Abgeordnetenhaus BERLIN Drucksache 15/ 2702

15. Wahlperiode

Bericht

des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2003

Der Berliner Beauftragte für den 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 neue Bericht schließt an den am 25. März 2003 vorgelegten Jahresbericht 2002 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2003 ab.

Wiederum werden die über Berlin hinaus bedeutsamen Dokumente in einem gesonderten Anlagenband („Dokumente zu Datenschutz und Informationsfreiheit 2003“) veröffentlicht, der gemeinsam mit dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg herausgegeben wird.

Dieser Jahresbericht liegt den Mitgliedern des Abgeordnetenhauses von Berlin vor und ist über das Internet (http://www.datenschutz-berlin.de) abrufbar.

Berlin, den 30. März 2004

Prof. Dr. Hansjürgen Garstka

Berliner Beauftragter für
Datenschutz und Informationsfreiheit

Die Drucksachen des Abgeordnetenhauses sind bei der Kulturbuch-Verlag GmbH zu beziehen.
Hausanschrift: Sprosserweg 3, 12351 Berlin-Buckow · Postanschrift: Postfach 47 04 49, 12313 Berlin, Telefon: 6 61 84 84; Telefax: 6 61 78 28.

BERICHT

des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2003

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 25. März 2003 vorgelegten Jahresbericht 2002 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2003 ab.

Wiederum werden die über Berlin hinaus bedeutsamen Dokumente in einem gesonderten Anlagenband („Dokumente zu Datenschutz und Informationsfreiheit 2003“) 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

Die Neugestaltung der Kommunikationsbeziehungen der staatlichen Institutionen untereinander einerseits, zu Wirtschaft, Bürgerinnen und Bürgern andererseits durch den verstärkten, ja teilweise ausschließlichen Einsatz von Informationstechnik (eGovernment) war eines der Ziele zweier großer Reformprojekte, die die öffentliche Diskussion des vergangenen Jahres dominierten: der Steuerreform und der Gesundheitsreform.

Mit dem Steueränderungsgesetz 2003 wurden die elektronische Lohnsteuerkarte eingeführt und die Datenflüsse zwischen Arbeitgeber und Finanzbehörden auf eine neue Basis gestellt. Die Einführung eines einheitlichen Identifikationsmerkmals für alle Steuerpflichtigen („E-Tin“) birgt trotz aller datenschutzrechtlichen Absicherungen die Gefahr, dass sich daraus eine (verfassungswidrige) Personenkennzahl entwickelt[1].

Noch weit größere Bedeutung für die Entwicklung des eGovernment wird dem Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GMG) zukommen. In das Sozialgesetzbuch Buch V (SGB V) wurde der programmatische Satz aufgenommen: „Zur Verbesserung der Qualität und Wirtschaftlichkeit der Versorgung soll die papiergebundene Kommunikation unter den Leistungserbringern so bald und so umfassend wie möglich durch die elektronische und maschinell verwertbare Übermittlung von Befunden, Diagnosen, Therapieempfehlungen und Behandlungsberichten, die sich auch für eine einrichtungsübergreifende fallbezogene Zusammenarbeit eignet, ersetzt werden.“

Neben der Verpflichtung der beteiligten Stellen, ähnlich wie bei der Finanzverwaltung, die Kommunikationsbeziehungen auf elektronische Übermittlungen umzustellen, werden zwei Medien eingeführt, die die Krankenversicherten persönlich stark betreffen werden: die persönliche elektronische Gesundheitsakte und die über die Funktionen der bisherigen Krankenversichertenkarte weit hinausgehende elektronische Gesundheitskarte. Ein völlig neues System zur Herstellung der Datentransparenz wird eine Flut von Datenflüssen zwischen den verschiedensten Stellen mit dem Ziel auslösen, die Kosten des Gesundheitswesens besser durchschaubar zu machen.

Das GMG setzt in großem Maßstab zwei Regelungen ein, die das Bundesdatenschutz 2001 (BDSG) neu eingeführt hat: Bei der Gesundheitskarte müssen die Anforderungen an mobile personenbezogene Speicher- und Verarbeitungsmedien erfüllt werden, die Verfahren zur

Herstellung der Datentransparenz realisieren ein Pseudonymisierungsmodell, das bisher einmalig ist[2].

Das Bundesdatenschutzgesetz (BDSG) selbst wurde Anfang des Jahres neu bekannt gemacht[3], was die Handhabung des ohnehin schwer lesbaren Gesetzes durch die Einbeziehung zwischenzeitlich erfolgter gesetzestechnischer und redaktioneller Änderungen wenigstens erleichtert. Von der grundsätzlichen Modernisierung des Datenschutzes[4], die im Koalitionsvertrag für die laufende Legislaturperiode vereinbart worden war, war nichts zu hören. Auch das ebenfalls vereinbarte Informationsfreiheitsgesetz des Bundes[5] kam nicht voran, ebensowenig das seit vielen Jahren geforderte und angekündigte Arbeitnehmerdatenschutzgesetz.

Die öffentlichen Diskussionen über die Fortentwicklung des Datenschutzes konzentrierten sich auf neue sicherheitspolitische Instrumente[6] sowie auf die Diskussion über Vorzüge der Chipkarte (Gesundheitskarte, Job-Card) oder weiterer Rasterfahndungen im Gesundheits- und Sozialwesen[7].

Zumindest ein positives Signal setzte die ehemalige Präsidentin des Bundesverfassungsgerichtes Jutta Limbach bei dem Festakt zum 25-jährigen In-Kraft-Treten des Bundesdatenschutzgesetzes am 11. Juni in Berlin[8]. Sie schloss den Festvortrag mit den Worten: „Wenn wir die modernen Informations- und Kommunikationschancen ohne Reue benutzen wollen, müssen wir für einen vorbeugenden Schutz des Rechts auf informationelle Selbstbestimmung sorgen. Denn der Datenschutz gewährleistet die staatsbürgerlichen Freiheiten, die ihrerseits das Lebenselixier einer demokratischen Gesellschaft sind.“ Sie fügt an, und der vorliegende Bericht möge dies hoffentlich erneut bestätigen: „Die Institution des Datenschutzbeauftragten ist daher einer der wichtigsten Garanten einer lebendigen Demokratie.“

Die höchstrichterliche Rechtsprechung musste sich wiederum mit einer Reihe datenschutzrechtlicher Probleme beschäftigen.

---

[1] vgl. 4.3.2
[2] vgl. 4.4.1
[3] Neufassung des Bundesdatenschutzgesetzes vom 14. Januar 2003, BGBl I, S. 66
[4] Roßnagel, Alexander; Pfitzmann, Andreas; Garstka, Hansjürgen: Modernisierung des Datenschutzrechts. Berlin: Bundesministerium des Innern, 2001. – Gutachten; vgl. hierzu Forderungen der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003, Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2003“, S. 11
[5] vgl. 4.9.2
[6] vgl. 3.1
[7] vgl. 4.4.3

Im Juli 2003 entschied das Bundesverfassungsgericht[9], dass Schriftstücke, für die ein Abgeordneter glaubhaft macht, dass sie ihm im Zusammenhang mit seiner parlamentarischen Arbeit anvertraut sind, in den Räumen des Bundestages auch bei einem Mitarbeiter eines Abgeordneten nicht beschlagnahmt werden dürfen. Mit dem Zeugnisverweigerungsrecht und dem Beschlagnahmeprivileg nach Artikel 47 Grundgesetz (GG) schütze die Verfassung das Vertrauensverhältnis, das im Einzelfall zwischen dem Abgeordneten und einem Dritten in Rücksicht auf die Mandatsausübung zustande gekommen ist. Das Gericht hat dabei unterschieden zwischen der unmittelbaren Herrschaftsmacht über Schriftstücke, die dem Direktionsrecht des Abgeordneten unterliegen, und den Fällen, in denen die rechtliche und tatsächliche Beherrschungsmöglichkeit des Abgeordneten soweit gelockert ist, dass der Schutzbereich des Artikel 47 GG verlassen wird. Danach dürfen Unterlagen, die sich in einem Mitarbeiterbüro befinden, nicht beschlagnahmt werden. Sie befinden sich nach der Entscheidung des Bundesverfassungsgerichts noch im Herrschaftsbereich des Abgeordneten.

Überraschenderweise hat das Bundesverfassungsgericht noch nicht über die Verfassungsbeschwerden gegen den „Großen Lauschangriff“ entschieden, die am 1. Juli Gegenstand einer mündlichen Verhandlung waren, bei der sich auch der Berliner Datenschutzbeauftragte geäußert hat. Sehr kritische Fragen der Richter, etwa dahingehend, ob tatsächlich nur technische Schwierigkeiten ein Garant für die informationelle Selbstbestimmung seien, lassen vermuten, dass das Gericht dieses neue, aber weitgehend ungenutzte Instrument der Strafverfolgung einer äußerst sorgfältigen Prüfung unterzieht.

Erstmals befasste sich der Bundesgerichtshof (BGH) mit den Aufgaben und der Unabhängigkeit eines Datenschutzbeauftragten[10]. Dem sächsischen Datenschutzbeauftragten war von der Landesregierung, der sich die Staatsanwaltschaft anschloss, vorgeworfen worden, durch die Veröffentlichung von Datenschutzverstößen des Landesjustizministers gegen seine Dienstpflichten verstoßen zu haben. Wie bereits zuvor das Landgericht Dresden[11] sprach der BGH den Landesbeauftragten frei, da er mit der Veröffentlichung pflichtgemäß gehandelt habe.

Auch in einem anderen Urteil unterstrich der BGH die Bedeutung der informationellen Selbstbestimmung. In einem Amtshaftungsverfahren hat er[12] einen Schadensersatzanspruch

---

[8] abgedruckt in: RDV 2002, S. 164
[9] Urteil vom 30. Juli 2003, Az.: 2 BvR 508/01 und 2 BvE 1/01
[10] Urteil vom 9. Dezember 2002, Az.: 5 StR 276/02. In: RDV 2003, S.84
[11] Urteil vom 7. November 2001, Az.: 4 KLs 420 Js 49212/00
[12] Urteil vom 23. Oktober 2003, Az.: III ZR 9/03

wegen eines 20 Monate dauernden rechtswidrigen Lauschangriffs bestätigt. Der Entscheidung des BGH liegt ein strafrechtliches Verfahren wegen Brandstiftung zugrunde, in dessen Verlauf die Polizei eine richterliche Anordnung über den verdeckten Einsatz technischer Mittel zur Erhebung personenbezogener Daten in der Wohnung des Vaters des Beschuldigten und später auch in der Wohnung des Beschuldigten selbst erwirkt hatte. Die Eröffnung des Hauptverfahrens war von der zuständigen Strafkammer abgelehnt worden, weil diese einen hinreichenden Tatverdacht nicht als gegeben ansah.

Das Bundesarbeitsgericht bestätigte, dass eine versteckte Videoüberwachung am Arbeitsplatz ausnahmsweise zulässig ist, wenn ein hinreichend konkreter Verdacht einer Straftat besteht und andere weniger beeinträchtigende Instrumente nicht zur Verfügung stehen[13].

Im Juni 2003 lief die mit äußerst schwierigen Aufgaben bis hin zu den datenschutzrechtlichen Folgen des 11. September 2001 belastete Amtszeit des Bundesdatenschutzbeauftragten Joachim Jacob aus. Obwohl dieser Zeitpunkt lange bekannt war, dauerte es bis November, bis sein Nachfolger Peter Schaar, vormals stellvertretender Hamburgischer Datenschutzbeauftragter, vom Bundestag zu seinem Nachfolger gewählt wurde. Am 17. Dezember erhielt er seine Ernennungsurkunde. Mit ihm nimmt erstmals ein Ökonom, und nicht ein Jurist, diese verantwortungsvolle Aufgabe wahr. Die auch im Modernisierungsgutachten eingeforderte Hinwendung zu mehr ökonomischen Betrachtungsweisen des Datenschutzes wird dadurch personell repräsentiert.

In der Europäischen Union waren die für den Datenschutz zuständigen Einrichtungen, insbesondere das Datenschutzreferat der Generaldirektion Binnenmarkt (Data Protection Unit) und die Datenschutzarbeitsgruppe nach Art. 29 der Europäischen Datenschutzrichtlinie (Art. 29 Data Protection Working Party) schwerpunktmäßig mit der Frage der Übermittlung von Flugpassagierdaten in die USA befasst. Eine Lösung, die die Rechtmäßigkeit des Zugriffs der US-Behörden auf teilweise auch sensitive Daten wie Daten zur Gesundheit und Religionszugehörigkeit sicherstellt, konnte im Berichtsjahr nicht erreicht werden[14].

Vorgelegt wurde von der Kommission am 15. Mai 2003 der Erste Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46)[15]. Darin kommt die Kommission zum Ergebnis, dass das Ziel, ein hohes Datenschutzniveau in der Gemeinschaft zu erreichen, erzielt worden sei. Dies sei insbesondere darauf zurückzuführen, dass die Richtlinie selbst einen der

[13] Urteil vom 27. März 2003, Az.: 2 AZR 51/02
[14] vgl. 4.7.1
[15] KOM(2003) 265 endg.

höchsten Datenschutzstandards weltweit aufweise[16]. Gleichwohl werden eine Reihe von Mängeln gerügt. So ist die Kommission der Auffassung, der von einigen Mitgliedstaaten (gemeint ist u. a. Deutschland) verfolgte Ansatz, dass das angemessene Schutzniveau in Drittländern durch die übermittelnde Stelle selbst vorgenommen werden soll, die Kontrolle durch die Aufsichtbehörden aber begrenzt ist, entspreche „offensichtlich nicht“ den Anforderungen der Richtlinie[17].

Auch auf europäischer Ebene wird eine Personalentscheidung künftig weitreichende Folgen haben. Nach einem langwierigen Verfahren haben das Europäische Parlament und der Rat am 22. Dezember beschlossen, den bisherigen Präsidenten der niederländischen Datenschutzbehörde Peter Hustinx zum Datenschutzbeauftragten für die Einrichtungen der Europäischen Union (European Data Protection Supervisor) und den spanischen hohen Richter Joaqin Bayo Delgado zu seinem Stellvertreter zu ernennen. Sie haben am 2. Februar 2004 ihr Amt angetreten.

1.2 Berlin

Wie im Vorjahr konzentrierte sich die datenschutzrechtliche Entwicklung auf Probleme der Anwendung des Berliner Datenschutzgesetzes und der spezialgesetzlichen Regelungen.

Eine Ausnahme bildete die Debatte um das Gesetz zur Einrichtung eines zentralen Personalüberhangmanagements, mit dem eine schnellere und effizientere Vermittlung von Personalüberhangkräften erreicht werden soll. Nachdem beim im Abgeordnetenhaus eingebrachten Gesetzentwurf die datenschutzrechtliche Dimension des Vorhabens offensichtlich völlig übersehen worden war, konnte im Laufe der parlamentarischen Beratung ein befriedigendes Ergebnis erzielt werden[18].

Die vom Abgeordnetenhaus[19] geforderte Anpassung des Meldegesetzes an die zwischenzeitlich erfolgten Änderungen des Melderechtsrahmengesetzes sowie an weitere Vorschläge zur Verbesserung des Datenschutzes ist wiederum nicht erfolgt. Stattdessen hat der Senat, ohne diese Änderungen abzuwarten, in einer Durchführungsverordnung weitere, aus unserer Sicht unverhältnismäßige Zugriffe erlaubt[20]. Auf Drängen des Unterausschusses Datenschutz

[16] a. a. O., S. 12
[17] a. a. O., S. 21, vgl. 4.7.1
[18] vgl. 4.4.1
[19] Beschluss vom 12. Dezember 2002, vgl. JB 2002, Anhang 1
[20] GVBl. 2003, S. 514

und Informationsfreiheit des Abgeordnetenhauses wurde der Vollzug der Verordnung ausgesetzt[21].

Die sowohl vom Unterausschuss, der Senatsverwaltung für Inneres und uns aus vor allem gesetzestechnischen Gründen für erforderlich gehaltene Novellierung von Datenschutz- und Informationsfreiheitsgesetz ist nicht vorangekommen. In der Sitzung des Unterausschusses vom 24. September 2002 hatte sich die Senatsverwaltung für Inneres bereit erklärt, mit uns zusammen zu überprüfen, ob das von uns seit 1990 vorgeschlagene Projekt, diese beiden Materien zusammen mit anderen informationsrechtlichen Regelungen in ein „Berliner Informationsgesetzbuch“ zusammenzuführen[22], verwirklicht werden kann[23].

Die Arbeiten an diesem Projekt entwickelten sich zwar aus verschiedenen Gründen nur zögerlich, blieben aber weiterhin aus unserer Sicht auf der Tagesordnung. Umso überraschter waren wir, als wir ohne vorherige Information einer Abgeordnetenhausdrucksache entnehmen mussten, dass aus der Sicht der Senatsverwaltung für Inneres das Projekt nicht weiterverfolgt werden sollte[24]. Demgegenüber gehen wir davon aus, dass die Arbeiten weitergeführt werden und in absehbarer Zeit zu einer wegweisenden Informationsgesetzgebung führen.

2. Technische Rahmenbedingungen

2.1 Entwicklung der Informationstechnik

Entwicklungstrends

Die Entwicklung der Informationstechnik wird – wie an dieser Stelle immer wieder dargestellt – seit langem von drei wesentlichen Trends bestimmt:

Erstens ist die ständige *Verbesserung des Preis-Leistungs-Verhältnisses* bei Informationstechnischen Systemen zu nennen, für jeden erkennbar in den aggressiven Werbemitteilungen der Elektronikmärkte und Discounter über höhere Taktfrequenzen der Prozessoren, größere Arbeits- und Plattenspeicher, bessere externe Speichermedien zur Aufnahme außerordentlicher Datenmengen. Und das alles bei einem grundsätzlich gleichbleibenden

[21] vgl. 4.1.2
[22] JB 1990, 1.2
[23] JB 2002, 1.2
[24] Abghs.-Drs. 15/1693 und 15/2123

Preisniveau. Auf der Festplatte der neuesten Discounterangebote lassen sich locker die melderechtlichen Daten der Berliner Bevölkerung abspeichern, wenn es nur darum ginge, sie lokal zu speichern und abzufragen. Die Leistungsdaten für den privaten Rechner zu Hause lassen sich nur mit seiner Rolle als Entertainment-Center rechtfertigen, auf dem der Spielfilmbedarf für Monate zum Direktabruf bereitgehalten wird. Wer mit einem solchen Rechner nur Büroaufgaben bewältigen und im Internet surfen will, hat Mühe, seinen Bedürfnissen angepasste Rechner zu erwerben.

