationsunternehmen erklärt werden. Er muss auch von anderen Diensteanbietern beachtet werden.

Pflicht zur Vorratsdatenspeicherung vorerst abgewendet

Bis zuletzt war vom Bundesrat auf Antrag des Rechtsausschusses die Einführung einer gesetzlichen Pflicht der Anbieter zur sechsmonatigen *„Vorratsspeicherung“* aller Verkehrsdaten, d. h. der Rufnummern der beteiligten Anschlüsse sowie des Beginns und des Endes der jeweiligen Verbindung nach Datum und Uhrzeit, im TKG gefordert worden. Letztlich war dies jedoch im Vermittlungsausschuss nicht durchsetzbar. Die Regelung zur Höchstspeicherfrist von sechs Monaten ist weiter als „Kann“-Bestimmung ausgestaltet. Damit wurde den Bedenken der Datenschutzbeauftragten des Bundes und der Länder Rechnung getragen, die eine vorsorgliche Speicherung von Daten ohne konkreten Anlass für künftige Strafverfolgungsmaßnahmen wiederholt als verfassungswidrig abgelehnt hatten[136].

Wie lange die klare Entscheidung des deutschen Gesetzgebers gegen eine Datenspeicherung auf Vorrat Bestand haben wird, ist allerdings fraglich, seit auf europäischer Ebene eine erneute Initiative zur Ausweitung der Überwachungsmöglichkeiten im Telekommunikationsbereich gestartet wurde. Auf der Ratstagung für Justiz und Inneres im April 2004 haben die vier EU-Mitgliedstaaten Frankreich, Irland, Schweden und Großbritannien den Entwurf eines Rahmenbeschlusses des EU-Rates vorgelegt, wonach alle Anbieter von Telekommunikations- und Internetdiensten in den EU-Mitgliedstaaten zur pauschalen Speicherung sämtlicher Daten über Nutzende dieser Dienste für einen Zeitraum von mindestens einem Jahr verpflichtet werden können[137].

135 ein Musterschreiben zur Ausübung des Widerspruchsrechts findet sich in unserem Internet-Angebot „Das Datenscheckheft online“ unter http://www.datenschutz-berlin.de/infomat/datensch/inhalt.htm

136 JB 2002, 5.1; JB 2003, 5.1

137 vgl. Entwurf eines Rahmenbeschlusses des Rates der Europäischen Union über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten einschließlich Terrorismus vom 28. April 2004 in der überarbeiteten Fassung vom 14. Oktober 2004

Dies solle der Zusammenarbeit im Bereich der Strafverfolgung und der Terrorismusbekämpfung dienen. Von dem Beschlussentwurf erfasst werden alle Verkehrsdaten der klassischen Telekommunikation im Fest- und Mobilfunk einschließlich der dazugehörigen Messaging-Dienste, ebenso aber auch Standortdaten, die Grundlage für die Erbringung so genannter Location Based Services sind. Im Bereich des Internets sind unter anderem Internet-Protokolle einschließlich E-Mail, WWW und Protokolle für die Sprachübermittlung betroffen. Derzeit berät eine Arbeitsgruppe des Rates den Vorschlag unter den Aspekten Verhältnismäßigkeit, Schutz der Grundrechte und Kosten für die Dienstleister, um eine konkrete Liste der betroffenen Verkehrsdaten aufzustellen.

Die Datenschutzbeauftragten des Bundes und der Länder haben in einer gemeinsamen Presseerklärung die Bundesregierung aufgefordert, den vorliegenden Entwurf abzulehnen[138]. Sie weisen in ihrer Kritik darauf hin, dass das grundgesetzlich garantierte Fernmeldegeheimnis eine Speicherung von Daten über die Nutzung öffentlicher Telekommunikationsnetze außer für betriebliche Zwecke nur zulässt, wenn ein konkreter Verdacht für eine Straftat von erheblicher Bedeutung besteht. Zudem würde eine flächendeckende Vorratsspeicherung von Kommunikationsdaten auch die Grundrechte auf freie Meinungsäußerung und auf ungehinderte Unterrichtung aus allgemein zugänglichen Quellen verletzen. Schließlich bestehen aus Sicht der Datenschützer erhebliche Zweifel daran, ob der Rahmenbeschluss mit Artikel 8 der Europäischen Menschenrechtskonvention („Recht auf Achtung des Privatlebens und der Korrespondenz“) vereinbar wäre. Auch zur Bekämpfung des Terrorismus können nur solche Maßnahmen beschlossen werden, die in einer demokratischen Gesellschaft notwendig sind und dem Verhältnismäßigkeitsgrundsatz entsprechen. Unter Hinweis auf den Rechtsrahmen der Europäischen Menschrechtsrechtskonvention hat auch die Art. 29-Datenschutzgruppe den vorliegenden Entwurf für nicht akzeptabel erklärt und den EU-Ministerrat zur Ablehnung aufgefordert[139].

Der Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder hat seine rechtlichen Bedenken gegen die Einführung einer Vorratsspeicherung von Verkehrsdaten in einer schriftlichen Stellungnahme im Rahmen eines von den Generaldirektionen für die Informationsgesellschaft sowie für Justiz und Inneres der EU-Kommission durchgeführten Konsultationsverfahrens ausführlich dargelegt. Er weist insbesondere darauf hin, dass dem Gesetzgeber mildere und grundrechtsschonendere Mittel zur Verfügung stehen, die eine Speicherung von Verkehrsdaten auf einen konkreten Tatverdacht beschränken und nicht präventiv für eine mögliche zukünftige Strafverfolgung vorsehen. Die notwendigen Instrumente sind bereits in der Konvention des Europarates zur Bekämpfung der Datennetzkriminalität

138 Gemeinsame Presseerklärung zum Entwurf eines Rahmenbeschlusses der Europäischen Union zur Vorratsspeicherung aller Daten über die Nutzung der Telekommunikation und des Internets vom 25. Juni 2004

139 vgl. Stellungnahme 9/2004 vom 9. November 2004 (WP 99)

(Cybercrime-Convention) enthalten, aber in zahlreichen Unterzeichnerstaaten – auch in Deutschland – noch nicht umgesetzt worden[140].

Identifikationspflicht beim Erwerb von Prepaid-Produkten

Nicht durchsetzen konnten sich die Datenschutzbeauftragten mit ihrer Forderung auf eine Verpflichtung der Telekommunikationsunternehmen, auf die Erhebung und Speicherung von Kundendaten (unter anderem Name, Anschrift und Geburtsdatum), soweit diese für betriebliche Zwecke nicht erforderlich sind, zu verzichten. Die in § 111 TKG festgeschriebene Pflicht zur Vorhaltung der Daten für Auskunftsersuchen der Sicherheitsbehörden trifft alle Anbieter, die geschäftsmäßig Telekommunikationsdienste erbringen und dabei Rufnummern vergeben oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern bereitstellen. Eine Ausnahmeregelung für *Prepaid-Produkte* (z. B. vorbezahlte Mobilfunkkarten) wurde nicht getroffen. Damit ist im Ergebnis eine anonyme Nutzungsmöglichkeit im Bereich der Telekommunikation nicht mehr möglich. Dies widerspricht zentralen datenschutzrechtlichen Grundsätzen. Die Hintergründe zu dieser Neuregelung hatten wir bereits im letzten Jahresbericht erläutert[141].