Zweitens *verkleinern* sich informationstechnische Komponenten rapide. Pervasive bzw. Ubiquitous Computing, also der allgegenwärtige Einsatz miniaturisierter informationstechnischer Systeme, war bereits vor zwei Jahren Thema an dieser Stelle[25]. Computer sind längst nicht mehr an die Form gebunden, die man gemeinhin mit ihnen verbindet: Kleine oder große Kästen mit Speichern und Verarbeitungschips, an denen Ein- und Ausgabegeräte unterschiedlicher Art angeschlossen sind. Computer können heute vielmehr in jedem der vielen Gegenstände des alltäglichen Gebrauchs integriert sein. Berührungslos auslesbare Speicher können als Tickets für viele Dienstleistungen, zum Beispiel auch im öffentlichen Nah- und Fernverkehrswesen, herhalten, sie können beliebige Gegenstände kennzeichnen und automatisiert erkennbar machen. Auf das Beispiel der Radio-Frequency-Identification- (RFID-) Etiketten kommen wir sofort zurück.

Drittens werden die informationstechnischen Systeme in dem Maße zunehmend *vernetzt*, in dem die kommunikationstechnischen Systeme an Verbreitung und Vielfalt gewinnen. An das Internet und die damit verbundene Vernetzung von Computern aller Art hat man sich mittlerweile gewöhnt; dass aber die oben beschriebenen minimalisierten IT-Komponenten ein geschwätziges Eigenleben entfalten können, wird in Zukunft unser Leben genauso bestimmen. Ein großer Motor wird dabei die zunehmende Verbreitung der drahtlosen Kommunikationstechniken sein. Dazu gehört auch die Möglichkeit, Speichermedien funktechnisch aus der Entfernung abzufragen.

Transponder allerorten – von Schutzengeln und Warenetiketten

Um anschaulich zu machen, wie man sich die Zukunft mit dieser Technologie vorstellen kann, wollen wir erneut Episoden aus dem Leben von Egon Digital erzählen. Egon Digital hatten wir bereits im Jahresbericht 2001 vorgestellt[26]. Damals wurde ein Szenario auf das

[25] JB 2001, 2.1
[26] JB 2001, 2.1

Jahr 2010 datiert, in dem wir den Segen der Ubiquitous Computing Systems (UCS) veranschaulichten, aber auch, was sie zur Aushöhlung der Persönlichkeitsrechte von Egon Digital beitragen konnten.

Zwei Jahre später, im Jahre 2012, hatte sich Egon Digital gerade daran gewöhnt, dass sein Kühlschrank für ihn die Planung seiner Lebensmitteleinkäufe übernommen hatte und dass eine automatische Rückkopplung mit dem Ernährungsberatungssystem seiner Krankenkasse dafür sorgte, dass der Kühlschrank nur mit individuell gesundheitsfördernden Nahrungsmittel gefüllt wird. Jetzt machte Egon neue Erfahrungen mit den Segnungen moderner Informationstechnik.

Egon hatte sich einen „Digitalen Schutzengel“ unter die Haut transplantieren lassen. Damit wurden weitere Risiken des täglichen Lebens von ihm ferngehalten. Seinem Hund und seiner Katze hatte er zwar schon vor acht Jahren einen Transponder-Chip einpflanzen lassen, damit sie immer sicher identifiziert werden konnten, wenn sie ausgebüxt waren oder wenn sie bei einem Unfall zu Schaden gekommen wären. Die nächste Generation dieser Chips war mit drahtloser Datenübertragung und einem Empfänger für das satellitengestützte Ortungssystem ausgestattet. Egon konnte also immer feststellen, wo sich seine Tiere befanden.

Egons „Digitaler Schutzengel“ konnte das auch, aber er konnte noch viel mehr: Sensoren maßen wichtige Körperdaten und wachten so über seine Gesundheit. Wenn er an den automatischen Dienstleistungssystemen seiner Bank Transaktionen durchführen wollte, brauchte er keine PIN oder keinen Fingerabdruck mehr. Der implantierte Chip sendete Egons digitale Erkennungsnummer aus, die bei besonders heiklen Anwendungen sogar elektronisch signiert war. Nicht nur Gesundheitswesen und Wirtschaft profitierten jedoch vom Einsatz des digitalen Engels, auch die öffentliche Sicherheit und Ordnung sollte mit dem Chip verbessert werden. Nach einigen spektakulären Sicherheitsvorfällen hatte der Innenminister durchgesetzt, dass die Betreiber der „Digitalen Schutzengel“-Dienste den staatlichen Sicherheitsbehörden den Online-Zugriff auf die Kundendatenbanken geben mussten, in denen verzeichnet war, welche digitalen Erkennungsnummern zu welcher Person gehören. Obwohl die Gesundheitsministerin es noch nicht gesetzlich durchgesetzt hatte, dass alle Personen einen solchen Chip tragen mussten, hatte sich die Technologie, weil kostengünstig und von hohem Nutzeffekt, längst weitgehend verbreitet. Deshalb konnten auf den öffentlichen Plätzen die fehleranfälligen Gesichtserkennungssysteme weitgehend abgebaut werden. Sie hatten ihren Nutzen verloren, denn es konnten jetzt jederzeit Dateien erstellt

werden, die genaue Aussage darüber trafen, wer sich wann auf diesen Plätzen aufgehalten hatte.

Egon Digital musste sich aber noch an andere Phänomene gewöhnen. Als er neulich im Park spazieren ging, hatte er sich an einem Kiosk eine Tüte Erdnüsse gekauft. Als er sie verzehrt hatte, warf er die Tüte so unachtsam in einen Müllbehälter, dass sie daneben und auf den Boden fiel. Ein paar Tage später erhielt er ein Verwarnungsgeld wegen der Verschmutzung öffentlicher Grünanlagen. Er konnte sich nicht erinnern, dass ihn jemand beobachtet hatte, erhob Einspruch und erfuhr, dass die Erdnusstüte mit einem elektronischen Etikett, einem RFID-Tag, ausgestattet war, welches die Tüte eindeutig erkennbar machte. In Verbindung mit Egons implantiertem Identifizierungschip ergab sich beim Kiosk eine datenmäßige Zusammenführung von Person und gekauftem Produkt, die von der Kioskkasse automatisch in eine zentrale Datenbank übertragen wurde, in der zu jedem produzierten Produkt der Status vermerkt war, also ob es noch im Regal beim Groß- oder Einzelhandel lag oder an wen es verkauft worden war. Als der Parkwächter – in Hamburg auch „Opticker" genannt – die leere Tüte auf dem Rasen fand, konnte somit sofort festgestellt werden, wer sie unsachgemäß entsorgt hatte.

Das Szenario befasst sich zunächst mit der Überlegung, Personen oder Tieren einen Chip unter die Haut zu pflanzen oder an Gegenständen zu befestigen, der elektromechanisch seinen eigenen Strom durch die Bewegung von Mensch und Tier erzeugt und vielfältige Funktionen der Datenübertragung wahrnehmen kann:

- Ortsbestimmung von Menschen (vor allem Kinder, geistig behinderte oder entführungsgefährdete Personen) und Gegenständen mit Hilfe des Global Positioning Systems (GPS) in Verbindung mit einer funkgestützten Datenübertragung,
- medizinische Überwachung von Risikopatienten,
- Verwaltung und Kontrolle von landwirtschaftlichen Nutztieren,
- Nutzung als elektronische „Handschelle" oder „Fußfessel",
- fälschungssichere Identifikation von Personen im Zusammenhang mit dem eCommerce.

Die unter der Bezeichnung „Digital Angel" bereits im Jahre 2000 propagierte Idee der amerikanischen Firma Applied Digital Solutions (ADS) ist zum Jahresende 2003 wieder ins Gespräch gekommen. Unter der Bezeichnung Veripay erscheint jetzt das Konzept als große Alternative für die Identifikation im Zahlungsverkehr wieder auf der Bildfläche.

Es gibt noch keine Hinweise darauf, dass die „Digital Angel“-Chips bereits zu einem Produkt geworden sind. Allerdings deutet nur Weniges in der Internet-Diskussion darauf hin, dass der digitale Schutzengel schützende Wirkung auf das Persönlichkeitsrecht der informationellen Selbstbestimmung entfalten könnte.

Das Szenario befasst sich als nächstes mit einem sehr ähnlichen technischen Produkt, dem Radio-Frequency Identification Tag (RFID). Dabei handelt es sich um elektronische Etiketten mit Transponder-Technologie, die an jedem Gegenstand angebracht werden können und von Lesegeräten über Funksignal dazu veranlasst werden, den Identifikator des Gegenstandes zurückzusenden. Dies kann auf geringeren Entfernungen ohne eigene aktive Stromversorgung erfolgen. Der Identifikator kann prinzipiell so lang sein, dass jeder Gegenstand, der auf der Welt produziert wird, eine eindeutige Kennung erhalten kann.

RFID-Etiketten gibt es schon seit einiger Zeit zur Identifikation von Produkten, vornehmlich im Zusammenhang mit der Kontrolle der Logistik oder zum Schutz der Markenidentität.

Die datenschutzrechtliche Problematik der RFID-Etiketten ergibt sich, wenn Produktidentifikatoren und Personenidentifikatoren in Zusammenhang gebracht werden. Dies wird vor allem beim Bezahlen der Produkte möglich sein. Dazu bedarf es nicht des im Szenario beschriebenen implantierten Identfikationschips des Käufers. Es reicht die heute im Zusammenhang mit elektronischen Zahlungsmitteln übliche Käuferidentifizierung, um zu erfassen, wer welchen RFID-identifizierbaren Gegenstand erworben hat. Es können also heimliche Käuferprofile von außerordentlicher Genauigkeit entstehen. Wenn die RFID-Chips außerdem nach dem Kauf aktiv bleiben, dann kann er nach Verlassen des Geschäfts heimlich verfolgt und überwacht werden. Verschärft wird das Problem durch die wesentlichen Fortschritte bei der Entwicklung leistungsfähiger Prozessoren und Speichersysteme. Bürgerrechtler befürchten, dass die Produktdaten aller produzierten Gegenstände in Verbindung mit den beim Kauf gewonnen Personenidentifikationen zu einer potenziell weltweit gesammelten Datenzusammenballung führen können[27].

Aus diesem Grunde müssen Wege zum datenschutzfreundlichen Einsatz der RFID-Etiketten gefunden werden, wenn sie stärkere Verbreitung finden sollen.

[27] Presseerklärung des Foebud e.V. vom 19. November 2003 mit einem Positionspapier diverser internationaler Verbraucherschutz- und Bürgerrechtsorganisationen über den Gebrauch von RFID auf und in Konsumgütern

So muss im Zusammenhang mit der Etikettierung von Waren die Existenz eines RFID-Etiketts an einem Produkt vom Käufer erkannt werden können. Da die Etiketten meist nicht unmittelbar erkennbar sind, sind Detektoren zu entwickeln, die der Käufer mitbringen kann oder die ihm vom Händler für den Einkauf zur Verfügung gestellt werden können. Der Käufer muss das Recht und die Möglichkeit haben, nach dem Kauf das RFID-Etikett zu entfernen oder unbrauchbar zu machen[28].

Vor diesem Hintergrund hat sich der Berliner Beauftragte für Datenschutz und Informationsfreiheit bereit erklärt, als Jurymitglied an einer Ausschreibung der Stiftung bridgeideas teilzunehmen. Den Preis gewann die Bürgerrechtsorganisation Foebud e.V. für die Entwicklung eines Gerätes zum Aufspüren von RFID Tags und den entsprechenden Lesegeräten.

Zurück zu den Anfängen – die Renaissance der zentralen Datenverarbeitung

Nach dem vorher Beschriebenen, in dem die Entwicklung zur allgegenwärtigen Informationsverarbeitung deutlich wird, mutet die Überschrift seltsam an, wenn über aktuelle Entwicklungen in der Informationstechnik geschrieben werden soll. Dennoch resultiert aus der ständigen Verbesserung des Preis-Leistungs-Verhältnisses ein deutlicher Trend zur Zentralisierung von Datenverarbeitung.

Die Frühzeit der Datenverarbeitung war von zentralen Rechenzentren bestimmt, in denen proprietäre Großrechner mit heute lachhaft erscheinenden Leistungsdaten jene Aufgaben wahrnahmen, die zur damaligen Zeit wirtschaftlich damit verarbeitet werden konnten. Anfang der 80er Jahre mutete es kühn an, wenn jemand solche Rechner für profane Büroaufgaben wie z. B. die Textverarbeitung einsetzen wollte. Daran hatte auch der bereits Mitte der 70er Jahre einsetzende Trend zur Dialogverarbeitung über Fernschreiber oder erste Bildschirmterminals nichts geändert. Mitte der 80er Jahre begann die Büroautomatisierung auf der Basis mittlerer Datentechnik, meist unter UNIX und seinen Derivaten. Die Büroarbeiten, jetzt im Wesentlichen Textverarbeitung, wurden von Terminals am Arbeitsplatz aus durchgeführt, die über keinerlei eigene Verarbeitungskapazitäten verfügten. Die gesamte Verarbeitung einschließlich der damals noch einfachen Bildschirmaufbereitung erfolgte durch das zentrale System.

[28] Presseinformation des brandenburgischen Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht vom 8. Dezember 2003; Entschließung der Internationalen Konferenz der Datenschutzbeauftragten zu Radio-Frequency Identification vom 20. November 2003, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2003“, S. 98

Personalcomputer waren schon Ende der 70er Jahre bekannt, wurden aber ausschließlich als Stand-alone-Rechner verwendet, weil die Vernetzung solcher Systeme technologisch noch nicht möglich war. Erst in den späteren 80er Jahren kamen die PC-Netze auf. Mit Abstand führendes Architekturmodell wurden dann die Client-Server-Netze, in denen eine Aufgabenteilung zwischen einem oder mehreren zentralen Servern einerseits und Clients am Arbeitsplatz vorgenommen wurde. Die Server boten die zentral vorzuhaltenden Dienstleistungen an, insbesondere zentrale Datenhaltung und zentrale Druckdienste. Da das Client-Server-Netz auch heute das vorherrschende Modell darstellt, ist das Angebot von Serverdiensten wesentlich erweitert worden, zum Beispiel Web- und Mailserver für den Verkehr mit Intranet und Internet. Die Clients führten die Verarbeitung durch, die am Arbeitsplatz gebraucht wurde: Grafische Aufbereitung der Bildschirminhalte, Office-Anwendungen, arbeitsplatzspezifische Anwendungen.

Aus der Sicht der Datenschutzes und der IT-Sicherheit entpuppte sich der vernetzte PC am Arbeitsplatz als besonderer Risikofaktor, weil das hohe Gebrauchspotenzial der Intelligenz am Arbeitsplatz gleichzeitig ein Missbrauchspotenzial bedeutet, das bis heute nur schwer beherrscht werden kann. Es hat lange gebraucht, bis sich die Erkenntnis durchsetzte, dass sicherheitsbedürftige Clients in der Regel nicht über Diskettenlaufwerke verfügen sollten; mehr und mehr gilt dies auch für CD-Laufwerke, weil sonst der normale Benutzer beliebig Kopien seiner Daten und Programme machen, fremde Daten einspielen und nicht vorgesehene Programme installieren kann. Bis heute ist es kaum möglich, gewieften PC-Nutzern den Weg zur Nutzung der Betriebssystemebene zu sperren, in der er jedwede Sicherheitstechnik umgehen kann. Mit diesen Risiken leben wir weitgehend. Unsere Kontrollen zeigen, dass es weitgehend der Verlässlichkeit der Mitarbeiter geschuldet ist, wenn keine Schadensfälle aufgetreten sind.

Wie bereits dargestellt, ist die Leistungsfähigkeit moderner PCs jedoch selbst bei kleinster Ausstattung so hoch, dass sie als Clients bei normalen Verwaltungs- und Büroanwendungen in Wirtschaft und Verwaltung nicht im Geringsten ausgelastet werden. Bei größerer Ausstattung gilt dies meistens auch für Server. Es liegt daher nahe, dass die Server in Zukunft mehr Dienstleistungen anbieten und Verarbeitungsleistungen, die vorher von den Clients getragen wurden, auf die Server zurückverlagert werden. Die Aufgabe der Clients bleibt es, für eine ergonomische und anspruchsvolle optische Datendarstellung zu sorgen, auch wenn die programmtechnische Aufbereitung der grafischen Darstellung bereits im Server erfolgt. Die Idee der „Thin Clients“ ist in den vergangenen Jahren vor allem von der Microsoft-Konkurrenz aufgeworfen worden. Ein ähnlicher Ansatz, der jedoch weniger die Leistungsbeschränkung

der Clients betont als vielmehr die Konzentration der Leistungen auf den Server, wird mit dem Begriff „Server Based Computing (SBC)“ erfasst.

Mit dieser Entwicklung verbinden sich Hoffnungen aus datenschutzrechtlicher und sicherheitstechnischer Sicht, weil die Manipulations- und Missbrauchsmöglichkeiten der Benutzer an den leistungsbeschränkten Arbeitsplatzgeräten erheblich verringert werden.

Allerdings wird sie erkauft durch die erneute Entstehung großer zentraler Datensammlungen. Insbesondere ist ein Trend erkennbar, dass private Provider den Nutzern anbieten, ihre gesamte Datenverwaltung zu übernehmen – von der Film- und Musiksammlung über das private Fotoalbum bis hin zur eigenen Buchführung. Die dabei entstehenden Datensammlungen mit dem Risiko der Bildung von Verhaltensprofilen und deren Missbrauch werden einen hohen Aufwand technisch-organisatorischer Sicherungen erfordern.

Nachtrag zur Geschwätzigkeit von Software

Im vorigen Jahr wurden an dieser Stelle diverse Beispiele genannt, in denen Hard- und Software für die Hersteller die Ausforschung ihrer Benutzer übernahmen[29] oder Sicherheitstechniken aufzwangen, die die durch den Benutzer selbstbestimmte Computernutzung wesentlich beschränken würden. Dabei wurde auch das aktuelle Betriebssystem Windows XP von Microsoft behandelt. Die Datenschutzbeauftragten haben sich in aller Welt inzwischen mit dem Phänomen des automatischen Betriebssystem-Updates bei Windows XP befasst, dessen Benutzung in den Lizenzierungsbestimmungen als obligatorisch vereinbart wird[30].

Durch das automatische Software-Update sollen notwendige Updates bzw. Patches, die zur Gewährleistung der Sicherheit und Aktualität von System- und Anwendungssoftware dienen sollen, über das Internet geladen und automatisch installiert werden.

Vor allem Betriebssystem-Updates sind jedoch als sicherheitskritisch zu bewerten, da sie in Betriebssystemfunktionen eingreifen und die Wirkung auf die sonstige Systemumgebung

[29] JB 2002, 2.1, vgl. auch Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März „TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden“, Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2003“, S. 20

[30] Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. August 2003 zu automatischen Software-Updates, vgl. a. a. O., S. 32; Resolution on Automatic Software Updates der 25. Internationalen Konferenz der Datenschutzbeauftragten vom 12. September 2003, vgl. a. a. O., S. 97

nicht einschätzbar ist. Hieraus ergibt sich die Notwendigkeit, vor einem weiteren Einsatz des veränderten Betriebssystems Tests und Freigabeverfahren durchzuführen, damit ein reibungsloser Echtbetrieb fortgesetzt werden kann.

Oft werden Konfigurationsdaten – möglicherweise mit personenbeziehbaren Daten – unbemerkt aus dem Personal Computer ausgelesen und an den Softwarehersteller übermittelt, womit die Anonymität der Softwarenutzung verletzt werden könnte.