Zugriff auf PIN, PUK und Passwörter erleichtert

Die Regelung zur manuellen Auskunft über Kundendaten an Strafverfolgungs- und Sicherheitsbehörden wurde dahingehend erweitert, dass nunmehr auch Auskünfte über solche Daten zu erteilen sind, mittels derer der Zugriff auf Endgeräte oder in diesen oder im Netz eingesetzte Speichereinrichtungen geschützt wird (z. B. *PIN*, *PUK* oder *Passwörter*). Basis hierfür können Auskunftsersuchen nach § 161 Abs. 1 Satz 1, § 163 Abs. 1 der Strafprozessordnung (Pflicht zur Zeugenaussage), die Datenerhebungsvorschriften der Polizeigesetze des Bundes oder der Länder zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder entsprechende Regelungen aus dem Bereich des Verfassungsschutzes, des Bundesnachrichtendienstes und des militärischen Abschirmdienstes sein. Den Kunden gegenüber muss der Diensteanbieter über eine derartige Auskunftserteilung Stillschweigen wahren. Aus Sicht des Datenschutzes ist diese Neuregelung inakzeptabel. Es ist nicht nachvollziehbar, weshalb der Zugriff etwa auf Passwörter unter derart leichten Bedingungen möglich sein soll, wenn auf die dahinter liegenden vom Fernmeldegeheimnis geschützten Angaben nur unter den Voraussetzungen der §§ 100 a ff. StPO, d. h. auf der Grundlage einer richterlichen Anordnung, zugegriffen werden darf.

[140] bereits JB 2000, 5.1

[141] JB 2003, 5.1

Datenschutzgerechter Einsatz von Fotohandys

Die IWGDPT hat sich auf ihrer 35. Sitzung am 14./15. April 2004 mit dem Datenschutz bei der Verarbeitung von Bildern und Tönen in Multimedia Messaging Services (*MMS*) befasst. Vor dem Hintergrund der leichten Handhabbarkeit und der verdeckten Einsatzmöglichkeiten der neuen Generation von *Fotohandys* empfiehlt die Arbeitsgruppe eine Verbesserung der Aufklärung und Unterrichtung der Nutzer über den datenschutzgerechten Umgang sowie die Implementierung von technischen Vorkehrungen, die die Betroffenen auf den Gebrauch der neuen Funktionen aufmerksam machen. Mögliche Mittel zur Erreichung dieses Ziels könnten ein Tonsignal sein, das ausgelöst wird, wenn die Fotografierfunktion in Betrieb ist, sowie die Entwicklung von Technologien, die es erlauben, die Fotografierfunktion in gekennzeichneten Bereichen („sicherer Hafen“, z. B. Fitnesscenter, Schwimmbäder) abzuschalten[142].

5.2 Teledienste

Telemediengesetz in Vorbereitung

Bund und Länder haben sich im November 2004 auf Eckpunkte zur Fortentwicklung der Medienordnung verständigt. Ein wesentliches Anliegen ist die Zusammenführung der materiellen Datenschutzregelungen für Tele- und Mediendienste in einem zukünftigen *Telemediengesetz* des Bundes[143]. Noch offen ist, ob mit der Neuordnung auch eine Änderung der Aufsichtsstruktur zugunsten einer Selbstkontrolle der Wirtschaft einhergehen soll, die die staatliche Kontrolle teilweise ersetzt. Die Länder wollen zeitgleich den Rundfunkdatenschutz an die neuen Regelungen im Bereich der Telemedien anpassen. Der bisherige Mediendienste-Staatsvertrag soll abgelöst werden, noch erforderliche Regelungsmaterien sollen in den allgemeinen Rundfunkstaatsvertrag übernommen werden. Eine Bund-Länder-Arbeitsgruppe unter Einbeziehung von Vertretern der Datenschutzbeauftragten des Bundes und der Länder wurde beauftragt, entsprechende Gesetzentwürfe zu erarbeiten, die eine politische Beschlussfassung bis Mitte des Jahres 2005 ermöglichen.

Speicherung von IP-Adressen zu Zwecken der Datensicherheit

Ein Petent bat uns in seiner Eingabe um die datenschutzrechtliche Überprüfung der Speicherung personenbezogener Daten bei der Nut-

[142] Arbeitspapier zu Datenschutz bei der Verarbeitung von Bildern und Tönen in Multimedia Messaging Services vom 14./15. April 2004, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2004“, S. 71

[143] zu den bisherigen Plänen für ein Elektronische-Medien-Datenschutzgesetz (EMDSG) bereits JB 2003, 5.1

zung eines Online-Angebots (Informationsportal und Internet-Chat). Der Diensteanbieter lässt im Auftrag HTTP-Logfiles im Format der Standard-Server-Konfiguration der Apache Software mit vollständigen IP-Adressen der anfragenden Nutzer über mehrere Monate speichern. Die Speicherung dient der Kontrolle, Analyse und Nachverfolgung unberechtigter Nutzungsvorgänge. IP-Adressen von potenziellen Störern und Angreifern werden im Rahmen einer Anzeige an die zuständigen Strafverfolgungsbehörden weitergegeben, wo die weiteren Ermittlungen betrieben werden.

IP-Adressen haben eine zentrale Bedeutung für die Funktion des Internets. Sie dienen der Übertragung der Daten zwischen dem Absender und dem Empfänger, d. h. der Weitervermittlung der zu übertragenden Datenpakete und Wegewahl (Routing) über das Internet. Jeder Rechner im Netz hat eine eindeutige *IP-Adresse*, die ihm vom Zugangsanbieter in der Regel nur für die Dauer einer Verbindung zugeteilt wird. Entgegen der Auffassung des Anbieters handelt es sich bei den von ihm gespeicherten IP-Adressen um personenbezogene Daten. Angesichts der vielfältigen Möglichkeiten, mit dem für einen Inhaltsanbieter regelmäßig zugänglichen Zusatzwissen und den verfügbaren Hilfsmitteln von einer IP-Adresse auf die dahinterstehende natürliche Person zu schließen, besteht sowohl für statische als auch für dynamisch (temporär) vergebene IP-Adressen zunächst die Vermutung des Personenbezugs. Diese Vermutung kann nur widerlegt werden, wenn der Diensteanbieter nachweist, dass in seinem konkreten Einzelfall eine Zuordnung zur Person des Nutzers nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, etwa indem er besondere technische oder organisatorische Schutzvorkehrungen getroffen hat, IP-Adressen nur gekürzt speichert oder allein zu statistischen Zwecken auswertet. Diese Voraussetzungen waren vorliegend nicht gegeben. Zum einen werden im Rahmen der Inanspruchnahme des Internet-Angebots verschiedentlich persönliche Daten (Name, E-Mail-Adresse) über Webformulare abgefragt, so dass sich die Nutzer in diesen Fällen gegenüber dem Anbieter eindeutig identifizieren und eine Verknüpfung mit der IP-Adresse ohne Probleme möglich ist. Zum anderen werden IP-Adressen im Falle eines Angriffs oder Missbrauchs an die zuständigen Strafverfolgungsbehörden im Rahmen einer Anzeige weitergegeben. Ein solches Vorgehen zielt gerade auf die Herstellung des Personenbezugs zur Ermittlung der Identität eines potenziellen Täters ab. Da eine Trennung zwischen den personenbeziehbaren IP-Adressen und solchen ohne Personenbezug bei der Protokollierung nicht durchgeführt wird und auch nicht sinnvoll durchführbar ist, müssen in der Konsequenz alle IP-Adressen so behandelt werden, als wären sie personenbezogene Daten.

Wir haben eine kurzfristige Speicherung und Auswertung der IP-Adressen unter dem Gesichtspunkt der Gewährleistung der Datensicherheit in der IT-Infrastruktur für zulässig erachtet. Die gesetzliche Ermächtigung hierfür ergibt sich mangels besonderer Regelungen in dem für das Online-Angebot einschlägigen Teledienstedatenschutzgesetz (TDDSG) aus § 9 BDSG. § 1 Abs. 2 TDDSG stellt eindeutig klar, dass das BDSG im Anwendungsbereich

des TDDSG jedenfalls subsidiär zur Anwendung kommen kann, wenn keine abschließende Spezialregelung vorliegt. Nach § 9 BDSG haben Daten verarbeitende Stellen die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführungen der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu § 9 genannten Anforderungen zu gewährleisten. Die Speicherung von Logfiles einschließlich der IP-Adressen stellt insoweit ein geeignetes Mittel zur Erreichung der Sicherheits- und Schutzziele des § 9 BDSG und seiner Anlage dar, als sie insbesondere zur Einrichtung einer wirksamen Zugangs- und Zugriffskontrolle nach den Nummern 2 und 3 der Anlage zu § 9 BDSG, aber auch für die Analyse und Nachverfolgung vergangener Angriffe und anderer Unregelmäßigkeiten (Portscans, Trojaneraktivitäten, Hacker-Attacken, DoS-Angriffe usw.) zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung objektiv erforderlich ist. Dabei muss allerdings verlangt werden, dass die verantwortliche Stelle auf der Grundlage einer Bedrohungsanalyse ein konkretes Datensicherheitskonzept entwickelt, aus dem sich die Unabdingbarkeit der Speicherung und Auswertung von IP-Adressen zur Erkennung und Beseitigung von Missbrauchs- und Angriffssituationen eindeutig ergibt. Zudem ist die Speicherung auf den hierfür unbedingt notwendigen Zeitraum zu begrenzen. Nur so kann den zentralen Zielen des Datenschutzrechts, nämlich Datenvermeidung und Datensparsamkeit, ausreichend Rechnung getragen werden. Diesen Anforderungen ist der Anbieter nachgekommen. Er hat überzeugend vorgetragen, dass ihm ein ebenso geeignetes oder sogar effektiveres Instrumentarium, das ohne die Speicherung von IP-Adressen auskommt, nicht zur Verfügung steht. Auch eine anlassbezogene Aktivierung der IP-Speicherung erst auf einen begründeten Verdacht hin und nur für eine verdächtige IP-Adresse ist nach seiner Aussage nicht realisierbar, da unerlaubte Eingriffe häufig nur punktuell erfolgten. Selbst wiederholte Angriffe (z. B. DoS-Attacken) könnten erst aufgrund der erfassten IP-Adressen als solche erkannt werden. Der von uns verlangten Begrenzung der Speicherdauer auf maximal *vier Tage* wurde entsprochen. Ferner wurde der gesetzlichen Forderung nachgekommen, die Nutzer bei Beginn des Nutzungsvorgangs über die Tatsache der Speicherung und die vorgesehene Dauer der Speicherung zu informieren.

Die Weitergabe der verdächtigen IP-Adressen an die Strafverfolgungsbehörden im Rahmen einer Anzeige ist gerechtfertigt. Die Diensteanbieter haben ein legitimes wirtschaftliches Interesse daran, Störungen und Angriffe nicht nur zu erkennen und gegebenenfalls zu beseitigen, sondern auch die Störer und Angreifer zur Verantwortung zu ziehen und damit zukünftigen Missbrauch zu verhindern. Die Übermittlung verstößt nicht gegen die strenge Zweckbindung nach § 31 BDSG. Danach dürfen personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, nur für diese Zwecke verwendet werden. Die Verwendung der Protokolldaten zum Nachweis im Rahmen der Rechtsverfolgung auf Initiative des Diensteanbieters wird von die-

sen Zwecken mit umfasst. Demgegenüber steht die Zweckbindung einer Herausgabe von Protokolldaten zur Verfolgung von Straftaten, die nicht im Zusammenhang mit der Datensicherheit stehen (z. B. unzulässige Inhalte), entgegen.

Einsatz von Spamfiltern und Virenscannern im Unternehmen

Im vergangenen Jahr sind vermehrt Unternehmen mit der Frage an uns herangetreten, ob der Arbeitgeber die an die Arbeitnehmer adressierten unerwünschten Werbe-E-Mails, so genannter Spams, und virenbehaftete E-Mails in jedem Fall zustellen muss oder ob er diese mit Hilfe von Filterprogrammen identifizieren und gegebenenfalls löschen darf.

Aus Sicht des Datenschutzes stellt sich hierbei die Frage nach einem Verstoß gegen das Fernmeldegeheimnis. Dabei ist zwischen dienstlicher und privater E-Mail-Kommunikation zu unterscheiden:

Gestattet der Arbeitgeber die *private E-Mail-Nutzung* am Arbeitsplatz – wozu er nicht verpflichtet ist –, wird er zum Anbieter von Telekommunikationsdiensten, da er die betrieblichen (elektronischen) Arbeitsmittel für fremde Zwecke zur Verfügung stellt[144]. Er unterliegt damit den Regelungen des TKG und ist gegenüber den Beschäftigten zum Schutz des Fernmeldegeheimnisses nach § 88 Abs. 1 TKG verpflichtet. Das Fernmeldegeheimnis umfasst nicht nur die Inhalte der Kommunikation, sondern auch ihre näheren Umstände. Es sind folglich sämtliche Verkehrsdaten, die Auskunft über die an der Kommunikation Beteiligten geben können, vor einer Preisgabe geschützt. Kenntnisse und Tatsachen, die dem Fernmeldegeheimnis unterliegen, dürfen nach § 88 Abs. 3 TKG grundsätzlich nur verwendet werden, soweit sie für die Zwecke der geschäftsmäßigen Erbringung der Dienste einschließlich des Schutzes der technischen Systeme auch erforderlich sind. Daraus ergibt sich, dass die Unternehmen aus Gründen der Datensicherheit zumindest virenbehaftete E-Mails oder solche, deren Anhänge ein Format aufweisen, das ausführbare Codes enthalten kann (z. B. Dateien mit den Erweiterungen *.exe, *.bat, *.com), nicht an die Arbeitnehmer zustellen müssen, sondern löschen können. Die Arbeitgeber können sich dabei insbesondere auf § 109 TKG berufen, der die Diensteanbieter sogar dazu verpflichtet, angemessene technische Vorkehrungen und sonstige Maßnahmen zum Schutz gegen unerlaubte Zugriffe und Störungen zu treffen. Die genaue Verfahrensweise ist den Beschäftigten jedoch vorher bekannt zu geben. Ferner sind die Beschäftigten in jedem Fall zu unterrichten, wenn an sie gerichtete E-Mails unterdrückt werden. Umgekehrt scheidet danach eine Rechtfertigung für die generelle Kontrolle der E-Mail-Inhalte etwa auf bestimmte Schlüsselwörter und die anschließende Löschung von vermeintlichen Spam-

[144] Je nach konkreter Ausgestaltung des Dienstes kann das Angebot des Arbeitgebers auch als Teledienst qualifiziert werden. Nutzungsdaten von Telediensten sind aber ebenfalls durch das Fernmeldegeheimnis geschützt, so dass sich in der rechtlichen Bewertung keine relevanten Unterschiede ergeben

Mails aus. Ein solches Vorgehen bleibt aber auf der Grundlage einer individuellen Einwilligung der Beschäftigten oder kollektiver betrieblicher Regelungen (Betriebsvereinbarungen) möglich, die die einschränkenden Voraussetzungen der privaten E-Mail-Nutzung formulieren und datenschutzkonforme Filtermechanismen präzise festlegen.

Gänzlich anders stellt sich die Rechtslage bei einem Verbot der privaten Nutzung in Bezug auf die rein dienstliche *E-Mail-Kommunikation* dar. In diesem Fall agiert der Arbeitgeber nicht als Anbieter von Telekommunikationsdiensten gegenüber seinen Beschäftigten und unterliegt insoweit nicht dem Fernmeldegeheimnis. Mit dem Eingang der dienstlichen E-Mail auf dem Mail-Server des Unternehmens ist der geschützte Telekommunikationsvorgang bereits beendet, da die E-Mail dem eigentlichen Adressaten, nämlich dem Arbeitgeber, vollständig zugestellt wurde. Wie bei herkömmlicher Dienstpost darf der Arbeitgeber jederzeit die Inhalte kontrollieren und Post ohne dienstlichen Bezug aussortieren und gegebenenfalls löschen. Damit ist auch der Einsatz von Spam-Filtern gerechtfertigt.