Gerade in der Entschließung der deutschen Datenschutzkonferenz wird auf den Tatbestand hingewiesen, dass Änderungen an automatisierten Verfahren zur Verarbeitung personenbezogener Daten oder an den zugrunde liegenden Betriebssystemen Wartungstätigkeiten im datenschutzrechtlichen Sinne sind und daher nur den dazu ausdrücklich ermächtigten Personen möglich sein dürfen. Im Berliner Datenschutzgesetz wurde diese Problematik aufgegriffen. In § 3 a BlnDSG wurden Anforderungen aufgelistet, die bei einer Wartung zu erfüllen sind, aber bei einem automatisierten Softwareupdate nicht erfüllt werden können.

Zusammenfassend kann nur empfohlen werden, dass ausschließlich überprüfbare, benutzerinitiierte Update-Verfahren eingesetzt werden, die keinen Datenaustausch mit dem Zielrechner erfordern.

2.2 Datenverarbeitung in der Berliner Verwaltung

Die finanzielle Situation des Landes hat sich im Berichtsjahr nicht verbessert. Dies ist Grund genug, verstärkt in die Modernisierung der informationstechnischen Infrastrukturen und Verfahren zu investieren. Dabei geht es nicht nur um zusätzliche Rationalisierungseffekte durch die Erweiterung und Modernisierung von Fachverfahren, sondern auch um Anwendungen, die unmittelbar Maßnahmen unterstützen sollen, die explizit zur Erzielung wichtiger Einsparungseffekte getroffen worden sind oder werden sollen. Beispiele hierfür sind die Automatisierung im Zusammenhang mit der Einrichtung des Stellenpools und die Datenverarbeitung zur Durchführung des Querschnittscontrollings, konkret bei den Transferleistungen im Bereich der Sozial- und Jugendhilfe und des Wohngeldes[31]. Unverändert ist aber auch festzustellen, dass auf Forderungen nach der Umsetzung adäquater Sicherheitskonzepte mit Wehklagen über die beengten Haushaltsmittel reagiert wird. Gleichwohl ist die Zahl der uns vorgestellten Sicherheitskonzepte aufgrund der aktuellen Rechtslage signifikant gestiegen[32].

[31] Näheres dazu in 3.4
[32] Näheres dazu in 3.5

IT-Politik in der Berliner Landesverwaltung

Die an dieser Stelle vielfach erwähnten Ziele des Einsatzes von Informationstechnik in der Berliner Verwaltung liegen nach wie vor in der Straffung von Verwaltungsabläufen, in der Personaleinsparung, in der Verbesserung der Arbeitsbedingungen der Mitarbeiter und der Steigerung der Bürgernähe. Die Bedienung des Bürgers soll schneller werden, seine Wege in der Verwaltung sollen kürzer werden oder gegebenenfalls gar ganz entfallen und seine Beratung soll stärker in den Vordergrund gerückt werden. Selbstverständlich geht vielen die Entwicklung dahin nicht schnell genug. Für die schnelle Umsetzung der Vorhaben fehlt das Geld, manche Vorhaben bedürfen der sorgfältigen Planung und Abstimmung. Manche Verzögerungen liegen darin, dass die Komplexität der Vorhaben zunächst falsch eingeschätzt wurde. Einige Projekte haben mittlerweile auch Verzögerungen dadurch erfahren, dass ihre datenschutzrechtliche Relevanz zunächst völlig falsch eingeschätzt, in Einzelfällen gar ignoriert wurde, so dass die Rechtmäßigkeit der Verfahren erst in mühsamen Nachverhandlungen und Nachverbesserungen erreicht werden konnte.

Der IT-Koordinations- und Beratungsausschuss des Landes (IT-KAB), dem wir in beratender Rolle angehören, hat sich in seinen Sitzungen im Berichtsjahr erneut mit Themen befasst, die die Richtung der konkreten Entwicklungsziele der Informationstechnik in der Berliner Verwaltung festlegen sollen.

Die Berliner IT-Infrastruktur soll einen modernen *Verzeichnisdienst* erhalten, der die bisher vorhandenen Verzeichnisse zusammenführt, das Verfahren ITVB (Integriertes Telefonverzeichnis Berlin) ergänzt und damit die elektronische Kommunikation der Behörden und ihrer Mitarbeiter über das Berliner Landesnetz verbessern soll. Die Aktualität und Vollständigkeit der verfügbaren Verzeichnisdaten sollen signifikant erhöht werden, indem die Behörden möglichst alle relevanten Informationen über die Erreichbarkeit der Mitarbeiter der Berliner Verwaltung zusammentragen. Zu diesem Projekt hat der Landesbetrieb für Informationstechnik (LIT) zunächst eine Voruntersuchung angefertigt, in der ein Entscheidungsvorschlag für eine Architektur des Verzeichnisdienstes gemacht wird.

Es besteht die Absicht, in nächster Zeit das *IT-Regelwerk* des Landes einer grundlegenden Erneuerung zu unterwerfen. Eine wichtige Rolle wird dabei die künftige Rechtsform des LIT sein. Ob der LIT eine GmbH oder als Anstalt öffentlichen Rechts eingerichtet wird, hat auch datenschutzrechtliche Konsequenzen.

IT-Sicherheitspolitik in Berlin

Die Aktivitäten des IT-KAB im Zusammenhang mit der IT-Sicherheit sind besonders herauszuheben. Eine Arbeitsgruppe des IT-KAB erarbeitet derzeit ein *Modellsicherheitskonzept* für die Berliner Verwaltung auf der Grundlage des IT-Grundschutzhandbuchs des Bundesamtes für Sicherheit in der Informationstechnik[33]. Die Arbeitsgruppe, an der auch wir teilnehmen, hat mehrfach dem IT-KAB berichtet.

Eine andere Gruppe des IT-KAB, die Arbeitsgruppe IT-Sicherheit, befasst sich allgemeiner mit der Umsetzung der IT-Sicherheitsrichtlinie[34]. Sie erarbeitet unter der Federführung der Senatsverwaltung für Inneres den jährlichen *IT-Sicherheitsbericht*, der von der Richtlinie verlangt wird. Der Bericht beruht im Wesentlichen auf den Eigenangaben der befragten Behörden. Danach sind in den meisten Behörden Sicherheitskonzepte zumindest in Teilbereichen schriftlich vorhanden und umgesetzt. Umgekehrt wird die Einschätzung der beiden Berliner Kontrollbehörden Rechnungshof und Datenschutzbeauftragter bestätigt, dass behördliche Sicherheitskonzepte nur selten vollständig vorliegen und umgesetzt sind. Es ist anzunehmen, dass auch die Umfrage für 2003 zu keinem anderen Ergebnis kommt.

Fast alle Behörden gaben an, dass sie dezentrale Firewalls für den Anschluss an das Berliner Landesnetz einsetzen[35] und Maßnahmen zum Virenschutz getroffen haben. Die vom Landesbetrieb für Informationstechnik angebotene Netzverschlüsselung im Bereich des Berliner Landesnetzes wurde nach dem Bericht nur von 9 Behörden genutzt, weitere sollten 2003 dazukommen.

Die größten Risiken sehen die Behörden im Befall mit Schadenssoftware, in Qualitätsmängeln der Software und in Irrtümern und Nachlässigkeiten der Mitarbeiter. Dieses Ergebnis scheint plausibel, nicht jedoch die Selbsteinschätzung der Behörden, von denen nur vier einräumten, dass die Behördenmitarbeiter kein ausreichendes Sicherheitsbewusstsein aufwiesen.

Die Arbeitsgruppe IT-Sicherheit hat auf ihren regelmäßigen Sitzungen neben den bereits genannten Themen noch weitere Themen behandelt:

---

[33] vgl. 3.5
[34] vgl. 3.5

- Das Bezirksamt Mitte stellte ein Konzept für den effizienten und sicheren Einsatz von PDAs (Personal Digital Assistent) zur Diskussion. Dabei handelt es sich um Computer im „Westentaschenformat“, die fast die volle Funktionalität herkömmlicher Computer oder Notebooks erreichen und die insbesondere für Aufgaben verwendet werden, die im Außendienst zu erledigen sind und infolgedessen auch besonderen Risiken ausgesetzt sind.

- Das Projekt MoBüD (*Mobile Bürgerdienste*) der Senatsverwaltung für Inneres soll den mobilen Einsatz von Rechnern für das Angebot von Behördendienstleistungen (vor allem Aufgaben des Landeseinwohneramtes) dort ermöglichen, wo die Bürger anzutreffen sind und sich so Behördengänge ersparen können, z. B. in Einkaufspassagen oder anderen belebten Plätzen. Auch hier ergeben sich spezielle Sicherheitsfragen durch den mobilen Einsatz und die drahtlose Verbindung mit Fachverfahren wie z. B. dem Berliner Einwohnerwesen (EWW).

- Einsatz eines zentralen *SPAM-Filters* für das Berliner Landesnetz im Landesbetrieb für Informationstechnik zur Abwehr der überbordenden Flut von Werbe-E-Mails. Problem dabei ist, dass sichergestellt werden muss, dass nicht unbeabsichtigt relevante E-Mails ebenfalls abgewehrt werden.

- Der Umgang mit den modernen multifunktionalen Schnittstellen vom Typ *USB* (Universal Serial Bus) war ebenfalls Gegenstand von Sicherheitsbetrachtungen. Mit USB-Schnittstellen können Einschränkungen der Hardware-Ausstattung von Systemen, die aus Sicherheitsgründen vorgenommen wurden (z. B. zur Verhinderung des Einsatzes mobiler Speichermedien an Clienten-Rechnern), unterlaufen werden (z. B. mit so genannten USB-Sticks, also Halbleiterspeichern für den unmittelbaren Anschluss an USB-Schnittstellen).

Aktuelle IT-Projekte des Landes

Mehr als in den Jahren zuvor sind wir über neue IT-Verfahren in der Berliner Verwaltung unterrichtet worden, allerdings nicht immer ohne Aufforderung, wie es der Gesetzeslage nach geboten gewesen wäre (§ 24 Abs. 3 Satz 3 BlnDSG). In manchen Fällen erfuhren wir erst auf Umwegen von laufenden Projekten.

---

[35] vgl. 4.8.3

Im Bereich der *Sicherheit und Strafverfolgung* wird nach wie vor auf das neue Polizeiliche Informations- und Kommunikationssystem *POLIKS* gewartet, welches das längst veraltete Informationssystem Verbrechensbekämpfung ablösen soll. Das Projekt wurde bereits im Jahre 1995 aufgesetzt, die Inbetriebnahme ist jetzt zunächst für Ende 2004 vorgesehen. POLIKS soll aus zwei Komponenten für die Vorgangsbearbeitung und die Datenhaltung bestehen. Daraus ergeben sich datenschutzrechtliche Fragen der Zugriffsdifferenzierung zwischen den beiden Komponenten.

Die Abteilung Verfassungsschutz der Senatsverwaltung für Inneres hat frühere selbst entwickelte Pläne zur Einführung einer datenbankgestützten *Amtsdatei* zur Unterstützung der fachlichen Arbeit des Verfassungsschutzes verworfen, weil sie die Nutzung eines in der Praxis in anderen Ämtern mit ähnlicher Aufgabenstellung erprobten Verfahrens bevorzugt.

In der *Ordnungsverwaltung* wartet man seit langer Zeit auf die Erneuerung des IT-Verfahrens *Einwohnerwesen*. Die ursprünglichen Pläne, in Zusammenarbeit mit einer anderen Großstadt ein neues Einwohnerwesen zu entwickeln, wurden aufgegeben. Auch in diesem Fall ist die verantwortliche Behörde, das Landeseinwohneramt, zu der Einsicht gelangt, dass es besser ist, eine auf dem Markt angebotene Branchen-Standardsoftware für das Meldewesen auf die Anpassbarkeit an Berliner Rahmenbedingungen zu untersuchen.

Das *Führerscheinwesen* wird inzwischen einer grundlegenden Modernisierung unterworfen, die frühestens im ersten Quartal 2004 wirksam werden wird. Auch in diesem Fall wurde ein Softwareprodukt ausgewählt, welches bereits in einer Vielzahl anderer Kommunen im praktischen Einsatz ist.

Das Fachverfahren für das *Ausländerwesen* soll ebenfalls eine Modernisierung erfahren, weil spätestens bis zum Ende des Jahres 2005 das proprietäre Betriebssystem BS2000 der Siemens-Großrechner im LIT abgelöst werden soll. Für die Erneuerung des Verfahrens wurde uns ein Projekthandbuch für die Voruntersuchung vorgelegt, mit dem die Voruntersuchung bis zum Ende 2003 abgeschlossen werden sollte. Da wir entgegen unserer Bitte über weitere Meilensteine der Voruntersuchung bisher nicht unterrichtet wurden, gehen wir davon aus, dass die Zeitvorstellungen zu optimistisch gesehen wurden.

Aus dem Bereich der *Justiz* gibt es nicht viel Neues. Ein guter Überblick über die Automation im Bereich der Gerichte ist im Internet dokumentiert. Das einheitliche IT-Fachverfahren *AULAK* (Automatische Verfahren Landgericht, Amtsgerichte, Kammergericht) hält mittlerweile Einzug in die Amtsstuben der Amtsgerichte. Dieses Projekt integriert die Aufgaben der

Büroorganisation und -kommunikation mit den bestehenden Fachverfahren im Gerichtswesen.

Dies war einer der wesentlichen Beratungspunkte einer Koordinierungsrunde der behördlichen Datenschutzbeauftragten der Amtsgerichte, die unter unserer Mitwirkung zustande kam[36].

Die Senatsverwaltung für *Finanzen* hat besondere Aktivitäten entfaltet, um IT-Verfahren aufzusetzen, die unmittelbar Einsparpotenziale erschließen sollen. Im Zusammenhang mit der Einrichtung eines *Stellenpools*[37] zur Verwaltung und Vermittlung der Personalüberhangs wurde auch ein IT-Projekt durchgeführt, welches diese Fachaufgabe unterstützen soll. Ein weiterer Schwerpunkt lag auf der Planung von Verfahren zum *Querschnittscontrolling*. Dabei sind zwei Vorhaben zu nennen: Das Verfahren ePBN (elektronisches Planen, Budgetieren, Navigieren) für das ziel- und wirkungsorientierte Querschnittscontrolling in den Transferbereichen Sozialwesen, Jugendwesen und Wohngeld)[38] und das Projekt *ZWoC* (Ziel- und wirkungsorientiertes Controlling), mit dem die Ausschreibung für ein Verfahren zum Querschnittcontrolling für andere Bereiche der Verwaltung vorbereitet werden soll.

Im *Gesundheitswesen* der Bezirke wird mit dem Projekt *SpDI32* die automatisierte Basisdokumentation der sozialpsychiatrischen Dienste vorangetrieben. Das Projekt ist aus Gründen der Ergonomie noch zwischen dem Hauptpersonalrat und der Verwaltung umstritten. Aus der Sicht des Datenschutzes ist das Projekt vorrangig in Hinsicht auf den technisch-organisatorischen Schutz von Bedeutung. Dennoch ist unserem Wunsch, ein den Anforderungen entsprechendes verfahrensspezifisches Sicherheitskonzept zur Prüfung zu erhalten, so lange nicht nachgekommen worden, bis wir erfuhren, dass das Verfahren probehalber im Echtbetrieb eingesetzt wird. Demzufolge haben wir unsere Beratung eingestellt und werden den Einsatz des Verfahrens mit Echtdaten einer datenschutzrechtlichen Kontrolle unterziehen. Ein ähnliches Problem ergibt sich bei dem Verfahren *Epidem*, mit dem die Umsetzung des Infektionsschutzgesetzes in den bezirklichen Gesundheitsämtern unterstützt werden soll.

Das bereits erwähnte Verfahren ePBN für das Querschnittscontrolling betrifft besonders die Sozialämter, da Daten aus dem Fachverfahren BASIS I (PROSOZ/S), mit dem die Sozialämter seit Jahren arbeiten, in das Controllingverfahren transferiert werden. Folgt man den Vorstellungen der Senatsverwaltung für Finanzen zur weiteren Entwicklung von ePBN, so dürfte

[36] vgl. 4.8.1
[37] vgl. 4.4.1
[38] vgl. 3.4

sich das Verfahren zu einem zweiten Fachverfahren der Sozialämter entwickeln[39]. Das Verfahren BASIS I selbst ist soweit renoviert worden, dass es jetzt auch auf einem fortgeschrittenen Betriebssystem betrieben wird. Da sich in diesem Zusammenhang Sicherheitsprobleme verstärkt haben, wurde für BASIS I ein Sicherheitskonzept entwickelt, das weitere grundlegende Strukturänderungen empfiehlt[40], ohne die eine hinreichende Sicherheit nicht erreicht werden kann.

In gleicher Weise ist das *Jugendwesen* von ePBN erfasst. Gleichzeitig wird ein modernes Informationssystem Berliner Jugendhilfe (*ISBJ*) geplant, welches die verschiedenen Fachverfahren des Jugendwesens (PROSOZ/J, Kita, Zentrale Vormundschaftskasse/Unterhaltsvorschusskasse – UVK/ZVK) zusammenführen soll.

Mit der Einbeziehung der Wohngeldes in das *ePBN* soll auch im *Wohnungswesen* das Querschnittscontrolling einziehen. Unter der Projektbezeichnung *InWo* (Informationssystem Wohnungswesen) sind die verschiedenen Fachverfahren des Wohnungswesens zusammengefasst worden. Damit wurden die bisherigen Großrechnerverfahren DVWOHN (WBS,Eigentümerdatei) und DVWO3 (Wohnungskataster) sowie das PC-Verfahren WOLES (Leerstand/Zweckentfremdung) abgelöst. Das Verfahren DiWo (Wohngeld) wurde in das neue Gesamtsystem unter einer gemeinsamen Benutzeroberfläche integriert.

Bei der *BVG* sind die Arbeiten am *elektronischen Ticketing* angesichts der Umstellungen im Vorstand zunächst nur unauffällig weiterverfolgt worden. Mitte des Jahres wurde das Projekt erneut neu aufgesetzt und in den Zusammenhang bundesweiter Bemühungen der Verkehrsunternehmen für ein elektronisches Fahrgeldmanagement gestellt. Die aktuellen Vorstellungen der BVG liegen noch nicht in datenschutzrechtlich prüfbarer Form vor. Die BVG ist darauf hingewiesen worden, dass alle früher diskutierten Zielsetzungen zur Verhinderung des gläsernen ÖPNV-Nutzers in Berlin weiterhin aufrechterhalten bleiben[41].