Veröffentlichung von Ergebnislisten durch Sportvereine im Internet

Die Arbeitsgruppe „Telekommunikation, Tele- und Mediendienste“ des „Düsseldorfer Kreises“ hatte sich mit einer Anfrage des Deutschen Sportbundes zur datenschutzkonformen Veröffentlichung von Ergebnislisten und Mitgliederdaten im Internet zu befassen. Von Seiten der Vereine besteht ein großes Interesse daran, namensbezogene Ergebnisse von Sportveranstaltungen und Wettkämpfen ins Internet zu stellen, ohne jedes Mal die Einwilligung der betroffenen Teilnehmer einzuholen.

Die Arbeitsgruppe kam in weitgehender Anlehnung an ein vom Innenministerium Baden-Württemberg herausgegebenes Merkblatt zum *Datenschutz im Verein*[145] mehrheitlich zu folgender Bewertung:

– Name und Anschrift der Funktionsträger dürfen auf der Grundlage des § 28 Abs. 1 Satz 1 Nr. 2 BDSG im Internet veröffentlicht werden. Ein berechtigtes Interesse des Vereins oder Verbands ist insoweit anzuerkennen. Überwiegende schutzwürdige Belange der Betroffenen sind nicht ersichtlich. Häufig liegt es sogar im Eigeninteresse der Funktionsträger, sich als Verantwortliche ihres Vereins nach außen in der Öffentlichkeit zu präsentieren. Die Angabe der privaten Telefonnummer oder E-Mail-Adresse bleibt aber freiwillig. Ferner müssen die Betroffenen vorab über die Veröffentlichung informiert werden.

– Werden auf Vereinsebene Spielergebnisse, Mannschaftsaufstellungen und Ranglisten mit den Namen der Aktiven im Internet veröffentlicht,

[145] Merkblatt Innenministerium Baden-Württemberg: Datenschutz im Verein, Stand 9/2004

so bemisst sich die Zulässigkeit nach § 28 Abs. 1 Satz 11 Nr. 3 BDSG. Danach ist eine Verarbeitung personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn die Daten allgemein zugänglich sind, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt. Die von einem Verein oder Verband ausgerichteten Veranstaltungen sind in der Regel öffentlich. Die Namen der Aktiven werden im Rahmen der Veranstaltung öffentlich bekannt gegeben. Es handelt sich damit üblicherweise um allgemein zugängliche Daten. Die Vereine haben zudem ein berechtigtes Interesse daran, über Ergebnisse auch im Internet zu kommunizieren. Allerdings können die von der Veröffentlichung Betroffenen auch ein schutzwürdiges Interesse am Ausschluss der Verarbeitung haben. Dies gilt umso mehr, als Daten im Internet weltweit abrufbar sowie einfach und schnell zugänglich sind. Bei der im Rahmen der Prüfung des § 28 Abs. 1 Satz 1 Nr. 3 BDSG vorzunehmenden Interessenabwägung ist aber zu berücksichtigen, dass bei der Veröffentlichung reiner Ergebnislisten nur mit Namen, Vereinzugehörigkeit und in begründeten Ausnahmefällen dem Geburtsjahrgang keine Anhaltspunkte dafür ersichtlich sind, dass das schutzwürdige Interesse der Aktiven an einem Ausschluss der Veröffentlichung gegenüber dem berechtigten Interesse des Vereins *offensichtlich* überwiegt. Sollte dies aufgrund einer besonderen persönlichen Situation doch der Fall sein, steht dem Betroffenen die Möglichkeit eines Widerspruchs gegen die Veröffentlichung nach § 35 Abs. 5 BDSG zu. Diese Vorschrift bleibt insoweit unberührt. Ferner müssen die Betroffenen vorab umfassend über die Veröffentlichung ihrer Daten informiert werden.

– Will der Verein darüber hinaus weitere Informationen über seine Mitglieder (aktive und passive) im Internet veröffentlichen (z. B. Fotos oder Einzelheiten des Wettkampfverlaufs), scheidet § 28 Abs. 1 Satz 1 Nr. 3 BDSG als Rechtsgrundlage aus, so dass eine vorherige schriftliche Einwilligung der Betroffenen – bei Minderjährigen der Erziehungsberechtigten – erforderlich ist.

Internetbetrug durch „Phishing“

Im Jahr 2004 hat die Zahl betrügerischer E-Mails deutlich zugenommen. Sie täuschen Anfragen seriöser Herkunft vor, um an persönliche Daten wie Passwörter oder Kreditkarteninformationen zu gelangen. Betroffen vom „*Password Fishing*“ (kurz: „*Phishing*“) ist vor allem das Online-Banking. Die Täter gehen dabei folgendermaßen vor: Zunächst richten sie eine Webseite ein, die derjenigen der betreffenden Bank täuschend ähnlich sieht. Dann werden deren Kunden in massenhaft versandten E-Mails, die vorgeblich ebenfalls von dieser Bank stammen, unter einem Vorwand (z. B. notwendige Aktualisierung von Datenbeständen) aufgefordert, einem in der

Mail enthaltenen Link zu folgen, der auf die gefälschte Kopie der Originalseite führt. Dort sollen die Kunden ihre Zugangsdaten, PIN oder TAN, eingeben. Tun sie dies, so erhalten die Täter Kenntnis von diesen Daten und können sie selbst einsetzen, um auf die Konten der Bankkunden zuzugreifen.

Die Betrüger nutzten dabei bekannte Schwachstellen von Browsern, die es ermöglichen, hinter einer URL eine Webseite zu verstecken, die die vertraulichen Daten entgegennimmt. Auch das URL-Spoofing und spezielle Javascripts sind häufig benutzte Verfahren. Aktuelle Software-Updates der Browser helfen, bereits genutzte Lücken zu schließen. Ferner ist eine besondere Sorgfalt der Nutzer beim Umgang mit ihren sensiblen Daten erforderlich. Diese verlangt allerdings eine umfassende Information der Öffentlichkeit.

Darauf hat auch die IWGDPT auf ihrer 36. Sitzung am 18./19. November 2004 in einem Arbeitspapier zum Thema Internetbetrug hingewiesen. Sie spricht sich für einen verstärkten Einsatz datenschutzfreundlicher Mittel und Verfahren zu dessen Bekämpfung aus[146].

5.3 Medien

Neues Verfahren bei der Rundfunkgebührenbefreiung aus sozialen Gründen

Aufgrund einer Änderung der Verordnung über die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht (*Rundfunkgebührenbefreiungsverordnung* – RGebBefrVO)[147] entscheidet in Berlin seit dem 1. Mai 2004 nach § 5 Abs. 2 RGebBefrVO der Rundfunk Berlin-Brandenburg (RBB) über die Anträge auf Befreiung von der Rundfunkgebührenpflicht aus sozialen Gründen. Die Träger der Sozialhilfe (bezirkliche Sozialämter) nehmen die Anträge lediglich entgegen, unterbreiten einen Entscheidungsvorschlag und sind ermächtigt, die Bescheide auszuhändigen. Bislang hatten in Berlin die Sozialämter in eigener Zuständigkeit über die Befreiung entschieden. Mit der Neuregelung des Verfahrens hat sich die zwischen uns und dem RBB strittige Frage, ob es eine ausreichende Rechtsgrundlage für die Übermittlung der Befreiungsgründe und weiterer Informationen von den Sozialbehörden an den RBB gibt, erledigt. Soweit nunmehr der RBB über die Gewährung der Befreiung selbst entscheidet, können die in zulässiger Weise bei den Sozialämtern erhobenen Daten auch an ihn weitergegeben

[146] Arbeitspapier zu Mitteln und Verfahren der datenschutzfreundlichen Bekämpfung des Internetbetrugs vom 18./19. November 2004, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2004“, S. 78

[147] Zweite Verordnung zur Änderung der Verordnung über die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht vom 16. März 2004, GVBl., S. 179

werden. Dies gilt unabhängig davon, ob die in § 5 Abs. 2 RGebBefrVO vorgesehene Aufgabenverteilung zwischen dem RBB und den Sozialämtern als Funktionsübertragung oder Datenverarbeitung im Auftrag qualifiziert wird. Selbst im Falle einer Funktionsübertragung wäre eine Datenübermittlung nach § 12 Abs. 1 Satz 2 BlnDSG zulässig.

Die Sozialämter ihrerseits müssen sich allerdings im Antragsverfahren damit begnügen, dass ihnen die Nachweise, mit denen der Antragsteller die Befreiungsvoraussetzungen glaubhaft macht (z. B. Einkommensnachweise, Mietverträge), vorgelegt werden. Die für die Prüfung der Befreiungsvoraussetzungen notwendigen Angaben können dann gesondert dokumentiert werden. Das Kopieren der Nachweise ist hingegen nur dann zulässig, wenn sämtliche zur konkreten Aufgabenerfüllung nicht erforderlichen personenbezogenen Daten, die in den Nachweisen enthalten sind, unkenntlich gemacht (geschwärzt) werden.

Beteiligung der Gebühreneinzugszentrale (GEZ) am Adresshandel

Bereits im letzten Jahr hatten wir über die Beteiligung der Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten (*GEZ*) am privaten *Adresshandel* berichtet[148]. Im Auftrag der Landesrundfunkanstalten, und damit auch des RBB, beschafft sich die GEZ ohne Wissen der betroffenen Bürger jährlich mehrere Millionen Adressdaten, die sie für flächendeckende „Direkt-Mailing-Aktionen“ nutzt. Nach einem Abgleich mit dem bei der GEZ geführten Datenbestand der Rundfunkteilnehmer werden nicht angemeldete Personen oder solche, die nur als Hörfunkteilnehmer gemeldet sind, angeschrieben und um Auskunft über das Bereithalten von Radio- und Fernsehgeräten gebeten.

Wir haben in der Vergangenheit gegenüber dem Rundfunk Berlin-Brandenburg mehrfach darauf hingewiesen, dass es in dem für öffentliche Stellen des Landes Berlin geltenden BlnDSG an einer erforderlichen Rechtsgrundlage für eine derartige Datenverarbeitung fehlt. Die Voraussetzungen des § 6 Abs. 1 Satz 2 BlnDSG sind nicht gegeben. Bei den gegen erhebliche finanzielle Leistungen beim kommerziellen Adresshandel angemieteten Datenbeständen handelt es sich nicht um offenkundige Daten, die für jedermann allgemein verfügbar wären. Die GEZ ist vielmehr bestrebt, selektierte und strukturierte Datenbestände zu erhalten, die über die reinen Adressangaben hinausgehen. So werden regelmäßig Informationen erhoben (z. B. Altersgruppe, Abonnenten einer Fernsehzeitschrift, Branchenangaben), die eine zielgruppengenaue Ansprache ermöglichen und in dieser Form gerade nicht ohne weiteres aus öffentlichen Registern oder sonst allgemein zugänglichen Quellen entnommen werden können. Aus diesem Grund kann auch nicht davon ausgegangen werden, dass schon wegen der Art der Daten schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden.

[148] JB 2003, 5.2

Um die Beschaffung von Daten beim kommerziellen Adresshandel gesetzlich zu legitimieren, soll der *Rundfunkgebührenstaatsvertrag* jetzt um eine Befugnis erweitert werden, nach der die Rundfunkanstalten und in deren Auftrag die GEZ personenbezogene Daten in analoger Anwendung des § 28 BDSG unter den gleichen Bedingungen verarbeiten dürfen wie privatwirtschaftliche Unternehmen. Eine entsprechende Änderung ist im Entwurf des 8. Rundfunkänderungsstaatsvertrags bereits vorgesehen, den die Ministerpräsidenten der Länder am 8. Oktober 2004 unterzeichnet haben. Dieses Vorhaben ist mit datenschutzrechtlichen Grundsätzen nicht zu vereinbaren. Darauf haben die für die Landesrundfunkanstalten zuständigen Datenschutzbeauftragten im Rahmen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder nachdrücklich hingewiesen[149]. Die Erhebung der Rundfunkgebühr stellt eine hoheitliche Aufgabe dar, die von den öffentlich-rechtlichen Rundfunkanstalten auch nur mit Mitteln des öffentlichen Rechts erfüllt werden kann. Den Rundfunkanstalten stehen hiefür bereits hoheitliche Befugnisse in ausreichendem Maße zur Verfügung. So wurde ihnen etwa von den Ländern das Recht zugestanden, im Falle der Anmeldung, der Abmeldung oder des Todes monatlich Einwohnerdaten aus den Melderegistern zu beziehen. Die Eröffnung des Zugriffs auf Datenbestände auch aus dem nicht-öffentlichen Bereich ist unverhältnismäßig. Zudem ist der Verweis auf § 28 BDSG verfehlt. Diese Vorschrift ist nur deswegen so weit gefasst, weil den nicht-öffentlichen Stellen als Normadressaten gerade keine hoheitlichen Befugnisse zustehen.

Wir haben in einer Stellungnahme gegenüber dem zuständigen Ausschuss für Europa- und Bundesangelegenheiten und Medienpolitik des Abgeordnetenhauses von Berlin unseren ablehnenden Standpunkt deutlich gemacht, gleichzeitig aber darauf hingewiesen, dass – sollte der politische Wille dahingehen, den Adressbezug gesetzlich zu gestatten – eine normenklare Erhebungsbefugnis unverzichtbar ist, die insbesondere die fundamentalen Prinzipien der Erforderlichkeit, der Zweckbindung und der frühzeitigen Löschung berücksichtigt, eine Rückübermittlung von Daten an den Adresshandel ausdrücklich verbietet und die Widerspruchsrechte der Betroffenen unberührt lässt.

Gemeinsame Prüfung der Gebühreneinzugszentrale

Im September 2004 haben wir zusammen mit den Landesbeauftragten für den Datenschutz der Länder Brandenburg, Bremen und Hessen bei der *GEZ* in Köln die Verarbeitung der beim Gebühreneinzug anfallenden personenbezogenen Daten überprüft. Schwerpunkte der dreitägigen Prüfung vor Ort waren die Organisation der Datensicherheit, der Umfang der Datenverarbeitung im aktiven Teilnehmerkonto, die Verarbeitung von Meldedaten, die

[149] Feststellung zur Beteiligung der GEZ am Adresshandel (8. Rundfunkänderungsstaatsvertrag) vom 28./29. Oktober 2004, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2004“, S. 17

Verarbeitung von Adressdaten aus dem privaten Adresshandel, das Löschungskonzept der GEZ, die Datenverarbeitung im Rahmen der Gebührenbefreiung, die länderübergreifenden Zugriffe der Rundfunkanstalten auf den Datenbestand der GEZ, die Datenverarbeitung durch die Gebührenbeauftragten und die Datenverarbeitung durch externe Dienstleister im Auftrag der GEZ. Über die Ergebnisse werden wir nach Fertigstellung des endgültigen Prüfberichts im nächsten Jahr berichten.

Redaktionsdatenschutz bei der Presse

Seit dem In-Kraft-Treten des novellierten Bundesdatenschutzgesetzes im Jahr 2001 und der Anpassung des Landespresserechts übt der *Deutsche Presserat* eine freiwillige Selbstkontrolle im Bereich des *Redaktionsdatenschutzes* aus. Der Gesetzgeber hat in Umsetzung der Vorgaben der EG-Datenschutzrichtlinie (Art. 9) zum Schutz der journalistischen Recherche und des Redaktionsgeheimnisses den redaktionellen Bereich der Presse weitgehend aus der Anwendung des BDSG herausgenommen und der staatlichen Aufsicht entzogen. Nur für die administrativ-wirtschaftliche Tätigkeit der Presseunternehmen (Verarbeitung von Abonnenten- und Arbeitnehmerdaten) gilt das BDSG uneingeschränkt.