Die *Berliner Wasserbetriebe* haben vor, die in Schächten befindlichen Wasserzähler mit Hilfe einer *Funkfernauslesung* abzulesen. Die Ableser der Wasserbetriebe sollen dann von langsam fahrenden Fahrzeugen aus mit mobilen Handheld-Endgeräten die mit entsprechenden Modulen ausgestatteten Zähler per Funk auslesen, damit sie dann in das Abrechnungsverfahren eingelesen werden können. Bei solchen Fernmessverfahren durch öffentlich-rechtliche kommunale Versorger ist § 31 a BlnDSG zu beachten. Unter anderem wird dort vorgeschrieben, dass die Einrichtung des Fernmessverfahrens nur zulässig ist, wenn die

[39] vgl. 3.4
[40] vgl. 4.4.3

Betroffenen erkennen können, wann der Dienst in Anspruch genommen wird und welcher Art der Dienst ist, und wenn der Teilnehmer den Dienst jederzeit abschalten kann, soweit dies mit dem Vertragszweck vereinbar ist (Prinzip „Rote Lampe – roter Knopf“). Das derzeit präsentierte Verfahren erfüllt die Vorschrift noch nicht. Es wird also darauf ankommen, das Verfahren so zu modifizieren, dass es den Vorgaben des Berliner Datenschutzgesetzes genügt.

3. Schwerpunkte im Berichtsjahr

3.1 Neue Sicherheitsideen - zu Lasten der Freiheit

Geschehene und verhinderte Terroranschläge, ausbleibende Fahndungserfolge oder die Verlockungen neuer technischer Möglichkeiten insbesondere im Bereich der Telekommunikation bilden spätestens seit dem 11. September 2001 die Grundlage für den Ruf nach einer Reihe neuer Maßnahmen zur Strafverfolgung und Gefahrenabwehr. Sie stellten einen wesentlichen Aspekt der öffentlichen Diskussion über den Datenschutz im Berichtszeitraum dar. Drei Themen sollen beispielhaft angesprochen werden: Die Videoüberwachung auf Bahnhöfen, die Telefonüberwachung zu präventiven Zwecken und die heimliche Nutzung der SMS-Technik. Die Forderung nach einer geradezu schrankenlosen Nutzung von DNA-Analysen, die im folgenden Abschnitt erörtert werden soll, fügt sich nahtlos an.

Am 6. April war auf dem Hauptbahnhof in Dresden vom Bundesgrenzschutz ein herrenloser Koffer gefunden worden, der einen mit hochexplosivem Sprengstoff sowie Schottersteinen gefüllten Schnellkochtopf enthielt, der nach Vermutung der Polizei auf dem belebten Bahnsteig hätte explodieren sollen. Die Tatsache, dass mit der im Bahnhof installierten Videokamera keine Aufzeichnungen gefertigt worden waren, löste bundesweit eine heftige Diskussion um die Forderung aus, dass künftig in Bahnhöfen flächendeckend Videoaufnahmen gespeichert werden sollten.

In der Tat, es ist Bestandteil des seit Ende der 90er Jahre entwickelten 3-S-Konzeptes (Service, Sicherheit, Sauberkeit) der Deutschen Bahn AG, für deren Beratung wir zuständig sind, in einer Vielzahl von Bahnhöfen Videoüberwachungsanlagen einzubauen[42]. In 3-S-Zentralen wird die Situation auf dem Bahnhof von besonders geschultem Personal beobachtet. Tritt ein sicherheitsrelevantes Ereignis ein, können die Aufzeichnung der Bilder sowie das Eingreifen von Sicherheitskräften veranlasst werden. Eine flächendeckende Speicherung wurde - abge-

---

[41] JB 2000, 3.2
[42] JB 1999, 3.2 und 4.6.3

sehen von den damit verbundenen technischen Schwierigkeiten - nicht für erforderlich gehalten, eine Rechtsgrundlage hierfür bestand und besteht auch weiterhin nicht. Nachdem mit dem BDSG 2001 eine Rechtsgrundlage für die Videoüberwachung und die Aufzeichnung der Aufnahmen unter besonderen Voraussetzungen geschaffen worden war (§ 6 b BDSG), können über die Beobachtung hinaus Daten gespeichert werden, wenn der Zweck dies verlangt und schutzwürdige Interessen nicht überwiegen (Abs. 3). Dies gilt für Bereiche, die als besonders gefährdet gelten. Insbesondere seit den Dresdener Vorkommnissen ist vor diesem Hintergrund die Ausweitung der Videoaufzeichnung auf Bahnhöfen, insbesondere im Bereich der Bahnsteige, geplant.

Die viel geforderte flächendeckende Erfassung und umfassende Speicherung von Videoaufnahmen ist gleichwohl nach wie vor nicht zulässig, auch wenn ihr Einsatz häufig als Allheilmittel gepriesen wird[43]. Das Grundrecht auf Freizügigkeit (Art. 11 GG), das zumindest in öffentlich zugänglichen Räumen auch von Privatunternehmen zu beachten ist, gewährleistet zusammen mit dem Recht auf informationelle Selbstbestimmung grundsätzlich die Möglichkeit, sich frei, unbeobachtet und ohne Aufzeichnungen befürchten zu müssen zu bewegen.

Noch viel größere Begehrlichkeiten als die Überwachung der körperlichen Bewegung im öffentlich zugänglichen Raum weckt die Überwachung der Telekommunikation. Die Aufzeichnung von Verkehrsdaten nicht nur auf der Netzebene, sondern auch bei der Nutzung von Tele- und Mediendiensten über den Zeitraum hinaus, der für die Abwicklung der damit verbundenen technischen und vertraglichen Notwendigkeiten erforderlich ist, war im Berichtszeitraum weltweit ein zentrales Thema. In Deutschland kam es im Rahmen der anstehenden Gesetzgebungsverfahren hierzu zu energischen Auseinandersetzungen[44].

Aber auch zur Überwachung der Telefongespräche selbst wird die Forderung erhoben, die bislang als rechtsstaatlich nicht erfüllbar galt, nämlich nach einer präventiven Telefonüberwachung. Während bislang das Abhören nur zur Strafverfolgung zulässig war, und zwar wenn eine Straftat von besonderem Gewicht vorliegt, besondere Tatsachen einen Verdacht begründen und in der Regel ein Richter die Maßnahme angeordnet hat, soll dies künftig auch zur vorbeugenden Verbrechensbekämpfung, also zur Gefahrenabwehr möglich sein. Das Bundesland Thüringen hat als Vorreiter bereits eine Rechtsgrundlage geschaffen (§ 34 a Polizeiaufgabengesetz), in anderen Ländern (z. B. Bayern) sind entsprechende Vorstöße gescheitert.

---

[43] vgl. 4.2.2
[44] vgl. 5.1

Im präventiven Bereich gibt es noch keine Beschuldigten; es gibt Vermutungen und Verdachtsmomente und es gibt Personen, an denen diese Vermutungen festgemacht werden. Es gibt auch keine Gewissheit, dass bestimmte Straftaten tatsächlich begangen werden, wenn die Polizei sie nicht verhindert. In diesem unsicheren Raum will der Staat seine Bürger überwachen, weil er die Möglichkeit sieht, Straftaten verhindern zu können. Die Überwachung der Telekommunikation greift hier allein in Grundrechte Unbeteiligter ein, weil eine Straftat noch nicht begangen worden ist und es auch ein Ermittlungsverfahren eben gerade noch nicht gibt. Bei einem derartigen Vorfeldeingriff kann niemand wissen, ob die Polizei auch seine Daten aus seiner unbeobachteten Kommunikation erhebt. Auch ein Schaden für die Telekommunikationsüberwachung im Rahmen eines Strafverfahrens wird von den Experten befürchtet.

Auch wenn noch gar keine ausdrückliche Rechtsgrundlage vorhanden ist, verlocken verfügbare Techniken schon zum Gebrauch. Ein Beispiel ist die Nutzung der Möglichkeiten der Stealth- (Tarnkappen-)Technik („Stille SMS“) beim Versenden von SMS-Nachrichten über Mobiltelefon.

Mit Hilfe (allgemein verfügbarer) Software können Nachrichten so an Handys geschickt werden, dass der Besitzer des Handys dies nicht bemerkt. Die Folge ist allerdings, dass beim Telekommunikationsunternehmen Verkehrsdaten insbesondere über den Standort des Handys entstehen. Im Berichtszeitraum wurde bekannt, dass sich die Polizei dieses Verfahren zunutze macht, um den Standort verdächtiger Personen, deren Handynummer sie kennt, zu ermitteln[45]. Eine ausdrückliche Rechtsgrundlage hierfür gibt es nicht, eine heftige dogmatische Diskussion darüber wurde ausgelöst, wie die vorhandenen Befugnisnormen (§§ 100 a, 100 g, 100 i Strafprozessordnung – StPO) entsprechend zurechtgebogen werden könnten. So recht gelingt es in keinem Fall. Jedenfalls greift die vom Bundesministerium der Justiz im Rahmen einer Kleinen Anfrage vertretene Auffassung, die §§ 161 Abs. 1, 163 Abs. 1 StPO reichten als Rechtsgrundlage aus, zu kurz. Der kleinste gemeinsame Nenner muss zumindest sein, dass eine richterliche Anordnung zur Herausgabe der Standortdaten durch den Netzbetreiber nach § 100 g StPO vorliegen muss, bevor die stille SMS versandt wird.

Bei einer stichprobenartigen Prüfung der Retente von Verfahren des Landeskriminalamtes, in denen eine stille SMS versandt worden ist, haben wir festgestellt, dass dies in den meisten Fällen der Fall war.

[45] Der Spiegel 15/2003, S. 192

Es bleibt das rechtsstaatlich bedenkliche Problem, dass sich bei dieser Vorgehensweise die Polizei überhaupt erst heimlich (nämlich durch Versenden der stillen SMS) die Voraussetzungen dafür schafft, damit die Rechtsgrundlagen für das weitere Vorgehen (nämlich das Herausverlangen der Standortdaten vom Netzbetreiber) vorliegen.

3.2 Der Ruf nach dem genetischen Fingerabdruck

Die Analyse des menschlichen Erbmaterials DNA zu Zwecken der Personenidentifizierung entwickelt sich zunehmend zu einem zentralen Instrument der Kriminalistik. Spektakuläre Fahndungserfolge, teilweise viele Jahre nach der Straftat, belegten dies in den letzten Monaten. So ist es nicht erstaunlich, dass im Berichtsjahr mehrere Gesetzesinitiativen auf Bundes- und Landesebene auf den Weg gebracht wurden, um den Anwendungsbereich für die DNA-Analyse auszuweiten bzw. die Anforderungen für eine Aufnahme in die Zentrale DNA-Analysedatei des Bundeskriminalamts abzusenken.

Die Bundesregierung hat einen Gesetzentwurf vorgelegt[46], mit dem zu den Straftaten von erheblicher Bedeutung als Anlasstat auch eine Straftat gegen die sexuelle Selbstbestimmung (§ 174 – 184 f. StGB) hinzutreten soll, wenn eine Prognose vorliegt, dass künftig Straftaten von erheblicher Bedeutung zu befürchten sind. Gleichzeitig sieht der Gesetzentwurf aber auch eine Präzisierung der Begründungspflicht der richterlichen Anordnung vor (§ 81 g Abs. 3 Satz 2 StPO). Danach müssen künftig Tatsachen, die für die Erheblichkeit der Straftat im Sinne des § 81 g Abs. 1 Ziff. 1 StPO bestimmend sind, Erkenntnisse, aufgrund derer Grund zu der Annahme besteht, dass gegen den Beschuldigten künftig Straftaten von erheblicher Bedeutung zu erwarten sein werden, und die in die Abwägung einfließenden Umstände im Einzelfall dargelegt werden.

Einzelne Bundesländer streben dagegen eine erhebliche Erweiterung des Kataloges der Anlasstaten an. Dies geht von einer Ausweitung auf alle Straftaten mit sexuellem Hintergrund als Anlasstat bis hin zur Aufnahme weiterer Delikte aus dem Bereich der Betäubungsmittelkriminalität. Gleichzeitig soll für die Aufnahme der Straftaten mit sexuellem Hintergrund in die BKA-DNA-Analysedatei eine Gefahrenprognose entfallen.

In Berlin wie auch in anderen Bundesländern bemüht sich die CDU um eine Bundesratsinitiative, mit der die DNA-Analyse rechtlich den erkennungsdienstlichen Maßnahmen gleichge-

[46] BT-Drs. 15/350

stellt werden soll. Der genetische Fingerabdruck soll entsprechend den Regelungen zum normalen Fingerabdruck zur Standardmaßnahme in der Verbrechensbekämpfung werden[47].

Vor einer Ausweitung des Anwendungsbereiches der DNA-Analyse zum Zwecke der Strafverfolgung hat eine Rechtsgüterabwägung unter besonderer Beachtung des Grundsatzes der Verhältnismäßigkeit zu erfolgen. Die DNA-Entnahme, -Analyse und -Speicherung greifen tief in das informationelle Selbstbestimmungsrecht des Einzelnen ein[48]. Die Entnahme des DNA-Materials stellt zunächst einen körperlichen Eingriff dar. Das DNA-Material selber darf nach § 81 e StPO untersucht werden zur Feststellung der Abstammung oder der Tatsache, ob aufgefundenes Spurenmaterial von dem Beschuldigten oder Verletzten stammt. Durch die Vorgaben des Gesetzgebers dürfen nur die nicht-codierten Teile der DNA untersucht werden. Bei den Untersuchungen des nicht-codierten Teils fallen bereits heute Zusatzinformationen an, die nach der Vorgabe des Gesetzgebers nicht untersucht werden dürfen. Unstrittig fällt als Zusatzinformation die Feststellung des Geschlechtes an, soweit die Standarduntersuchungen durchgeführt werden. Möglich sind heute auch schon Zusatzinformationen durch eine Altersabschätzung, über bestimmte Haarfarben oder eine ethnische Zuordnung. Der Begriff „Zusatzinformation“ besagt, dass es sich nicht um ausdrücklich untersuchte Informationen handelt, sondern um Abfallprodukte der Untersuchungen. Es gibt keine Garantie dafür, dass durch Fortschritte in der Analysetechnik nicht immer mehr Zusatzinformationen anfallen, die im Einzelfall von Interesse sein können. Sowie bei Untersuchungsaufträgen auch heute schon einmal ausdrücklich nach dem Geschlecht gefragt wird, obwohl § 81 e StPO eine Untersuchung darauf nicht erlaubt, besteht die Gefahr, dass mit immer mehr Informationen, die bei den Untersuchungen als Nebenprodukt abfallen, immer mehr Begehrlichkeiten geweckt werden.

Die Tatsache, dass heute immer mehr Spuren am Tatort aufnehmbar sind, die menschliche DNA enthalten, birgt zusätzliche Risiken in sich. Bereits die kleinste aufgefundene Hautschuppe ist Träger des DNA-Identifizierungsmusters. Die Beweislast wird damit für alle, die Spuren hinterlassen haben, erdrückend. In Anhörungen haben Experten immer wieder darauf hingewiesen, dass auch bewusst falsche Spuren durch am Tatort hinterlassenes fremdes DNA-Material gelegt werden können. Dies kann die Zigarette mit Speichel oder ein einzelnes Haar einer anderen Person sein. Für den dann Verdächtigten ist es schwer, sich gegen die hohe Übereinstimmungswahrscheinlichkeit nach einer DNA-Untersuchung zur Wehr zu setzen.

---

[47] Abghs.-Drs. 15/1798

[48] Beschluss des Bundesverfassungsgerichts vom 14. Dezember 2000, Az.: 2 BvR 1741/99

Die Ausweitung auf weniger gewichtige Straftaten, aber auch die Bestrebungen, die DNA-Identifizierungsmuster rechtlich dem Fingerabdruck gleichzusetzen, werden der Tiefe eines solchen Eingriffs in das Recht auf informationelle Selbstbestimmung nicht gerecht. Der Fingerabdruck enthält keine so weitgehenden Zusatzinformationen über den Inhaber. Er enthält keine Gesundheitsinformationen und Wahrscheinlichkeiten über den Ausbruch bestimmter Krankheiten. Er ist auch nicht ohne Wissen des Inhabers aus den unterschiedlichsten Körpersubstanzen zu gewinnen. Aus datenschutzrechtlicher Sicht verbietet sich damit ein Vergleich der Maßnahmen.

Auch die Tendenz, den Richtervorbehalt bei eingriffsintensiven Maßnahmen wie der DNA-Analyse oder auch der Speicherung in der BKA-DNA-Analysedatei zu streichen, ist nicht hinnehmbar. Dem Richter muss vielmehr eine viel stärkere eigene Prüfpflicht für das Vorliegen der gesetzlichen Vorgaben und die Einhaltung des Grundrechts der Erforderlichkeit zukommen. Dem Richtervorbehalt kommt eine grundrechtssichernde Funktion zu. Seine Bedeutung wird umso größer, je tiefer in Grundrechte eingegriffen wird.

Auch bei der Entscheidung über eine Aufnahme in die DNA-Analysedatei kommt dem Richtervorbehalt und damit einer einzelfallorientierten unabhängigen Prognoseentscheidung für die Begehung künftiger Straftaten von erheblicher Bedeutung eine große Wichtigkeit zu. Die gesetzliche Regelung einer einzelfallbezogenen Begründungspflicht durch den Richter wäre deshalb ein wichtiger Schritt. Wünschenswert sind auch spezielle für derartige Anordnungen zuständige Richter, um die erforderliche Sachkenntnis einfließen lassen zu können.

Die Datenschutzbeauftragten des Bundes und der Länder haben eine Entschließung zu den Bestrebungen in den einzelnen Bundesländern, die Anwendung der DNA-Analyse zu erweitern, verabschiedet[49].

3.3 Elektronische Werbung

Am 27. Januar 2004 teilte der EU-Kommissar Erkki Liikanen (Finnland) mit, dass im Dezember 2003 der Anteil der unerwünschten Werbebotschaften bei den empfangenen E-Mails in Europa erstmals über 50 % (52 %) gestiegen ist. Es gibt Befürchtungen, dass bald nur noch jede dritte empfangene E-Mail keine Werbe-Mail ist. Diese stellen nicht nur eine Belästigung des Betroffenen dar. Sie werden zunehmend auch zu einem negativen Wirtschaftsfaktor, da

[49] Entschließung vom 16. Juli 2003, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2003“, S. 34

es für viele Unternehmen immer zeitaufwendiger und schwieriger wird, Werbe-E-Mails von wichtiger Geschäftspost zu trennen. So verwundert es nicht, dass Bill Gates vor kurzem angekündigt hat, in den nächsten anderthalb Jahren eine Software zu entwickeln, die den Empfang von unerwünschten Werbe-E-Mails nicht nur erschwert, sondern verhindert.

Nicht nur im E-Mail-Bereich ist die Anzahl der Werbebotschaften sprunghaft gestiegen, auch bei der Werbung per Telefax und SMS steigt die Anzahl der Eingaben Betroffener. Demgegenüber spielt die telefonische Werbung nur eine untergeordnete Rolle. Insbesondere für die Werbe-E-Mails hat sich der Begriff „SPAM“ durchgesetzt. Der Namensgeber ist ein einfacher Dosenschinken (Spiced Ham), dessen Genuss offenbar genauso viel Freude bereitet wie das Lesen einer Werbe-E-Mail. Das Thema SPAM ist inzwischen zu einem beliebten Thema in den Medien geworden. Zeitungen titeln dieses Thema mit Überschriften wie „Geisel des Internets“, „Eine Plage namens SPAM“, „Feldzug gegen den SPAM-Müll“, „Es ist die Pest, die reine Pest“, „Verdammt und zugemüllt“ etc. Politiker in vielen Ländern überlegen, wie man erfolgreich gegen SPAM kämpfen kann. So will etwa der australische Minister für Kommunikation und Informationstechnologie Richard Alston die Versender von unverlangten Werbe-Botschaften mit bis zu umgerechnet 650.000 Euro Strafe belegen.

Rechtliche Bewertung

Die Versendung unerwünschter elektronischer Werbung kann sowohl gegen datenschutzrechtliche, aber auch gegen zivilrechtliche und wettbewerbsrechtliche Vorschriften verstoßen. Zivilrechtlich werden vor allem Verstöße gegen das Eigentum (Faxpapier), das Recht am eingerichteten und ausgeübten Gewerbebetrieb sowie das allgemeine Persönlichkeitsrecht angenommen. Nach §§ 823, 1004 BGB kann der Betroffene wegen Verletzung eines Rechtsgutes einen Unterlassungsanspruch und /oder Schadensersatzansprüche geltend machen.

§ 1 des Gesetzes gegen den unlauteren Wettbewerb (UWG) sanktioniert Wettbewerbshandlungen, die gegen die guten Sitten verstoßen. Rechtsfolgen sind auch hier Unterlassungs- bzw. bei Verschulden Schadensersatzansprüche. Eine der Fallgruppen der Sittenwidrigkeit nach § 1 UWG ist der „Kundenfang“. Hierzu zählt auch die unverlangte elektronische Werbung. Es kann grundsätzlich davon ausgegangen werden, dass wettbewerbswidrige elektronische Werbebotschaften auch einen Verstoß gegen das Datenschutzrecht des Betroffenen darstellen. Nur in den Grenzen des Wettbewerbsrechts hat die verantwortliche Stelle ein berechtigtes Interesse an der Datenerhebung, -verarbeitung und -nutzung zu Werbezwecken.

Das Datenschutzrecht des Betroffenen ist ausnahmsweise dann nicht tangiert, wenn die verantwortliche Stelle E-Mail-Adressen, Faxnummern etc. (zufällig) generiert. Da die verantwortliche Stelle bei der Versendung der elektronischen Werbung keine Information darüber hat, ob die E-Mail-Adresse bzw. die gewählte Nummer existiert und zu einer natürlichen Person gehört, ist das informationelle Selbstbestimmungsrecht des Betroffenen in diesen Fällen nicht tangiert.

Nach ständiger Rechtsprechung des BGH[50] stellen unaufgeforderte Werbeanrufe bei Privatpersonen eine besonders schwere Beeinträchtigung des allgemeinen Persönlichkeitsrechts (Privatsphäre) der angerufenen Person dar. Durch die Anrufe werde der auf eigene Kosten und im eigenen Interesse des Inhabers unterhaltene Telefonanschluss grob missbraucht. Es werde praktisch unkontrollierbar in die Lebensgewohnheiten des Angerufenen eingedrungen, der Werbende bestimme den Zeitpunkt der Werbemaßnahme und dränge sie der angerufenen Person in seiner häuslichen Umgebung auf. Auch bei vorheriger brieflicher Ankündigung des Anrufes bleibt der Anruf rechtswidrig. Diese Werbeanrufe stellen einen Verstoß gegen § 1 UWG dar, wenn die angerufene Person zuvor nicht ausdrücklich oder konkludent ihr Einverständnis mit dem Anruf erklärt hat. Ein vermutetes Einverständnis reicht anders als im geschäftlichen Bereich nicht aus.

Die Werbung per Telefax beurteilt der BGH[51] im Ergebnis ähnlich wie die per Telefon: bei Privatpersonen ist sie grundsätzlich unzulässig. Besonders berücksichtigt wird hierbei, dass den Empfängern der Werbung zusätzliche Kosten für Papier und Toner entstehen und das Empfangsgerät für einige Zeit blockiert wird. Zudem müssten die Empfänger Zeit, Mühe und zusätzliches Personal aufwenden, um die Werbebotschaft als solche zu identifizieren und auszusondern.

Zur Beurteilung der Zulässigkeit von unverlangt zugesandten Werbe-E-Mails liegt noch keine höchstrichterliche Rechtsprechung vor. Von den Instanzgerichten hält die Mehrzahl diese Form der Werbung bei fehlender vorheriger Einwilligung für unzulässig. Die Werbung muss ausdrücklich erklärt worden oder mutmaßlich vorhanden sein.

Das LG Berlin[52] begründet die Unzulässigkeit der unaufgeforderten Zusendung von Werbe-E-Mails und den Verstoß gegen § 823 Abs. 1 BGB damit, dass die Empfänger die E-Mails

---

[50] vgl. umfangreiche Nachweise bei Wolber, Tanja; Eckhardt, Jens: Zulässigkeit unaufgeforderter E-Mail-Werbung? In: DB 2002, S. 2581 (2582, Fn. 7) und Baumbach, Adolf; Hefermehl, Wolfgang: Wettbewerbsrecht. München: C. H. Beck, 2001, § 1 UWG (Rn. 67)

[51] Urteil vom 25. Oktober 1995, Az.: I ZR 255/93

[52] Beschlüsse vom 14. Mai 1998, Az.: 16 O 301/98 und vom 2. April 1998, Az.: 16 O 201/98

nur unter Verursachung von Kosten für Telefon- und Providergebühren lesen und als Werbung erkennen können. Das Gericht betont, dass diese Anforderungen grundsätzlich unabhängig davon gelten, ob es sich bei den Empfängern um Privatpersonen, Freiberufler oder Gewerbetreibende handelt.

Unaufgeforderte Werbung liegt vor, wenn der Empfänger der E-Mails der Zusendung zuvor nicht zugestimmt hat oder das Einverständnis nicht aufgrund bestehender Geschäftsbeziehungen vermutet werden kann. Der Versender der E-Mail-Werbung ist darlegungs- und beweispflichtig für das Vorliegen dieser Voraussetzungen. Ein Interesse an Werbe-E-Mails kann keineswegs allein deshalb vermutet werden, weil der potenzielle Empfänger auf seiner Homepage auch seine E-Mail-Adresse angegeben hat.

Die EG-Datenschutzrichtlinie für die elektronische Kommunikation[53] sieht jetzt außerhalb bestehender Geschäftskontakte die „Opt-in-Lösung“ vor. Obwohl dieses Ergebnis von den Gerichten auch durch die Auslegung der Generalklausel des § 1 UWG erzielt wurde, hat die Bundesregierung in dem Entwurf eines Gesetzes gegen den unlauteren Wettbewerb[54] die elektronische Werbung im Einzelnen geregelt. § 7 des Entwurfes stellt dabei in Abs. 2 Nrn. 2 und 3 klar, dass Werbung mit Telefonanrufen, unter Verwendung von automatischen Anrufmaschinen, Faxgeräten oder elektronischer Post eine unzumutbare Belästigung darstellt und damit rechtswidrig ist, sofern nicht eine Einwilligung des Adressaten vorliegt. Eine Änderung gegenüber dem bisherigen Rechtzustand ist insbesondere darin zu sehen, dass diese Regelung auch im geschäftlichen Bereich uneingeschränkt gilt. Der Gesetzentwurf verbietet auch Werbung mit elektronischen Nachrichten, unter Verschleierung oder Verheimlichung der Identität des Absenders.

Für die Wirtschaft ist insbesondere von Bedeutung, dass der Gesetzentwurf nunmehr Klarheit schafft bei der Frage, in welchem Umfang Kunden elektronisch beworben werden können. Hier hat sich der Gesetzgeber für ein „Soft-opt-in-Prinzip“ entschieden (§ 7 Abs. 3 des Entwurfs). Danach kann das Unternehmen Kunden, die nicht der elektronischen Werbung widersprochen haben, für ähnliche Waren und Dienstleistungen werben, wenn der Kunde bei der Erhebung der Adresse und bei jeder Nutzung klar und deutlich darauf hingewiesen wird, dass er diese Nutzung jederzeit untersagen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

---

[53] vom 12. Juli 2002, ABl. EG L 201, S. 37
[54] BT-Drs. 15/1487

Technische Hintergründe

Das E-Mail-Verfahren, eines der ältesten Anwendungen im Internet, ist ein sehr einfach gehaltenes Verfahren. Es kommt ohne Absenderkontrolle, ja sogar ohne Absenderangabe aus. Der E-Mail-Versand erfolgt dabei ähnlich wie bei der bekannten Briefpost. Es genügt die korrekte Angabe der Empfängeradresse, um einen Empfänger zu erreichen. Da die Angabe des Absenders optional ist und eine Überprüfung der Absenderangaben nicht stattfindet, ist auf diese Angaben in E-Mails in der Regel kein Verlass.

Alle Angaben zu Empfänger, Absender, Erstellungsdatum und den am Transport beteiligten Systemen (MTAs) finden sich im Kopf der Nachricht (Header).

Die Rückverfolgung zum Urheber der Nachricht kann nur über die Angaben im (erweiterten) Header der Nachricht erfolgen. Hier tragen sich alle Mail-Transport-Systeme ein, welche die Nachricht weitergeleitet haben. Aber auch hier gilt: Jeder MTA übernimmt die Transporthistorie vom sendenden System und ergänzt sie um einen eigenen Eintrag. Ein MTA trägt in die Transporthistorie sowohl Informationen zum eigenen System (Name oder IP-Adresse, Datums- und Zeiteintrag) sowie zumindest die IP-Adresse des MTA ein, von dem die Nachricht empfangen wurde. Alle weiteren Angaben in der E-Mail wie Absender, Erstellungsdatum und bisherige Transporthistorie können problemlos vom vorhergehenden MTA gefälscht oder verfälscht worden sein. Spammer nutzen diesen Umstand gezielt, um ihre Urheberschaft zu verbergen, so dass auf diesem Wege eine Rückverfolgung in den meisten Fällen unmöglich ist. Sie nutzen dabei fehlkonfigurierte MTAs, welche E-Mail unbeschränkt annehmen und weiterleiten (sogenannte „open relays“) oder versenden schlicht aus dem Ausland.

Selbstschutzmaßnahmen und Vorsorge

Der SPAM-Problematik lässt sich zurzeit nur mittels Inhalts- und Header-Analyse entgegenwirken. Hierbei wird nach bestimmten Merkmalen in eingegangenen E-Mails gesucht. Die „Treffer“ werden ausgefiltert. Diese SPAM-Filter werden mittlerweile in den verschiedensten Varianten als Software für Endgeräte und MTAs oder als Dienstleistung angeboten. Allen gemein ist, dass sie immer nur so gut sein können wie das ihnen zugrunde liegende Regelwerk. Im Allgemeinen rechnet man mit einer Fehlerkennungsrate von mindestens 10 % (falsch positive und falsch negative Treffer). So sind diese Filter eine große Hilfe bei der Vorsortierung – die endgültige Entscheidung zum Löschen sollten sie nicht treffen.

Noch wünschenswerter als mit Programmen gegen SPAM zu kämpfen wäre es, erst gar nicht so viele unerwünschte E-Mails zu erhalten. Hier hilft es bereits, die eigene E-Mail-Adresse möglichst nur an ausgewählte Personen weiterzugeben und niemals auf SPAM-Mails zu antworten. Erst recht nicht, wenn dort suggeriert wird, man könnte sich aus diesen Verteilern austragen – die Antwort (oder ein Klick auf den angegebenen Link) bestätigt dem SPAM-Versender, dass die E-Mail nicht nur empfangen, sondern offenbar auch gelesen wurde. Der „Wert" dieser Adresse steigt und wird gewinnbringend an andere SPAM-Versender weiterverkauft!

Unser Tipp: Mehrere E-Mail-Adressen nutzen und gut überlegen, welche davon wo veröffentlicht bzw. an wen sie weitergegeben werden. Weitere Tipps und Hinweise zu Selbstschutzmaßnahmen werden auf unserer Website[55] veröffentlicht.

3.4 Controlling bei sozialen Transferleistungen – ein Modellprojekt der Verwaltungsreform?

Im Jahresbericht 1999 berichteten wir über das Vorhaben, Methoden des Querschnittscontrollings im Zuge der Verwaltungsreform in der Berliner Verwaltung einzuführen[56]. Damals wurde im Zusammenwirken mit einer Unternehmensberatung von der Senatsverwaltung für Gesundheit und Soziales ein Pilotprojekt bei der Umsetzung des sozialpolitischen Programms „Integration durch Arbeit" durchgeführt. Die Unternehmensberatung entwickelte dafür ein Programm, bei dem der Zugriff auf die personenbezogenen Daten der Hilfeempfänger auf diejenigen Sachbearbeiter der Sozialämter beschränkt war, die ohnehin mit dem Fall beschäftigt waren. Für die Auswertung auf dem zentralen Server der Senatsverwaltung wurden die identifizierenden Daten mit einem symmetrischen Verschlüsselungsverfahren pseudonymisiert und es wurde sichergestellt, dass die Senatsverwaltung den Schlüssel nicht verwenden kann. Rechtsgrundlage für die Zweckänderung der Sozialdaten war § 67 c Abs. 3 Sozialgesetzbuch (SGB) X , da das zeitlich begrenzte Pilotprojekt als Organisationsuntersuchung eingestuft werden konnte.

Drei Jahre später führte die Senatsverwaltung für Bildung, Jugend und Sport ein weiteres Pilotprojekt im Bereich der Jugendberufshilfe durch. Es wurde die inzwischen unter dem

[55] http://www.datenschutz-berlin.de/spamschutz
[56] JB 1999, 4.4.3

Namen ePBN (electronic Product Budget Navigator) weiterentwickelte Software der gleichen Unternehmensberatung eingesetzt.

Beide Pilotprojekte betrafen inhaltlich scharf abgegrenzte und vergleichbare Fragestellungen: Wie können die Angebote der Sozial- und Jugendhilfe zur Eingliederung von Hilfeempfängern in den Arbeitsmarkt so gestaltet werden, dass die vorhandenen Mittel mit optimalem Erfolg eingesetzt werden?

Anfang 2003 unterrichtete uns der behördliche Datenschutzbeauftragte der Senatsverwaltung für Finanzen offiziell darüber, dass seine Verwaltung beauftragt sei, einen Senatsbeschluss vom 17. Dezember 2002[57] umzusetzen, wonach bis zum 1. Juni 2003 das IT-Verfahren ePBN für das integrierte Berichtswesen für die Transferausgaben der Bezirke in den Bereichen Jugend, Soziales und Wohnen im Echtbetrieb in allen Bezirksverwaltungen einzuführen war. Zu dem Auftrag gehörte auch unsere Beteiligung, die aus gesetzlichen Gründen ohnehin geboten war und die gemeinsam mit dem behördlichen Datenschutzbeauftragten durchzuführende Vorabkontrolle enthielt.

Die Entscheidung des Senats, ePBN im gesamten Bereich der sozialen Transferleistungen des Landes einzusetzen, beruhte auf Erfahrungen der Pilotprojekte und erfolgte ohne Ausschreibung. Deswegen bestand in der Projektbegleitung das Problem, dass keine Ausschreibungsunterlagen existierten, von denen ein Pflichtenheft konkrete – und über allgemeine politische Absichtserklärungen hinausgehende – Aussagen zu den Projektzielen hätte geben können. Statt dessen wurden uns diverse Dokumente überreicht, die ausschließlich von der Unternehmensberatung erstellt und offenkundig von der für das Projekt verantwortlichen Senatsverwaltung für Finanzen nicht weiter geprüft worden waren.

In einer ersten Stellungnahme gegenüber der Senatsverwaltung für Finanzen stellten wir fest, dass die Unterlagen insgesamt keine verbindliche Verfahrensbeschreibung darstellten. Zum Teil wurden die Möglichkeiten beschrieben, die das Programmpaket bieten kann, zum Teil gab es auf den engeren Informationsbedarf unseres Haus zugeschnittene Angaben, die jedoch angesichts der Unverbindlichkeit der Verfahrensunterlagen nicht von aktuellem Wert waren. Wir machten darauf aufmerksam, dass parallel zu unserer Unterrichtung ständige Modifikationen des Verfahrens aufgrund der Diskussionen in den betroffenen Verwaltungen erfolgten, jedoch eine verbindliche Planungsunterlage der Senatsverwaltung für Finanzen nicht vorlag. Deutlich wurde nur die verständliche Absicht der Unternehmensberatung, für

[57] Senatsbeschluss Nr. 780/02

das finanz- und fachpolitische Controlling im Bereich der Sozialhilfe die notwendige Software zu liefern.

Wir erbaten von der Senatsverwaltung für Finanzen eindeutige Aussagen, wie das Querschnittscontrolling durchgeführt werden soll, welche Daten über welche Personen (Klienten, Mitarbeiter) in welchem Zustand (personenbezogen, pseudonym, anonym, aggregiert) zwischen verschiedenen datenschutzrechtlichen Verantwortungsträgern übermittelt werden sollten. Auf der Grundlage dieser Unterrichtung hatten wir eine erschöpfende Stellungnahme zu den datenschutzrechtlichen Aspekten zugesagt.

In Unkenntnis rechtlicher Gegebenheiten hatte die auch insoweit von der Senatsverwaltung nicht unterstützte Unternehmensberatung den Senatsbeschluss als Rechtsgrundlage für das Projekt ePBN angegeben. Der in den Pilotprojekten herangezogene § 67 c Abs. 3 SGB X war auf das neue Projekt nicht mehr anwendbar, weil das Controlling auf Dauer angelegt ist und somit nicht mehr als Organisationsuntersuchung angesehen werden konnte.

Nach § 67 c Abs. 5 SGB X dürfen für Zwecke der Planung im Sozialleistungsbereich erhobene oder gespeicherte Daten von den Leistungsträgern für ein bestimmtes Vorhaben der Planung im Sozialbereich verändert oder genutzt werden. Die Sozialdaten sind zu anonymisieren, sobald dies nach dem Forschungs- oder Planungszweck möglich ist. Bis dahin sind jene Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können (Pseudonymisierung). Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Planungszweck dies erfordert. Das auf Dauer angelegte Querschnittscontrolling kann als Planungsvorhaben nach § 67 Abs. 5 SGB X angesehen werden, denn es soll dadurch die Finanz- und Sozialplanung im Bereich der Leistung nach Bundessozialhilfegesetz (BSHG) dauerhaft beeinflusst werden.