Im Januar 2004 legte der Presserat erstmalig einen Tätigkeitsbericht zum Redaktionsdatenschutz vor. Darin werden die in den vergangenen zwei Jahren ergriffenen Maßnahmen dokumentiert. Der Presserat erweiterte z. B. den bestehenden Pressekodex im Hinblick auf den Datenschutz in Redaktionen um einige Regelungen und gab einen Leitfaden mit Empfehlungen für Verlage heraus. Anfang 2002 wurde ein zusätzlicher „Beschwerdeausschuss Redaktionsdatenschutz“ eingerichtet. Die dort behandelten Beschwerden und die Spruchpraxis dieses Ausschusses werden in dem Bericht ebenfalls beschrieben.

Der erste Bericht des Presserates zum Redaktionsdatenschutz zeigt in Teilbereichen einerseits positive Ansätze zu einer wirksamen Selbstregulierung und Selbstkontrolle. Andererseits macht er aber auch deutlich, wo die Grenzen der Tätigkeit des Presserates liegen. So hat sich zwar ein hoher Anteil an Zeitungs- und Zeitschriftenverlagen freiwillig der Kontrolle durch den Presserat unterworfen. Es gibt aber nach wie vor eine nennenswerte Zahl von Verlagen, die sich dieser Kontrolle nicht unterworfen haben. Hier besteht eine eklatante Schutzlücke. Zudem hat nur etwas mehr als die Hälfte der Verlage die im administrativen Bereich gesetzlich vorgeschriebenen betrieblichen Datenschutzbeauftragten bestellt. Nur die Hälfte dieser Datenschutzbeauftragten nimmt zusätzlich entsprechende Aufgaben auch im Bereich des redaktionellen Datenschutz wahr, was selbst der Presserat für wünschenswert hält.

6. Aus der Dienststelle

6.1 Entwicklung

Im Laufe des Jahres konnten die durch Weggang, Beurlaubung oder Elternzeiten entstandenen Vakanzen durch qualifizierte und engagierte Mitarbeiterinnen und Mitarbeiter überbrückt werden. Allerdings machten sich bereits wenige Monate nach In-Kraft-Treten des Anwendungstarifvertrags vom 1. August 2003 die fatalen Konsequenzen bemerkbar, die damit verbunden sind. Es zeigte sich bei uns wie andernorts, dass in der Regel die entstehenden Zeitguthaben nicht dazu genutzt werden, ein Zeitkonto aufzubauen, das in ferner Zukunft einen vorzeitigen Ruhestand ermöglicht. Vielmehr werden entsprechend den Möglichkeiten, die der Tarifvertrag bietet, die Guthaben regelmäßig abgebaut. Dies führt zu einer effektiven Minderung der zur Verfügung stehenden Arbeitszeit bei Angestellten, die selbst in unserer kleinen Dienststelle nahezu dem Wegfall von zwei Stellen gleichkommt. Diese Situation macht es erforderlich, für die angesichts unserer vielfältigen Aufgaben ohnehin viel zu geringe Personalausstattung für die nächsten Haushaltsjahre trotz der schwierigen Haushaltslage des Landes eine Aufstockung des Stellenplans anzustreben.

6.2 BürgerOffice

Das mit dem Umzug in das Dienstgebäude An der Urania 4 – 10 eingerichtete *BürgerOffice* als eigenständige Organisationseinheit zur zentralen Betreuung von Bürgerinnen und Bürgern vor allem bei der Eingabenbearbeitung hat seine Aufgaben in vollem Umfang aufgenommen und bewährt sich sowohl nach außen als auch nach innen. Eine neue Form der Aufgabenteilung zwischen BürgerOffice (front office) und Referententätigkeit (back office) macht gegenüber den Petenten die Aufgabenteilung transparenter und schafft die Möglichkeit, von den Fachreferenten erarbeitete Ergebnisse in anonymisierter Form für die künftige Arbeit, aber auch für weitere Anfragen zur Verfügung zu stellen.

Bei einer in etwa gleich großen Anzahl von Vorgängen insgesamt waren im Arbeitsgebiet Gesundheit und Soziales deutlich mehr Fälle als im Vorjahr zu verzeichnen. An zweiter Stelle folgt das bisher führende Arbeitsgebiet Wirtschaft. Deutlich angestiegen sind auch die Vorgänge aus den Bereichen Innere Sicherheit und Wissenschaft und Forschung.

Entsprechend der allgemeinen Entwicklung änderte sich die Form der Eingaben erneut eklatant. Mehr und mehr Eingänge erreichen uns nur noch über E-Mail; große Sorgen hinsichtlich der Vertraulichkeit scheinen nicht zu bestehen, da die von uns angebotene Möglichkeit der Verschlüsselung kaum genutzt wird. Wir halten gerade in dieser Situation daran fest, dass wir zwar allgemeine Anfragen über offene E-Mail beantworten, soweit es in den Ein-

gaben um personenbezogene Daten geht, aber auf den normalen Postweg übergehen.

Auch bei uns ist die oben beschriebene Belästigung durch Spam erheblich. Eine einwöchige Aufschreibung im ruhigen August zeigte folgende Zahlen: Von insgesamt 579 E-Mail-Eingängen waren 438 nicht auf unsere Aufgabenstellung bezogen, sondern Informationsmüll, darunter eine Vielzahl von Fehlermeldungen zu E-Mails, die wir niemals versandt hatten. Auch aus eigenem Interesse beteiligen wir uns an den weltweiten Aktivitäten zur Eindämmung dieser Seuche[150].

6.3 Zusammenarbeit mit dem Parlament

Der Unterausschuss „Datenschutz und Informationsfreiheit“ des Ausschusses für Inneres, Sicherheit und Ordnung des *Abgeordnetenhauses* tagte 2004 vierzehnmal und beriet dabei eine Vielzahl von Themen. Insbesondere wurden grundlegende und kontroverse Themen aus den Jahresberichten 2002 und 2003 erörtert. Die Entschließungen des Unterausschusses zum Jahresbericht 2002 wurden vom Abgeordnetenhaus in der Sitzung am 13. Mai 2004 angenommen[151]; auch der Jahresbericht 2003 ist vollständig beraten, die Entschließungen werden Anfang 2005 dem Plenum des Abgeordnetenhauses vorliegen.

6.4 Zusammenarbeit mit anderen Stellen

Das Datenschutzgesetz verpflichtet zur Zusammenarbeit mit allen Stellen, die mit Kontrollaufgaben des Datenschutzes betraut sind (§ 24 Abs. 4 BlnDSG). Diese Verpflichtung erstreckt sich auch auf den Bereich der *Informationsfreiheit*, deren Wahrung uns ebenfalls anvertraut ist (§ 18 IFG).

Das zentrale Gremium für die Zusammenarbeit in Deutschland auf dem Gebiet des Datenschutzes ist die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die in diesem Jahr im Saarland zu Gast war. Jeweils unter Gastgeberschaft des Saarländischen Rundfunks fanden die üblichen zwei Sitzungen am 25./26. März und am 28./29. Oktober in Saarbrücken statt. Die Beschlüsse zeigen erneut die Bandbreite des Datenschutzes[152].

Die besondere Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht des Landes *Brandenburg*, Dr. Alexander Dix, wurde fortgesetzt.

[150] vgl. 6.4

[151] Anhang 1

[152] vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2004“, S. 9 ff.

An den Sitzungen der Arbeitsgemeinschaft der Obersten Datenschutzbeauftragten für den Datenschutz (*„Düsseldorfer Kreis“*) in München am 6./7. Mai und am 25./26. November sowie deren Arbeitsgruppen zu verschiedenen Themen nahmen wir teil. Die Arbeitsgruppen „Internationaler Datenverkehr“[153] und „Telekommunikation, Tele- und Mediendienste“[154] werden von uns selbst betreut, eine Arbeitsgruppe zu konzerninternen Datenübermittlungen wurde von uns initiiert.

Auch die *Arbeitsgemeinschaft der Informationsbeauftragten*, die für die Wahrung der Informationsfreiheit zuständig sind, tagte zweimal: am 2. Juni in Düsseldorf und am 22. November in Berlin. Hauptthemen waren der verbesserte Zugang zu den Umweltinformationen durch die neue Richtlinie der Europäischen Union sowie die Öffentlichkeit der Sitzungen staatlicher Gremien[155].

Auf europäischer Ebene ist der Berliner Beauftragte für Datenschutz und Informationsfreiheit deutscher Ländervertreter in der Art.-29-Datenschutzgruppe. Die *Europäische Konferenz der Datenschutzbeauftragten* fand am 22./23. April in Rotterdam statt.

Die *Internationale Konferenz der Datenschutzbeauftragten* am 15./16. September in Breslau unterstrich die Rolle, die inzwischen die Staaten Mittel- und Osteuropas bei der Fortentwicklung des Datenschutzes spielen.

Unter unserem Vorsitz und erneuter Unterstützung des brandenburgischen Landesbeauftragten tagte die *Internationale Arbeitsgruppe Datenschutz in der Telekommunikation* im Rahmen der Internationalen Konferenz der Datenschutzbeauftragten zunächst am 14./15. April in Buenos Aires. Am Tag zuvor nahmen die Delegierten an einer gemeinsamen Sitzung mit der Federal Trade Commission der USA und argentinischen Verbraucherschutzinstitutionen zur Spam-Thematik teil, die ihrerseits die Arbeitsgruppensitzung besuchten. Die zweite Sitzung fand am 18./19. November in Berlin statt[156].

Die auf unsere Initiative im April 2003 in Berlin gegründete Internationale Konferenz der Informationsbeauftragten (ICIC) hatte ihre zweite Sitzung bereits mit über 100 Teilnehmern am 5./6. Februar in Kapstadt/Südafrika. Für die 3. Sitzung 2005 wird Mexiko als Gastgeber fungieren.

[153] vgl. 4.7.2

[154] vgl. 5.2

[155] vgl. Anlagenband, a.a.O., S. 93 ff.

[156] vgl. Anlagenband, a.a.O., S. 71 ff.

6.5 Europäische Akademie für Informationsfreiheit und Datenschutz

In Zusammenarbeit mit der *Europäischen Akademie* wurden drei Veranstaltungen durchgeführt:

Am 27./28. Mai bot die Akademie das Dach für eine Kooperationssitzung einiger europäischer Datenschutzbehörden zur Koordinierung der Anerkennung verbindlicher Unternehmensregelungen[157]. Das die technischen Diskussionen im ganzen Jahr beherrschende Problem des datenschutzgerechten Einsatzes von RFID war Thema eines internationalen Workshops am 30. September und 1. Oktober. Am 11./12. November fand schließlich ein ebenfalls international besetzter Workshop zu genetischen Daten und Biobanken statt, an dem international renommierte Pharmaunternehmen und -verbände teilnahmen. Die Ergebnisse werden im Internet veröffentlicht.

6.6 Öffentlichkeitsarbeit

Im Mittelpunkt der *Öffentlichkeitsarbeit* stand das 25-jährige Bestehen der Dienststelle im November 2004. Weiträumig angekündigt und von der Presse wohlwollend begleitet folgten mehrere Veranstaltungen aufeinander: ein erster Workshop für Unternehmerinnen und Unternehmer kleinerer Firmen in Kooperation mit der Industrie- und Handelskammer, ein Schnupperkurs für Schülerinnen und Schüler in Zusammenarbeit mit der Robert-Jungk-Oberschule in Charlottenburg-Wilmersdorf, ein gut besuchter Tag der offenen Tür in unserer neuen Dienststelle, an der sich auch die benachbarten Dienststellen im Haus (Rechnungshof, Landeszentrale für politische Bildungsarbeit), Kollegen (Bundesdatenschutzbeauftragter, brandenburgischer Landesbeauftragter) und Verbündete (Gesellschaft für Datenschutz und Datensicherung, Verbraucherzentrale Berlin) beteiligten. Die Mitarbeiterinnen und Mitarbeiter der Dienstbehörde engagierten sich außerordentlich, Sketche, die auf DVD zur Verfügung stehen werden, machten für die Besucher die Probleme des Datenschutzes und der Informationsfreiheit auf ungewöhnliche Weise greifbar.

Die Feierstunde am 4. November 2004 stellte ohne Zweifel den Höhepunkt dar. Der Präsident des Abgeordnetenhauses, der Regierende Bürgermeister, die Vorsitzende des Unterausschusses Datenschutz und Informationsfreiheit, die Industrie- und Handelskammer, der Bundesdatenschutzbeauftragte, der Europäische Datenschutzbeauftragte und die Vorsitzende der Internationalen Konferenz der Datenschutzbeauftragten trugen dazu bei. Die Bundesministerin für Verbraucherschutz, Ernährung und Landwirtschaft hielt eine sehr persönliche Rede, die die Geschichte der Informationsfreiheit in Berlin beleuchtete. Der Präsident des Verfassungsgerichtshofes hielt die Festrede zur datenschutzrechtlichen Rechtsprechung des Gerichtes.

[157] vgl. 4.7.1

Um den Datenschutz auch über das Jahr präsenter zu machen, beschlossen wir eine verstärkte Teilnahme an Tagen der offenen Tür:

– „33. Tag der offenen Tür der Berliner Polizei 2004“ am 16. Mai 2004
– „Lange Nacht der Wissenschaften“ am 12. Juni 2004
– „Tag der offenen Tür im Abgeordnetenhaus von Berlin“ am 19. Juni 2004
– „Jugendverbraucherschutztag“ im FEZ am 8. September 2004.

Alles waren gute Erfolge: Am Tag der offenen Tür der Polizei haben mehr als 1.000 Menschen unseren Stand besucht. Ergänzt wurde dies durch Neuauflagen unserer Broschüren und Aufkleber und durch neuartige Werbemittel, zum Umgang mit personenbezogen Daten bei der Wahlwerbung wurde ein neuer Ratgeber entwickelt.

Berlin, 15. März 2005

Prof. Dr. Hansjürgen Garstka

Berliner Beauftragter für Datenschutz und Informationsfreiheit

Beschlüsse des Abgeordnetenhauses vom 13. Mai 2004

Bericht des Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2002

zu Erste DNA-Reihenuntersuchung in Berlin

(3.3, Drs. S. 38 ff)

Der Senat wird aufgefordert, dafür zu sorgen, dass der Polizeipräsident in Berlin die Verfahrensweise bei der Durchführung von DNA-Reihenuntersuchungen innerhalb des ersten Halbjahres 2004 durch eine Geschäftsanweisung regelt, die die vom Berliner Beauftragten für Datenschutz und Informationsfreiheit vorgelegten Kriterien berücksichtigt.

zu Verbesserung bei den Aktenauskünften

(4.1.2, Drs. S. 56 ff)

Der Senat wird aufgefordert, dafür zu sorgen, dass der Polizeipräsident in den Fällen, in denen kein Auskunftsverweigerungsgrund entsprechend § 50 Abs. 2 ASOG vorliegt, Betroffenen Auskunft über die Herkunft gespeicherter Daten sowie die Adressaten von Datenübermittlungen erteilt.

zu Vorgriffsregelungen können Ärger bereiten

(4.2.1, Drs. S. 62 f)

Der Senat wird aufgefordert, bei der Umsetzung von Rahmenrecht darauf zu achten, dass rechtzeitig eine landesrechtliche Eingriffsgrundlage geschaffen wird.

zu Was Hard- und Software über uns verraten

(hier: Einsatz von Windows XP; 2.1, Drs. S. 11, 13)

Der Senat wird aufgefordert, dafür zu sorgen, dass nach der bevorstehenden Umstellung der im Land Berlin eingesetzten Microsoft-Betriebssysteme von MS Windows NT auf MS Windows XP die automatische Aktualisierung von Windows XP nur mit Wissen und Wollen der für die Datenverarbeitung

verantwortlichen Stellen aktiviert werden kann. Es muss sichergestellt sein, dass bei der automatischen Aktualisierung von Windows XP nur mit Wissen und Wollen der für die Datenverarbeitung verantwortlichen Stellen aktiviert werden kann. Es muss sichergestellt sein, dass bei der automatischen Aktualisierung keine schutzbedürftigen Daten an die Server des Herstellers übertragen werden können.

zu Beschwerde über Gerichtsvollzieher

(4.3.1, Drs. S. 70)

Der Senat wird aufgefordert, dafür zu sorgen, dass die Zustellung von Vollstreckungsunterlagen durch Gerichtsvollzieher verschlossen erfolgt.

zu Sozialdaten – Steht die technische Sicherheit noch auf einer guten Basis?