Die in § 67 c Abs. 5 SGB X gegebene Befugnis zur Änderung des Verarbeitungszwecks bezieht sich auf die Leistungsträger. Träger der Sozial- und Jugendhilfe und des Wohngeldes ist zwar das Land Berlin. Jedoch erfüllt das Land Berlin diese Aufgabe durch die zuständigen Verwaltungseinheiten, die im Rahmen ihrer Aufgabenerfüllung als speichernde Stelle im Sinne des Datenschutzrechts und des Sozialdatenschutzrechts auftreten. Nach § 67 Abs. 9 Satz 3 SGB X sind insoweit die Organisationseinheiten verantwortlich speichernde Stellen, die Aufgaben nach einem der besonderen Teile dieses Gesetzbuchs funktional durchführen. Dies sind in Berlin die zuständigen Ämter der Bezirksverwaltung, z. B. die Sozial- und Jugendämter und Wohngeldstellen, nicht jedoch die Senatsverwaltung für Soziales und schon

gar nicht die Senatsverwaltung für Finanzen. Von den Bezirksämtern wäre eine Übermittlung personenbezogener Sozialdaten an die Senatsverwaltung für Finanzen nicht zulässig, da es dafür keine Rechtsgrundlage gibt. Keine Bedenken bestehen jedoch dagegen, dass Ergebnisse des Querschnittcontrollings ohne Personenbezug (d. h. anonymisiert oder pseudonymisiert) an die Senatsverwaltung für Finanzen übermittelt werden. Da die Ergebnisse des Querschnittscontrollings aggregierte Daten sind, ist auch für die Einzeldaten, aus denen die aggregierten Daten erzeugt werden, kein Personenbezug erforderlich.

Praktisch bedeutet dies, dass die bei den Leistungsträgern für das Querschnittscontrolling verfügbaren personenbezogenen Daten vor der Übermittlung an die für das Querschnittscontrolling zuständige Stelle anonymisiert werden müssen. In Frage kommt auch eine unidirektionale Pseudonymisierung, die es zwar ermöglicht, den Datensätzen später entstehende Daten zuzuordnen, die aber jegliche Rückschlüsse auf die betroffene Person ausschließt.

Nach den uns zuerst übergebenen Unterlagen sollten auch personenbezogene Daten von Mitarbeitern der Leistungsträger erhoben werden. Nachdem wir auf die rechtlichen Rahmenbedingungen für die Verarbeitung dieser Daten hingewiesen hatten, wurde entschieden, dass von der Verarbeitung solcher Daten abgesehen wird.

Später wurde deutlich, dass die Einführung von ePBN in drei Phasen erfolgen soll. In der *ersten* Phase sollen die Daten aus den Fachverfahren PROSOZ/S (Sozialhilfe), PROSOZ/J (Jugendhilfe) in InWo (Wohngeld) unidirektional pseudonymisiert werden, bevor sie in den zentralen Auswertungsdatenbestand überführt werden. Allein diese Phase sollte nach dem Willen der Senatsverwaltung für Finanzen zunächst in die Vorabkontrolle einbezogen werden. Für die anderen Phasen sollte eine gesonderte Unterrichtung erfolgen.

In der *zweiten* Phase ist vorgesehen, dass zusätzliche Daten, die zwar bei der Einzelfallbearbeitung anfallen, aber nicht im Fachverfahren verfügbar sind, zusätzlich erfasst werden. Zur Pflege dieser Daten durch den Sachbearbeiter ist eine bidirektionale Pseudonymisierung vorgesehen, also eine Pseudonymisierung, die der Sachbearbeiter wieder rückgängig machen kann. Für diese Phase ist eine Rechtsgrundlage noch nicht erkennbar.

Gleiches gilt für die *dritte* Phase, in der die ziel-/wirkungsorientierte Steuerung sogar auf den Einzelfall zurückgreifen soll, somit also ein zweites Fachverfahren in den drei Transferbereichen entsteht.

Schließlich wurde verabredet, dass in der ersten Phase an der Schnittstelle zwischen Fachverfahren und ePBN auf bestimmte unveränderbare Merkmale des Leistungsempfängers ein kryptografisches Pseudonymisierungsverfahren angewendet wird. Alle anderen identifizierenden Angaben werden gelöscht und nicht in den zentralen Auswertungsdatenbestand überführt. Offen ist noch, wie der räumliche Bezug im Auswertungsbestand hergestellt wird, da die Adresse die Pseudonymität in den meisten Fällen aufheben würde. Wir haben empfohlen, keine feineren Strukturen als die Statistischen Gebiete zu verwenden.

Für die Pseudonymisierung hat die Unternehmensberatung den Einsatz des AES-Algorithmus (Advanced Encryption Standard) empfohlen. Als das aktuelle symmetrische Standardverschlüsselungsverfahren ist der AES sicher die richtige Wahl für Verschlüsselungsprobleme in geschlossenen Benutzergruppen oder als symmetrische Komponente hybrider Verschlüsselungsverfahren (wie z. B. PGP), als unidirektionales Pseudonymisierungsverfahren ist es jedoch geradezu kontraproduktiv, denn mit dem gleichen Schlüssel, mit dem das Pseudonym aus den Grunddaten ermittelt wird, können die Grunddaten wieder aus dem Pseudonym errechnet werden. Unser Vorschlag war, einen kryptografischen Hash-Algorithmus zu verwenden, der unumkehrbar ist[58]. Den Vorschlag, den Algorithmus SHA-1 (Secure Hashing Algorithm) zu verwenden, haben wir akzeptiert.

Die Diskussion um die Gestaltung des ePBN ist längst nicht abgeschlossen. So wurde von der Unternehmensberatung jüngst ins Feld geführt, dass nach Ansicht beteiligter Behörden im zentralen Datenbestand eine Konsistenzprüfung der eingestellten Datenbestände erfolgen müsse, obwohl die Daten aus Fachverfahren stammen, die gleichzeitig Zahlungsverfahren sind, und daher intensiven Prüfungen unterzogen waren. Es wurde deshalb vorgeschlagen, dass bestimmte Daten, die den Rückgriff auf die Originalvorgänge erlauben, befristet in den zentralen Datenbestand aufgenommen werden, obwohl dies der Pseudonymisierung entgegenstünde. In der gesetzten Frist könnten Inkonsistenzen ermittelt werden und die notwendigen Klärungen bei den Sachbearbeitern erfolgen. Eine solche Maßnahme stünde nicht im Widerspruch zu § 67 c Abs. 5 SGB X, denn diese Regelung verlangt die Anonymisierung, sobald dies vom Planungszweck möglich ist. Diese zeitliche Eingrenzung hat den Sinn, Plausibilitätsprüfungen noch zu ermöglichen, bevor die Anonymisierung erfolgt.

Diese Maßnahme führt aber auch dazu, dass die Daten zunächst noch im personenbezogenen Zustand in den zentralen Datenbestand überführt werden. Da eine Rechtsgrundlage für die Übermittlung von Sozialdaten zum Zwecke des Querschnittscontrollings an eine Senats-

verwaltung, z. B. die Senatsverwaltung für Finanzen, nirgendwo zu erkennen ist, wäre dies nur möglich, wenn der zentrale Datenbestand in der datenschutzrechtlichen Verantwortung der Sozialämter läge.

Wir erwarten auch noch die Vorlage der Risikoanalyse und des Sicherheitskonzepts für ePBN. Ein früherer Entwurf einer solchen Unterlage war in methodisch fragwürdiger Weise erarbeitet worden[59], so dass die Vollständigkeit der Risikoanalyse nicht gewährleistet sein konnte. Wir haben der Senatsverwaltung für Finanzen empfohlen, nach dem eigenen vorbildlichen Vorgehen bei der Erarbeitung der Risikoanalyse und des Sicherheitskonzepts für das IT-Verfahren zum Stellenpool eine Fachberatung durch BSI-akkreditierte Grundschutzauditoren in Anspruch zu nehmen.

Zusammenfassend haben wir bei der Vorabkontrolle von ePBN sonderbare Erfahrungen gemacht:

- In dem gesamten bisherigen Verfahren, das sich bisher etwa ein Jahr lang hinzieht, haben die Projektverantwortlichen bei der Senatsverwaltung für Finanzen nicht einen konstruktiven Beitrag für die datenschutzrechtliche Gestaltung des Verfahrens eingebracht. Es gibt zwar politische Absichtserklärungen des Senats und des Abgeordnetenhauses von Berlin sowie von Vertretern dieser Gremien, aber es gibt keine operable Darstellung der Ziele, die mit dem Einsatz von ePBN verbunden sind, oder der Fragestellungen, die damit beantwortet werden sollen. Mit Ausnahme der genannten Absichtserklärungen gibt es keine Vorgaben, nach denen sich das beauftragte Softwareunternehmen zu orientieren hätte.

- Das beauftragte Softwareunternehmen, das auch als Unternehmensberatung tätig wurde, war völlig frei, mit uns über die datenschutzrechtliche Gestaltung des Verfahrens zu verhandeln. Da alle grundsätzlichen Vorgaben fehlten, entwickelte sich in dieser Zusammenarbeit ein Trial-and-Error-Vorgehen von beiden Seiten. Mögen der Unternehmensberatung exzellente Fähigkeiten in der Programmierung des komplexen Verfahrens attestiert werden können; allerdings lagen weder datenschutzrechtliche Kenntnisse noch Erfahrungen zu technisch-organisatorischen Datenschutzfragestellungen noch das Gespür für die datenschutzgerechte Gestaltung von solchen IT-Verfahren vor. Dies führte vielfach zu Missverständnissen und Fehlinterpretationen,

---

[58] Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder: Datenschutzfreundliche Technologien. Schwerin: Landesbeauftragter für den Datenschutz Mecklenburg-Vorpommern, 1998, S. 17 ff. – Broschüre

[59] vgl. 3.5

die wegen der strikten Passivität der verantwortlichen Senatsverwaltung nur mühsam im Dialog aufgelöst werden konnten.

- Gleichzeitig wurde von politischer Seite erheblicher Erfolgsdruck ausgeübt, der sich mittelbar auch auf uns auswirkte. Dem zitierten Senatsbeschluss vom 17. Dezember 2002, der das offizielle Startsignal gab, ging ein Berichtsauftrag des Abgeordnetenhauses von Berlin vom 13. Juni 2002[60] voraus, der ebenfalls am 17. Dezember 2002 erfüllt wurde. Der Ausschuss für Verwaltungsreform und Kommunikations- und Informationstechnik behandelte das Thema auf seiner 23. Sitzung am 23. Oktober 2003[61] sehr ausführlich, aber ohne unsere Beteiligung. Dabei wurde deutlich, dass unsere Einwände offenbar überraschend kamen, weil unsere Beteiligung an den Pilotprojekten letztlich zu guten Ergebnissen führten. Dabei wurde übersehen, dass die Projekte sich schon von der Konkretisierung ihrer Fragestellungen wesentlich vom ausgeweiteten Verfahren unterschieden. Erkennbar war auch die Ungeduld, mit der alle Fraktionen auf die Realisierung des Projektes warteten. Allerdings wurde bei allen genannten Anlässen betont, dass die Projekteinführung in Übereinstimmung mit den datenschutzrechtlichen Bestimmungen und damit nicht gegen unsere wesentlichen Einwände erfolgen sollte.

3.5 Risikoanalysen und Sicherheitskonzepte – der Weg zu einer sicheren Datenverarbeitung

Seit Beginn der Datenschutzgesetzgebung gibt es Vorschriften, die von den Daten verarbeitenden Stellen verlangen, dass die Daten so verarbeitet müssen, dass sie bei ihrer Verarbeitung nicht Unbefugten zur Kenntnis gelangen dürfen, dass Unbefugte keine Veränderungen an den Daten oder an den Programmen vornehmen können und dass die Daten, Programme und Systeme für die Sicherstellung der ordnungsgemäßen Datenverarbeitung zur Verfügung stehen müssen, wenn sie gebraucht werden. Um diese Ziele zu erreichen, besteht die Verpflichtung, die dafür notwendigen technischen und organisatorischen Maßnahmen zu ergreifen. Es wird verlangt, dass die Maßnahmen dem Schutzzweck angemessen sein und dem Stand der Technik entsprechen sollen.

[60] Abghs.-Drs. 15/1146
[61] Inhaltsprotokoll VerwRefKIT 15/23

Angemessenheit und Eignung technischer und organisatorischer Maßnahmen zum Datenschutz

Die wichtigste Frage, die sich die Daten verarbeitenden Stellen zu stellen haben, lautet daher, welche Maßnahmen getroffen werden müssen, welche entsprechen dem Schutzzweck und verhindern in angemessener Weise jeglichen unbefugten Zugriff auf die Daten. Das BDSG und andere Landesgesetze, die die Datensicherheitsvorschriften noch nicht dem heutigen Methodenwissen angepasst haben, versuchen dies mit einem Katalog von Kontrollanforderungen zu lösen. Diese Anforderungen definieren relativ konkret, was im Einzelnen erreicht werden muss. Zu jeder Anforderung lassen sich Checklisten möglicher Maßnahmen zusammentragen, aus denen man sich die tatsächlich oder vermeintlich geeignetsten aussuchen kann. Je nachdem, mit welchem Vorverständnis diese Auswahl getroffen wird, trägt sie dann die Handschrift des Haushälters, der arbeitsüberlasteten IT-Stelle, des Technikfreaks oder der Fachkraft für informationstechnische Sicherheit. Die methodische Schwäche der abgeschlossenen Kontrollanforderungskataloge liegt mittlerweile darin, dass die vielfältige Ausprägung moderner Informationstechnik und die sich daraus ergebenden tatsächlichen Anforderungen von den Katalogen nicht mehr immer abgebildet werden können.

Einige Bundesländer – so auch Berlin – sind bei der letzten Novellierung ihrer Datenschutzgesetze daher einen anderen Weg gegangen. Sie definieren abstraktere Ziele, die erreicht werden müssen, und verlangen, dass zur Erreichung dieser Ziele Sicherheitskonzepte entwickelt und umgesetzt werden, die auf Risikoanalysen beruhen. Bevor entschieden wird, welche Maßnahmen getroffen werden, ist zuverlässig und vollständig zu ermitteln, gegen welche konkreten Risiken die Maßnahmen wirken sollen. Damit erhält auch die Forderung nach der Angemessenheit zum Schutzzweck erst einen Sinn: Angemessen ist eine Maßnahme dann, wenn sie ein erkanntes Risiko so weit mindert, dass das Restrisiko akzeptiert werden kann. Missbräuchlich war dagegen die manchmal den Forderungen der Datenschutzbeauftragten entgegengehaltene Ansicht, das Gebot der Verhältnismäßigkeit verlange, den Aufwand für Datensicherheitsmaßnahmen auf jeden Fall zu relativieren.

Rechtliche Rahmenbedingungen

§ 5 BlnDSG bestimmt, dass bei der Verarbeitung personenbezogener Daten Maßnahmen zu treffen sind, die geeignet sind, Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der personenbezogenen Daten zu gewährleisten, und dass ferner die Verarbeitung dieser Daten revisionsfähig und transparent erfolgt. Vor der Entscheidung über den Einsatz oder eine we-

sentliche Änderung der automatisierten Datenverarbeitung sind die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzepts zu ermitteln. Bereits im Januar 1999 wurde für die Berliner Verwaltung die IT-Sicherheitsrichtlinie[62] erlassen, in der festgelegt wurde, dass für die verschiedenen Sicherheitsdomänen Sicherheitskonzepte zu erstellen sind. Sicherheitsdomänen sind dabei alle logisch, organisatorisch oder räumlich zusammengehörenden Bereiche mit einheitlichen Sicherheitsanforderungen. Konkreter aber verlangt die Richtlinie, dass für die zentrale IT-Infrastruktur (Landesnetz, Sicherheitsrechenzentrum, Grenznetz) Sicherheitskonzepte existieren müssen, die hohen Schutzbedarf befriedigen, dass behördenbezogene Sicherheitskonzepte zumindest den Grundschutz für mittleren Schutzbedarf gewährleisten sollen und dass für die Sicherheitsdomänen der IT-Verfahren verfahrensspezifische Sicherheitskonzepte vorliegen müssen. Dabei ist eine Hierarchie erkennbar: Da die Behörden auch die zentrale IT-Infrastruktur nutzen, bauen die behördlichen Sicherheitskonzepte auf dem der zentralen Infrastruktur auf. Da die IT-Verfahren in den behördlichen Infrastrukturen (lokale Netzwerke) betrieben werden, bauen die verfahrenspezifischen Sicherheitskonzepte auf den behördlichen Sicherheitskonzepten auf.

Sicherheitskonzepte in der Berliner Verwaltung

Fünf Jahre nach Erlass der Richtlinie kann von einer flächendeckenden Ausstattung der öffentlichen Stellen Berlins mit solchen Sicherheitskonzepten nicht die Rede sein. Selbstverständlich gibt es technische und organisatorische Maßnahmen, Regelungen zu bestimmten sicherheitsrelevanten Fragestellungen wie Datensicherung, Umgang mit Passwörtern und manches andere, methodisch erstellte Konzepte liegen jedoch nur in Ausnahmefällen vor und wurden häufig aufgrund unserer Forderungen bei neuen IT-Verfahren erstellt. Allerdings häufen sich die Fälle, in denen uns verfahrens- und behördenspezifische Sicherheitskonzepte zur Kenntnisnahme oder Stellungnahme vorgelegt werden. Die Unterscheidung zwischen guten und schlechten Sicherheitskonzepten, die am „grünen Tisch“ zu treffen ist, ergibt sich zunächst daraus, wie präzise die Konzepte nach anerkannten methodischen Vorgaben erarbeitet worden sind. Ist zum Beispiel die vorhergehende Schutzbedarfsfeststellung zutreffend? Macht die Vorgehensweise bei der Risikoanalyse plausibel, dass sie vollständig ist, dass also die Behandlung wichtiger Risiken nicht vergessen worden ist? Wird die Auswahl der Maßnahmen im Sicherheitskonzept durch eine Restrisikoanalyse gerechtfertigt? Geprüft werden kann auf dem Papier nur die Plausibilität, Vollständigkeit und methodische Klarheit,

[62] Richtlinie zur Gewährleistung der notwendigen Sicherheit beim IT-Einsatz in der Berliner Verwaltung vom 5. Januar 1999, DBl. I 1999, S. 5 ff.

nicht jedoch die Richtigkeit. Diese kann wie auch die Umsetzung der Sicherheitskonzepte nur vor Ort kontrolliert werden.

Manche der vorgelegten Sicherheitskonzepte waren nach den genannten Kriterien nicht zu beanstanden. Fast in allen diesen Fällen waren Beratungsunternehmen eingebunden worden, die sich ganz oder teilweise auf diese Aufgaben spezialisiert haben. Am Beispiel des Sicherheitskonzepts für die IT-Anwendung im Rahmen des Stellenpools zeigte sich, dass BSI-akkreditierte Grundschutzauditoren auch unter engem Zeitdruck akzeptable Sicherheitskonzepte entwickeln können.

Die meisten Fehler werden bereits bei der Risikoanalyse gemacht. Ein Fehler ist, dass die betrachteten Risiken willkürlich ausgewählt erscheinen, vielleicht in einem Brainstorming oder in Workshops ohne weitere methodische Hilfsmittel ermittelt wurden, so dass die Vollständigkeit nicht plausibel gemacht werden kann. Oft entsteht der Eindruck, dass nur die Risiken betrachtet werden, für deren Eindämmung bereits Maßnahmen erkannt oder gar getroffen wurden oder die mit einfachen Mitteln verringert werden können. Ein weiterer Fehler bei der Durchführung von Risikoanalysen liegt darin, dass man schon bei der Zusammenstellung der zu analysierenden Risiken auf Maßnahmen zurückgreift, die sich mindernd auf die Risiken auswirken. In diesem Falle ist für den Revisor nicht erkennbar, aus welchem Grunde bestimmte Risiken aus der Analyse ausgeblendet wurden. Das Sicherheitskonzept muss die Maßnahmen explizit benennen, die gegen ein bestehendes Risiko getroffen worden sind, gleichgültig, ob die Maßnahmen vor der Analyse bereits getroffen waren oder nicht.

Vorgaben des BSI

Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) hat 1992 das *IT-Sicherheitshandbuch* veröffentlicht[63]. Es war bald klar, dass die Anwendung dieses Handbuchs zur Erarbeitung von Sicherheitskonzepten nur in besonderen Fällen, in denen ein hoher Schutzbedarf zu decken ist, angemessen sein konnte, weil der Aufwand dafür sehr hoch ist. Eine Überarbeitung hat das IT-Sicherheitshandbuch daher nicht mehr erfahren. Die beschriebene abstrakte Methodik für die Durchführung einer Bedrohungs- und Risikoanalyse und der Ableitung von Maßnahmen daraus ist nach wie vor einschlägig, die technikbezogenen Beispiele und Maßnahmenvorschläge sind dagegen weitgehend veraltet.

Seit 1995 veröffentlicht das BSI in etwa jährlichen Abständen eine Fortschreibung des *IT-Grundschutzhandbuchs* als Loseblatt-Sammlung[64], als CD oder im Internet[65]. Das Grundschutzhandbuch bietet eine vereinfachte Methode für die Risikoanalyse und die Auswahl geeigneter Maßnahmen an, beschränkt sich aber ausdrücklich auf den Einsatz bei niedrigem oder mittlerem Schutzbedarf.

Die Schutzbedarfsanalyse

Das Grundschutzhandbuch beginnt mit einer Schutzbedarfsanalyse, in der festgestellt werden soll, in welchem Umfang seine Anwendung angemessen und in welchen Zusammenhängen ergänzende Sicherheitsanalysen erforderlich sind. Dies könnte zum Beispiel die Durchführung einer Risikoanalyse nach dem IT-Sicherheitshandbuch sein.

Es wird nur sehr grob unterschieden zwischen IT-Systemen mit niedrigem bis mittlerem Schutzbedarf für den Fall, dass die Schadensauswirkungen begrenzt sind, mit hohem Schutzbedarf für den Fall, dass die Schadensauswirkungen beträchtlich sind, oder mit sehr hohem Schutzbedarf bei existenziell bedrohlichen oder katastrophalen Schäden. Die Schäden können dabei in

- den Folgen von Verstößen gegen Gesetze, Vorschriften oder Verträge,
- der Beeinträchtigung des informationellen Selbstbestimmungsrechts,
- der Beeinträchtigung der persönlichen Unversehrtheit,
- der Beeinträchtigung der Aufgabenerfüllung,
- der negativen Außenwirkung oder – last but not least –
- finanziellen Auswirkungen

bestehen. Im Hinblick auf das informationelle Selbstbestimmungsrecht wird von sehr hohem Schutzbedarf gesprochen, wenn ein Missbrauch personenbezogener Daten für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten würde. Zur schärferen Eingrenzung bestimmter Schutzbedarfskategorien macht es Sinn, bei den Bewertungen nach den Grundbedrohungen der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten und Systeme zu differenzieren. Es gibt IT-Systeme, deren Ausfall verheerende Wir-

[63] BSI (Hrsg): IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik. Bonn: Bundesdruckerei, 1992, Download ist möglich über http://www.bsi.bund.de/literat/kriterie.htm

[64] BSI (Hrsg.): IT-Grundschutzhandbuch. Standard-Sicherheitsmaßnahmen. Köln: Bundesanzeiger Verlag, 2002

kungen haben kann, bei denen jedoch Verletzungen der Vertraulichkeit weniger ins Gewicht fallen (z. B. Steuerungssysteme bei strahlentherapeutischer Behandlung, von Nuklearanlagen); es gibt andere IT-Systeme, in denen die Beeinträchtigungen der Datenintegrität schlimmere Auswirkungen haben als Verletzungen der Vertraulichkeit (z. B. Kassenverfahren) und letztlich andere Systeme, in denen es vor allem auf die Vertraulichkeit der Daten ankommt (z. B. medizinische Register). Aus datenschutzrechtlicher Sicht ist vor allem relevant, wann Daten verarbeitet werden, die vor allem hinsichtlich der Vertraulichkeit hohen oder sehr hohen Schutzbedarf ausweisen: Dies dürfte immer dann der Fall sein, wenn besondere Daten im Sinne von § 6 a BlnDSG, Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen, Daten im Rahmen der Strafverfolgung oder des Verfassungsschutzes oder dispositive (bewertende) Daten über Personen vorliegen.

Im Falle des IT-Verfahrens im Stellenpool wurde unsere Forderung nach der Eliminierung bestimmter dispositiver Personaldaten (z. B. Gesamtnoten dienstlicher Beurteilungen, Gründe für die Beendigung von Arbeitsverhältnissen) von den später eingeschalteten Grundschutz-Auditoren bestätigt und durchgesetzt, weil sonst ergänzende Sicherheitsanalysen erforderlich gewesen wären.

Die Risikoanalyse

Der für die Wirksamkeit eines Sicherheitskonzepts entscheidende Schritt ist die Risikoanalyse. Wenn hier Fehler gemacht werden, werden im Sicherheitskonzept falsche Maßnahmen umgesetzt, die untragbare Risiken bestehen lassen. Die Risikobetrachtungen nach dem IT-Sicherheitshandbuch und dem IT-Grundschutzhandbuch unterscheiden sich erheblich, jedoch ist in beiden Fällen Vollständigkeit gewährleistet, wenn die Methoden strikt angewendet werden. Die Methode nach dem IT-Sicherheitshandbuch ist naturgemäß komplexer, aber logisch nachvollziehbar und macht das Grundprinzip deutlich:

Zunächst müssen alle Anwendungen und Datenbestände ermittelt und hinsichtlich der Schäden bei Eintreten der Grundbedrohungen bewertet werden. Danach werden die einzelnen Objekte der Anwendungen, Daten und ihrer Umgebungen (Infrastruktur, Hardware, Datenträger, Paperware, Software, Anwendungsdaten, Kommunikationskomponenten, Personen) und deren Bedeutung für die Grundbedrohungen erfasst. Dann werden die Bedrohungen auf die Objekte konkretisiert. Am Ende dieses Schrittes ist bekannt, wie der Schaden pro Objekt bei Eintreten einer Bedrohung bewertet wird (Schadenswert in einer fünfstufigen Skala).

---

[65] http://www.bsi.de/gshb/deutsch/menue.htm

Als Nächstes wird bewertet, wie häufig eine Bedrohung zu einem Schadensfall an einem Objekt führt (Häufigkeitswert in einer fünfstufigen Skala). Das Wertepaar {Schadenswert, Häufigkeitswert} beschreibt das Risiko, denn es gibt an, wie häufig welcher Schaden an einem Objekt entstehen kann. Da man kleine Schäden häufiger ertragen kann als große, muss entschieden werden, mit welcher Häufigkeit welche Schäden als tragbar angenommen werden sollen oder nicht (Entscheidungstabelle zur Ermittlung der tragbaren und untragbaren Risiken). Gegen die untragbaren Risiken müssen Maßnahmen ergriffen werden, die den Schadenswert und/oder den Häufigkeitswert so weit reduzieren, dass das Risiko in den tragbaren Bereich der Entscheidungstabelle rutscht. Das Sicherheitskonzept steht, wenn am Ende eine Restrisikoanalyse nachweist, dass alle zuerst untragbaren Risiken auf ein tragbares Maß reduziert worden sind.

Dieses recht komplizierte Verfahren verwendet zwar Skalenwerte, aber sowohl die Schadenswerte als auch die Häufigkeitswerte und allemal die Entscheidung, wann Risiken tragbar sind und wann nicht, lassen sich objektiv nicht bestimmen. Daher verlangt die Vorgehensweise nach dem IT-Sicherheitshandbuch das diskurshafte Zusammenwirken von Vertretern verschiedener Interessen und fachlicher Kompetenzen. Es wird dringend empfohlen, die Diskurse unter neutraler Moderation zu führen, um die Durchsetzung einseitiger Interessen zu verhindern. Zum Beispiel darf ein vernünftiges Sicherheitskonzept nicht am entschlossenen Widerstand des Finanzverantwortlichen scheitern. Andererseits soll die Umsetzung eines Sicherheitskonzeptes ein Unternehmen oder eine Behörde nicht selbst existenziell oder in seiner Aufgabenerfüllung bedrohen.

Wesentlich einfacher verläuft die Risikoanalyse mit dem Grundschutzhandbuch. Das Grundschutzhandbuch benennt derzeit insgesamt 54 Komponenten unterschiedlicher Art, die als Bausteine für die Modellierung des zu analysierenden IT-Systems oder der zu analysierenden IT-Anwendung verwendet werden können. Die Weiterentwicklung des IT-Grundschutzhandbuchs besteht unter anderem darin, dass die Zahl der Komponenten kontinuierlich erhöht wird, um immer mehr reale IT-Systeme mit diesen Bausteinen modellieren zu können. Jedem dieser Bausteine sind konkrete Gefährdungen zugeordnet, die auf ihnen lasten, und konkrete Maßnahmen, mit denen sie reduziert werden können. Alle Gefährdungen und Maßnahmen werden genau beschrieben. Sind alle Bausteine des Modells erfasst, können alle Gefährdungen aufgelistet werden. Dann muss entschieden werden, welche Gefährdungen im realen Fall relevant sind, d. h., ob sie aufgrund besonderer Verhältnisse nicht bestehen, ob genannte Maßnahmen bereits ergriffen und somit die Gefährdungen reduziert

wurden oder ob die angebotenen Maßnahmen ergriffen werden müssen, um die Sicherheit zu gewährleisten.

IT-Sicherheitskonzepte

Die Ausführungen zu den Methoden der Risikoanalysen machen bereits deutlich, dass sich bei der Anwendung der beschriebenen Methoden das Sicherheitskonzept beinahe von selbst ergibt. Beim Sicherheitshandbuch ist am Ende klar, gegen welche Risiken Maßnahmen ergriffen werden müssen. Es bietet Hilfestellungen, die aber nicht mehr aktuell sind und somit nur Anregungen geben können. Da das Sicherheitshandbuch aber nur mit Expertenwissen durchgeführt werden kann, dürfte es unproblematisch sein, aktuelle Maßnahmen gegen untragbare Risiken zu finden.

Das ständig aktualisierte IT-Grundschutzhandbuch bietet nach der Analyse einen Katalog von Maßnahmen an. Er ist zunächst darauf zu prüfen, ob er Maßnahmen enthält, die bereits getroffen wurden. Dann ist zu prüfen, ob auf Maßnahmen verzichtet werden kann, weil sie sich gegen Gefährdungen richten, die nicht vorliegen. Bei dem Rest handelt es sich um Maßnahmen, die für die Umsetzung des Sicherheitskonzepts von Bedeutung sind.

Die Dokumentation des Sicherheitskonzepts muss in allen Fällen die vollständige Risikoanalyse nachvollziehbar und deutlich machen, weshalb bezüglich der angebotenen Maßnahmen welche Entscheidungen getroffen wurden.

Die IT-Sicherheitsrichtlinie vom 5. Januar 1999 schreibt vor, wie ein Sicherheitskonzept in der Berliner Verwaltung aufgebaut werden muss:

Neben der Benennung des Anwendungsbereichs (Behörde, Verfahren), also der Beschreibung der behandelten Sicherheitsdomäne, muss es die Risikoanalyse, die Beschreibung der Maßnahmen und eine Restrisikoanalyse, die die Beseitigung aller untragbaren Risiken nachweist, enthalten sein. Ferner gehört zum Sicherheitskonzept die Benennung der Verantwortlichkeiten sowie ein Umsetzungsplan, der einen Zeitplan, Prioritätsfestlegungen, Fortschreibungsregeln und die Kosten spezifiziert.

Das Berliner Modellsicherheitskonzept

Ein wichtiges Projekt des IT-KAB[66] ist derzeit die Erarbeitung eines Modellsicherheitskonzepts für die Berliner Verwaltung durch eine spezielle Arbeitsgruppe, in der wir mitarbeiten. Grundlage für die Erarbeitung dieses Modellsicherheitskonzepts ist das IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik. Dabei werden zu den einzelnen dort beschriebenen Komponenten, die für die Berliner Verwaltung relevant sind, die im Handbuch vorgeschlagenen Maßnahmen darauf hin untersucht, ob die damit zu reduzierenden Gefährdungen überhaupt zutreffen, die Maßnahmen bereits getroffen worden sind oder aber doch noch einer Umsetzung bedürfen. Dieses Vorgehen ist für Verfahren, die höchsten mittleren Sicherheitsbedarf aufweisen, legitim. Abzuwarten bleibt jedoch, ob die Behörden, die das Modellsicherheitskonzept später anwenden, den Modellcharakter tatsächlich anerkennen oder das Modellkonzept mehr oder weniger unangepasst übernehmen. Dies wäre jedoch ein wesentliches Missverständnis über den Zweck des Modellsicherheitskonzepts, denn selbstverständlich muss jede Behörde die meisten im Modell erfolgten Abwägungen anhand der behördenspezifischen Verhältnisse überprüfen.

4. Aus den Arbeitsgebieten

4.1 Öffentliche Sicherheit

4.1.1 Polizei

Der „Fall Mahmoud“ – junge Intensivtäter

> *Im Frühjahr ging der „Fall Mahmoud“ durch die Presse. Es handelte sich um einen jungen Intensivtäter, der seit seinem zehnten Lebensjahr wegen rund 80 Straftaten – teilweise während der Bewährungszeit – bei der Polizei aktenkundig wurde. Diesen Fall hatte ein leitender Kriminalpolizist in einem Aufsatz in einer Fachzeitschrift aufbereitet.*

Der Polizeibeamte hatte – leicht anonymisiert – detailliert über die Stationen der kriminellen Karriere sowie über die persönliche Entwicklung, das soziale Umfeld und die familiäre Situation des Betroffenen berichtet. Der Aufsatz[67] listet ausführlich sämtliche gegen den Betroffe-

[66] vgl. 2.2

[67] Henninger, Markus: Konsequente Inkonsequenz / Die „kriminelle Karriere“ des Mahmoud R. und ihre justizielle Würdigung. In: Kriminalistik 8-9 (2002), S. 513 ff.

nen geführten Ermittlungsverfahren auf. Den Namen hatten Journalisten durch Recherchen in der Szene schnell herausgefunden und veröffentlicht[68] .

Datenschutzrechtliche Probleme ergeben sich daraus, ob

- und gegebenenfalls in welcher Funktion der Autor (Kriminalpolizist) auf das polizeiliche Informationssystem zugegriffen hat,
- der Zugriff mit Genehmigung des Polizeipräsidenten in Berlin erfolgte,
- eine Genehmigung für die Fertigung des Aufsatzes vorlag und
- der Text des Aufsatzes vor der Veröffentlichung von dem Polizeipräsidenten in Berlin genehmigt wurde.

Der Polizeipräsident hat uns mitgeteilt, dass diese Fragen nahezu deckungsgleich Gegenstand eines Strafermittlungsverfahrens sind. Die Berliner Polizei sei sowohl als Strafverfolgungsbehörde als auch als Dienstbehörde eingebunden. Die jeweiligen Pflichtenkreise würden sich überlagern. Er bezweifele außerdem, dass in dem Aufsatz überhaupt personenbezogene Daten veröffentlicht wurden. Er bat, eine Stellungnahme erst nach Abschluss des Strafermittlungsverfahrens abgeben zu können. Dem haben wir ausnahmsweise wegen der besonderen Sensibilität des Einzelfalles entsprochen. Grundsätzlich jedoch sind die strafrechtlichen Ermittlungen losgelöst von einer Stellungnahme an den Datenschutzbeauftragten zu betrachten.

Der Fall hat dazu geführt, dass zwischen Justizverwaltung und Polizei eine Diskussion über den Umgang mit jugendlichen Intensivtätern einsetzte. Sie führte zur Erarbeitung einer gemeinsamen Richtlinie von Polizei und Staatsanwaltschaft zum Umgang mit Intensivtätern, an der wir rechtzeitig beteiligt wurden.

Zunächst wurde definiert, wer als Intensivtäter eingestuft wird. Bei der Polizei und der Staatsanwaltschaft wurden Koordinatoren und deren Aufgaben bestimmt sowie die Einzelheiten eines Informationsaustauschs mit Hinweis auf die Rechtsgrundlagen und die Löschungsfristen festgeschrieben. Unsere Anregungen sind dabei berücksichtigt worden.

Weiterhin hat die ressortübergreifende Arbeitsgruppe zur Kinder- und Jugenddelinquenz ein Präventionskonzept entwickelt, das Beiträge der Jugendhilfe zur präventiven kriminellen Karriere und zum sachgerechten Umgang mit jungen Intensivtätern enthält.

---

[68] Der Spiegel 12/2003, S. 54, 58

Richtlinien für den kriminalpolizeilichen Meldedienst

Ein Bürger hat uns um die Prüfung der Rechtmäßigkeit von verschiedenen Datenspeicherungen in der vom BKA geführten Arbeitsdatei PIOS – Innere Sicherheit (APIS) und im Kriminalaktennachweis (KAN) gebeten. Dabei ging es um zwei Verfahren aus den Jahren 1997 und 2000 wegen Verstoßes gegen das Versammlungsgesetz (Plakat-Entrollen auf dem Vordach einer Gebäudeeingangshalle) und Hausfriedensbruch (Erklettern des Berliner Fernsehturmes und Versuch, ein Zelt aufzubauen bzw. ein Plakat aufzuhängen).

Der Polizeipräsident hat die Meldungen an das BKA damit gerechtfertigt, dass der Betroffene offensichtlich zu Mitstreitern der Umweltorganisation Robin Wood gehört, die durch plakative, zum Teil beträchtliche Störungen verursachende Aktionen auf deren Ziele aufmerksam machen wollen. Diese hoch emotionalisierten Personen, die auch vor riskanten und sich und andere in Gefahr bringenden Aktionen nicht zurückschrecken, begehen zumeist Straftaten wie Verstöße gegen das Versammlungsgesetz, Hausfriedensbruch und Sachbeschädigung. In den von Robin Wood aufgegriffenen Themenfeldern wie Anti-AKW- bzw. Anti-Castor-Protesten ist es in der Vergangenheit zu Überschneidungen mit der militanten, linksextremistischen Szene und von dort aus begangenen, unaufgeklärt gebliebenen schwersten Straftaten wie beispielsweise Brand- und Hakenkrallenanschlägen gegen die Deutsche Bahn AG gekommen. Auch die Info-Box am Potsdamer Platz war wiederholt Zielobjekt linksextremistischer Angriffe, zu denen auch Brandanschläge zählten.