(4.4.3, Drs. S. 100)

Der Senat wird aufgefordert, dafür zu sorgen, dass die Empfehlungen der mit der Erstellung der Risikoanalyse und des Sicherheitskonzepts für Basis I (PROSOZ/S) beauftragten Unternehmensberatung zügig in allen Bezirken umgesetzt werden, soweit dies trotz der gesetzlichen Änderungen im Sozialwesen geboten ist.

zu Informationsfreiheit in Berlin

(hier: Verbraucherinformationsgesetz; 4.9.2, Drs. S. 161 f)

Der Senat wird aufgefordert, einen Entwurf zur Fortentwicklung des „Gesetzes zur Information der Verbraucherinnen und Verbraucher im Lebensmittelverkehr im Land Berlin“ dahin gehend vorzulegen, dass den Verbraucherinnen und Verbrauchern selbst ein Recht auf Zugang zu den Informationen eingeräumt wird, die bei den Behörden über Produkte im Geltungsbereich des Gesetzes vorliegen.

Wahrung der Persönlichkeitsrechte bei Film- und Fernsehaufnahmen

Der Senat wird aufgefordert, dafür Sorge zu tragen, dass Film- oder Fernsehaufnahmen nicht mit öffentlicher Unterstützung zu einer Verletzung von Persönlichkeitsrechten führen.

Insbesondere ist bei Aufnahme in Diensträumen der öffentlichen Verwaltung die vorherige ausdrückliche Einwilligung der von den Aufnahmen erfassten Personen einzuholen, sofern es sich um Verwaltungsmitarbeiterinnen und -mitarbeiter bei der Arbeit oder um antragstellende Bürgerinnen und Bürger handelt.

Bei Aufnahmen im häuslichen Bereich in Begleitung von Amtspersonen ist die Einwilligung der Betroffenen spätestens am Vortag der Film- oder Fernsehaufnahmen einzuholen. Dies gilt insbesondere auch für die Herausgabe personenbezogener Daten zur Vorbereitung der Film- oder Fernsehaufnahmen.

Auszug aus dem Geschäftsverteilungsplan

Stand: 1. Januar 2005

Prof. Dr. Hansjürgen Garstka	**Berliner Beauftragter für Datenschutz und Informationsfreiheit**
Dipl.-Informatiker Hanns-Wilhelm Heibey	Vertreter
Anja-Maria Gardain	Leitungsreferentin, Pressesprecherin, Justiziariat
Cristina Vecchi	Sekretariat
	Zentraler Bereich
Prof. Dr. Hansjürgen Garstka	Bereichsleiter
	Zentrale Aufgaben
Anja-Maria Gardain	AG: Internationaler und europäischer Datenschutz, Informationsfreiheit
Dr. Philip Scholz	AG: Telekommunikation, Tele- und Mediendienste, Presse und Rundfunk, eGovernment
Dipl.-Germanistin Laima Nicolaus	Redaktion von Veröffentlichungen, Bibliothek, Rechtsprechungssammlung, Intranet
	Allgemeine Verwaltung
Doris Werth	Haushaltsplanung und -bewirtschaftung, Büroorganisation, Beauftragte für den Haushalt
Alexandra Bertermann	Personalangelegenheiten
Carola Peplau	Rechnungsstelle, Sekretariat
Dorothea Marx	Raumbewirtschaftung

Bereich Recht

Dagmar Hartge	Bereichsleiterin AG: Verfassungsorgane, Finanzen, Nachrichtendienste, Grundsatzangelegenheiten des Datenschutzrechts sowie des Strafverfolgungs-, Sicherheits- und Ordnungsrechts
Kerstin Göhler	Sekretariat, Archiv
	BürgerOffice
Volker Brozio	Leitung; Öffentlichkeitsarbeit AG: Stadtentwicklung, Schule
Detlef Schmidt	AG: Inneres, Bezirksämter
Sabine Krissel	Geschäftsstelle, Sekretariat
Sandra Ließmann	Sekretariat
	Recht
Dipl.-Volkswirt Dr. Rainer Metschke	AG: Wissenschaft, Forschung und Statistik, Gesundheit
Dr. Claudia Golembiewski	AG: Justiz, Soziales
Daniel Holzapfel	AG: Wirtschaft, Zivilrecht (insbes. Vereinsrecht)
Birgit Saager	AG: Personaldaten, Wirtschaft
Dr. Ulrich von Petersdorff	AG: Rechtliche Bewertung von IT-Verfahren, Kultur

Bereich Informatik

Dipl.-Informatiker Hanns-Wilhelm Heibey	Bereichsleiter Recht und Politik der Informationstechnik (u. a. DV im Auftrag), Landesübergreifende Infrastrukturprojekte (außer Netzen), Kryptographie, Chipkarten, Koordination bei komplexen Beratungs- und Kontrollprojekten

	Informatik I
Dipl.-Physiker Joachim Laß	Payment-Systeme, Biometrie, Überwachungssysteme (z. B. Videoüberwachung), Organisation von Rechenzentren, Proprietäre Betriebssysteme, Nichtautomatisierte Datenverarbeitung AG: Finanzen, Wirtschaft, Inneres (Einwohner- und Ausländerwesen, ITDZ)
Jürgen Horn	Beratung der behördlichen und betrieblichen Datenschutzbeauftragten, Koordination der Kontrollen im privaten Bereich, Organisation des Datenschutzes, Unterrichtungspflicht nach § 24 Abs. 3 Satz 3 BlnDSG AG: Verfassungsorgane, Senatskanzlei, Stadtentwicklung, Justiz, Betriebe Behördlicher Datenschutzbeauftragter
Dipl.-Informatiker Ralf Hauser	Microsoft-Betriebssysteme, Bürosysteme, Lokale Netze incl. Wireless LAN, Mobile Computer AG: Gesundheit, Verkehr
Dipl.-Dokumentar Axel Tönjes	Führung des Registers nach §§ 4 d, 4 e BDSG, Ubiquitous Technologies (u. a. RFID), Grundsatzfragen AG: Kultur, Schule, Sport
	Informatik II
Dipl.-Informatikerin Ursula Zabel	Berliner Landesnetz, Telekommunikationssysteme AG: Inneres, Wissenschaft und Forschung
Dipl.-Informatiker Gerrit Oldenburg	Internet
Carsten Schmidt	UNIX, LINUX, SAP R/3, Firewallsysteme, Wartung und Fernwartung, Personalinformationssysteme AG: Soziales, Standesämter, Arbeit, Jugend

André Drescher

Systemverwaltung
Webmaster

Berliner Beauftragter für Datenschutz und Informationsfreiheit (BlnBDI)
An der Urania 4 – 10, 10787 Berlin
Telefon: (0 30) + 1 38 89-0,
Telefax: (0 30) 2 15 50 50
E-Mail: mailbox@datenschutz-berlin.de,
Internet: http://www.datenschutz-berlin.de

Agenda:
AG = Arbeitsgebiet

Stichwortverzeichnis