Der Betroffene war 1997 anlässlich der Jahrespressekonferenz der Deutschen Bahn AG mit sechs weiteren Personen auf das Vordach der Gebäudeeingangshalle der Deutschen Bahn AG gestiegen, um ein Transparent „Castor-Züge stehen still – wenn der neue Bahnchef will. Robin Wood“ zu entrollen. Als er nach seiner Festnahme erkennungsdienstlich behandelt werden sollte, leistete er Widerstand. Das Verfahren wurde eingestellt. Bei dem anderen Vorgang stieg er mit zwei anderen Personen mit Bergsteigerausrüstung an der Außenseite des Berliner Fernsehturmes an Stahlseilen empor. Sie versuchten, in 60 Metern Höhe ein Hochgebirgszelt und ein Transparent „S.O.S. ITOIZ“ anzubringen. Abgeworfenen Flugblättern war zu entnehmen, dass es sich um eine Protestaktion gegen den Bau eines Staudammes in Spanien handelte.

Die Polizei hält die Speicherung der Daten in APIS und KAN aus Gründen der Gefahrenabwehr und künftigen Strafverfolgung für erforderlich und geboten.

Nach der damaligen Rechtslage richtete sich die Zulässigkeit der Speicherung nach den Richtlinien für den kriminalpolizeilichen Meldedienst in Staatsschutzsachen (KPMD-S) in Verbindung mit der Errichtungsanordnung von APIS. Danach durften personenbezogene Daten nur unter folgenden Voraussetzungen in APIS gespeichert werden:

- Zuordnung der Straftaten zum Katalog der Staatsschutzdelikte,
- zu anderen Straftaten, sofern wegen der Angriffsrichtung, des Motivs des Täters oder dessen Verbindung zu einer Organisation der Verdacht besteht, dass mit der Tat Ziele im Sinne von Nr. 1 der KPMD-S verfolgt werden,
- Straftatvorwürfe gegen ein Objekt (Person, Institution oder Sache), aus denen sich der Verdacht ergibt, dass der Betroffene Ziele im Sinne von Nr. 1 der KPMD-S verfolgt und keine Erkenntnisse vorliegen, die eine Erfassung wegen des Motivs des Täters ausschließen würden.

Ziel von Nr. 1 der KPMD-S war es u. a., durch Sammlung und Auswertung von Nachrichten und Unterlagen Hinweise für die Verhütung und Aufklärung von Straftaten zu gewinnen, die gegen die freiheitlich-demokratische Grundordnung, den Bestand und die Sicherheit des Bundes oder eines Landes gerichtet sind oder die eine ungesetzliche Beeinträchtigung der Amtsführung von Mitgliedern verfassungsmäßiger Organe des Bundes und der Länder zum Ziel haben.

Im vorliegenden Fall konnten die Straftaten nicht dem Katalog der Staatsschutzdelikte zugeordnet werden. Sie richteten sich auch nicht gegen die freiheitlich-demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes. Den Datenspeicherungen lagen Ermittlungsverfahren wegen Hausfriedensbruch, Verstoßes gegen das Versammlungsgesetz und Widerstandes gegen Vollstreckungsbeamte zugrunde. Ein Zusammenhang mit linksradikalen Anschlägen bei Castor-Transporten auf die Deutsche Bahn AG konnte ebenso wenig nachgewiesen werden wie schwerer Landfriedensbruch.

Die Verfolgung von Zielen nach Nr. 1 KMPD-S war nicht erkennbar, da sich die Aktionen der Robin-Wood-Mitglieder gegen die Beseitigung von Defiziten im Bereich des Umweltschutzes sowie gegen die Verwendung von Atomenergie – und nicht gegen die freiheitlich-demokratische Grundordnung – richteten.

Zwischenzeitlich wurde in einer Neufassung der Richtlinie im Jahr 2001[69] die Meldeschwelle erheblich herabgesetzt. Danach sind nach Nr. 2 KPMD-PMK neben den bisherigen Straftatbeständen insbesondere Straftaten, die in Würdigung der Umstände, der Tat und/oder der Einstellung des Täters Anhaltspunkte dafür geben, dass sie den demokratischen Willensbildungsprozess beeinflussen sollen, der Erreichung oder Verhinderung politischer Ziele dienen oder sich gegen die Realisierung politischer Entscheidungen richten, meldepflichtig.

Mit ihren Aktionen wollen die Mitglieder von Robin Wood zwar den demokratischen Willensbildungsprozess im Bereich Umweltschutz und Energie beeinflussen. Es ist aber mit dem Wesen der Demokratie nicht vereinbar, wenn jede politische Motivation unter dem Verdacht steht, sich gegen die freiheitlich-demokratische Grundordnung zu richten.

Anhaltspunkte für eine staatsfeindliche oder gar terroristische Motivation des Betroffenen bei der Begehung der vorliegenden Straftaten waren nicht erkennbar. Der Betroffene wollte mit seinen Aktionen auf angebliche Missstände im Bereich der Castor-Transporte aufmerksam machen bzw. über den Bau eines umweltpolitisch diskutablen Staudamm-Projektes in Spanien informieren.

Der Polizeipräsident hat ohne weitere Begründung erklärt, dass die weitere Speicherung zulässig ist, weil nach Würdigung der Umstände Anhaltspunkte dafür vorliegen, dass sie der Erreichung oder Verhinderung politischer Ziele dienen.

Öffentlichkeitsfahndung im Internet

Bereits 1998[70] hatten wir über die Problematik der Fahndung im Internet sowohl in rechtlicher als auch in technischer Hinsicht berichtet. Durch das Strafverfahrensänderungsgesetz 1999 (§§ 131 a bis 131 c Strafprozessordnung (StPO)) sind die Probleme in rechtlicher Hinsicht im Wesentlichen gelöst. Öffentlichkeitsfahndungen sind regelmäßig vom Richter, die tatsächliche Umsetzung vom Staatsanwalt anzuordnen.

Der Polizeipräsident hat eine Fahndungsseite eingerichtet, die Personen mit Bild und Angaben zur Person und zum Tatgeschehen enthält, die als Straftäter gesucht werden (regelmäßig über einen Zeitraum von drei Monaten), per Haftbefehl gesuchte Täter, die durch operative Fahndung nicht festgenommen werden konnten oder bei denen herkömmliche Fahn-

[69] Richtlinie für den kriminalpolizeilichen Meldedienst in Fällen politisch motivierter Kriminalität (KPMD-PMK)

dungsmaßnahmen ausgeschöpft sind. Diese Veröffentlichungen im Internet müssen geeignet sein, die Suche nach dem Straftäter entscheidend zu fördern. Das entspricht dem Beschluss des Berliner Abgeordnetenhauses[71].

Im vergangenen Jahr[72] hatten wir über die Öffentlichkeitsfahndung im Internet im Zusammenhang mit den Krawallen am 1. Mai 2002 und die Zusage der Staatsanwaltschaft berichtet, dass die Bilder der Personen, die sich gestellt haben oder die identifiziert wurden, unverzüglich aus dem Internet herausgenommen werden. Die Aktion war bis Jahresende 2002 befristet.

Nachdem die Polizei uns mitgeteilt hatte, dass die Daten gelöscht seien, haben wir im Internet recherchiert und nicht nur die Bilder selbst, sondern auch die Historie der Bilddateien gefunden. Auch auf den Seiten von Suchmaschinen waren die Bilder noch enthalten. Damit hat sich der von uns immer wieder gegebene Hinweis bestätigt, dass die Veröffentlichung der Fahndungsaufrufe im Internet nicht zuletzt deshalb gegenüber herkömmlichen Fahndungsmethoden erheblich eingriffsintensiver ist, weil diese Bilder nicht mehr vollständig zurückgeholt werden können. Löschungen entfalten nicht zwangsläufig Wirkung.

Bei der Prüfung vor Ort bestätigte sich, dass Mängel bei den technisch-organisatorischen Maßnahmen zur Öffentlichkeitsfahndung im Internet bestanden:

- Es existierten keine Vorschriften bzw. Dienstanweisungen darüber, in welcher Art und Weise die Einstellung, Änderung und Löschung von Dokumenten – also Texten und Grafiken – zu protokollieren und sicherzustellen ist.

- Es gab keine Regelungen darüber, ob (und wo) die Dokumente zur Ablage kommen sollen oder nicht.

- Es gab keine Verantwortlichen für die Rechte-Vergabe innerhalb des Content-Management-Systems (CMS), über das die Internet-Seiten gepflegt werden.

- Es wurden keine Maßnahmen gegen die Archivierung durch Suchmaschinen und Web-Archive getroffen.

---

[70] JB 1998, 3.4
[71] Abghs.-Drs. 13/3817, vgl. auch JB 2001, Anlage 1
[72] JB 2002, 4.1.2

- Es sind keinerlei Maßnahmen getroffen oder Überlegungen angestellt worden, wie der Senatsbeschluss zur Sicherstellung der Authentizität der eingestellten Fahndungsaufrufe umgesetzt werden kann.

Die Mängel wurden eingeräumt und beseitigt.

Freier Bürger nach Haftentlassung?

Ein Bürger ist nach längerer Haft in Berlin entlassen worden. Etwa zwei Wochen später wurde er in Bayern von der Polizei kontrolliert. Die Beamten erklärten ihm, dass er sich eigentlich noch in Haft befinden müsste, und wollten seinen Entlassungsschein sehen. Weil er diesen nicht bei sich hatte, konnte die Angelegenheit erst nach längerer Zeit geklärt werden.

Der Bürger war aufgrund einer Meldung des Polizeipräsidenten noch in der Haftdatei bei dem Bundeskriminalamt gespeichert. Die Daten zur Entlassung des Bürgers aus der Justizvollzugsanstalt sind erst nach dem Eingang der Entlassungsmitteilung knapp eine Woche nach der Personenkontrolle in Bayern in die Haftdatei eingestellt worden. Die Polizei hat uns dazu mitgeteilt, dass die Aktualisierung der Haftdatei regelmäßig erst ein bis zwei Wochen nach der Entlassung – jedoch immer zeitnah nach Eingang der Mitteilung bei dem Landeskriminalamt – erfolgen würde. Dieser Zeitraum ist zu lang. Der Polizeipräsident hat die Senatsverwaltung für Justiz gebeten, darauf hinzuwirken, die Mitteilungen von Haftdaten möglichst taggenau zu versenden.

Kriminalitätsschwerpunkt ISVB

Dem Berliner Beauftragten für Datenschutz und Informationsfreiheit steht nach dem Berliner Datenschutzgesetz das Recht zu, einen Strafantrag wegen Verstoßes gegen das Datenschutzgesetz zu stellen, wenn dies im öffentlichen Interesse geboten ist. Die Staatsanwaltschaft übersendet uns die Fälle mit der Bitte um Prüfung, ob ein Strafantrag von Amts wegen gestellt werden soll, wenn der für die Verfolgung erforderliche Strafantrag nicht gestellt worden ist.

In den vergangenen Jahren hat sich die Zahl der von uns gestellten Strafanträge ständig erhöht. Festzustellen ist dabei, dass fast alle uns vorgelegten Fälle unbefugte Abfragen aus

dem ISVB durch Mitarbeiter des Polizeipräsidenten betreffen. Teilweise erfolgten diese Abfragen nur ein- oder zweimal zu privaten Zwecken, teilweise bestanden auch Verbindungen zum Bereich der organisierten Kriminalität. Im ISVB getätigte Abrufe werden bei der Polizei protokolliert und sind bis zu einem Zeitraum von zwei Jahren überprüfbar. Allerdings ist die Protokollierung nicht geeignet, den Nachweis des unbefugten Abrufes zu erleichtern, denn der Abfragegrund wird nicht mit protokolliert. Er muss im Einzelfall im Nachhinein ermittelt werden.

Da wir uns über den Ausgang der Verfahren unterrichten lassen, in denen wir Strafantrag von Amts wegen gestellt haben, haben wir Kenntnis von einem Urteil[73] erhalten, in dem ein Polizeimitarbeiter zu einer Geldstrafe von 100 Tagessätzen verurteilt worden ist, weil er sechsmal unbefugt Daten einer Person im ISVB abgefragt hatte. Bemerkenswert an dem Urteil ist der Hinweis des Richters, dass offenbar bei der Berliner Polizei in nicht geringem Umfang bei den ISVB-Abfragen gegen das Berliner Datenschutzgesetz verstoßen wird. Der Richter stellt fest, dass angesichts der vermehrt auftretenden Fälle darauf geschlossen werden könne, dass die nötigen Kontrollmaßnahmen nicht in angemessenem Umfang durchgeführt werden.

Wir werden den Polizeipräsidenten erneut auffordern, dass Protokollierungsverfahren aus datenschutzrechtlicher Sicht zu verbessern.

4.1.2 Verfassungsschutz

Die Senatsverwaltung für Inneres hat ein Gesetz zur Änderung des Gesetzes zur Ausführung des Gesetzes zu Artikel 10 Grundgesetz und zur Änderung des Verfassungsschutzgesetzes Berlin vorgelegt[74]. Mit diesem Gesetz setzt auch das Land Berlin das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 um, mit dem nach dem 11. September 2001 das Bundesverfassungsschutzgesetz geändert worden war. Neben klarstellenden Regelungen enthält das Berliner Gesetz Befugniserweiterungen für die Verfassungsschutzbehörde in Anknüpfung an die Regelungen des Bundesverfassungsschutzgesetzes. So werden Datenerhebungsbefugnisse der Verfassungsschutzbehörde bei Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen geregelt. Es werden Erhebungsbefugnisse bei Postdienstleistern, Luftfahrtunternehmen und Telekommunikationsunternehmen geregelt.

[73] AG Tiergarten, Urteil vom 18. September 2003, Az.: 266 Ds 87/03
[74] Abghs.-Drs. 15/1973

Eine Befugnis zum Einsatz eines IMSI-Catchers ist in das Berliner Verfassungsschutzgesetz nicht aufgenommen worden.

Bereits im Gesetzgebungsverfahren zum Terrorismusbekämpfungsgesetz haben sich die Datenschutzbeauftragten kritisch gegenüber den nunmehr durch die Aufnahme in das Bundesverfassungsschutzgesetz bereits auf Bundesebene umgesetzten umfangreichen Auskunftsbefugnissen des Verfassungsschutzes gegenüber Kreditinstituten, Finanzdienstleistungsinstituten, Finanzunternehmen, Luftfahrtunternehmen sowie Post-, Telekommunikations- und Teledienstеunternehmen geäußert. Nach wie vor haben wir erhebliche Zweifel an der Erforderlichkeit dieser eingriffsintensiven Befugnisse für die Bekämpfung des Terrorismus. Insbesondere die Möglichkeit, personenbezogene Daten zukünftiger Telekommunikationsverbindungen zu erheben, stellt einen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung der hiervon Betroffenen dar. Zum einen handelt es sich hierbei um eine Datenerhebung auf Vorrat, bei der eine spezielle Güterabwägung sowie die Prüfung des Grundsatzes der Verhältnismäßigkeit für die zukünftig anfallenden Daten gerade nicht möglich ist. Zum anderen sind von der Maßnahme Betroffene hier nicht nur die tatsächlich überwachten Personen, sondern alle Personen, die unter Nutzug der genannten Technologien mit der vom Verfassungsschutz beobachteten Person in Kontakt gestanden haben. Damit ist der Kreis der Betroffenen erheblich weiter als bei anderen Maßnahmen.

Die Datenschutzbeauftragten haben bereits im Gesetzgebungsverfahren zum Terrorismusbekämpfungsgesetz darauf hingewiesen, dass wegen der mit diesen Befugnissen verbundenen schwerwiegenden Eingriffe in das Grundrecht auf informationelle Selbstbestimmung den Berichtspflichten und der sich anschließenden Evaluation der Maßnahmen eine besondere Bedeutung zukommt. Wünschenswert wäre es hierbei aus unserer Sicht gewesen, wenn der Bundesgesetzgeber die Berichtspflicht dahingehend geregelt hätte, dass die Berichte auch Aufschluss darüber geben, wie viele Personen tatsächlich von einer Maßnahme betroffen waren und welchem Personenkreis sie angehört haben. Eine Differenzierung zwischen den vom Verfassungsschutz beobachteten Personen und Dritten unter Angabe der genauen Zahlen würde die Aussagekraft der Berichte entscheidend verbessern. Nur auf dieser Grundlage kann auch die Evaluierung dem Ziel näher kommen, den Erfolg und tatsächlichen Nutzen der gesetzlichen Regelungen auf der Grundlage der mit ihnen verbundenen Grundrechtseingriffe bewerten zu können.

Trotz der weiterhin gegenüber dem Terrorismusbekämpfungsgesetz bestehenden grundsätzlichen datenschutzrechtlichen Bedenken sehen wir in dem vorgelegten Entwurf eine maßvolle Umsetzung der Regelungen des Gesetzes in Berliner Landesrecht. Wir begrüßen insbe-

sondere, dass die Eingriffsschwellen zugunsten der Betroffenen im Gegensatz zum Bundesverfassungsschutzgesetz angehoben werden. Auch der Verzicht auf die im Bundesverfassungsschutzgesetz erfolgte Einführung technischer Mittel zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes und zur Ermittlung der Geräte- und Kartennummern wird von uns aus datenschutzrechtlicher Sicht ausdrücklich begrüßt. Ebenso begrüßen wir den Verzicht auf die Übernahme der Befugnis, technische Mittel zum Schutz der bei einem Einsatz in Wohnungen tätigen Personen verwenden zu dürfen, soweit dies zur Abwehr von Gefahren für deren Leib, Gesundheit oder Freiheit unerlässlich ist.

In diesem Zusammenhang weisen wir auch auf eine Entschließung der Datenschutzbeauftragten des Bundes und der Länder auf der 65. Konferenz am 27./28. März 2003 in Dresden hin, die noch einmal auf die Pflicht zur Kennzeichnung von Daten aus besonders eingriffsintensiven Erhebungen hingewiesen haben[75].

4.2 Ordnungsverwaltung

4.2.1 Melde- und Personenstandswesen

Statt Meldegesetz: Änderung der DVO-Meldegesetz

Anstelle des seit vielen Jahren angemahnten Entwurfes zur Novellierung des Landesmeldegesetzes hat der Senat eine Änderungsverordnung zur DVO-Meldegesetz beschlossen, mit der der Kreis von Empfängern regelmäßiger Datenübermittlungen und der im Rahmen von automatisierten Abrufverfahren berechtigten Behörden erweitert werden sollte[76].

Die Erforderlichkeit und die Eilbedürftigkeit der beabsichtigten Regelungen noch vor der Novellierung des Meldegesetzes können wir nicht erkennen. Auch ist der Umfang der damit zur Verfügung gestellten Daten zu weitreichend und mit dem Grundsatz der Datensparsamkeit (§ 5 a BlnDSG) nicht vereinbar.

Der weit überwiegende Teil von Melderegisteranfragen dient dem Ziel, die aktuelle Wohnanschrift des Betroffenen festzustellen. Zu diesem Zweck ist es bei der Einrichtung von automatisierten Abrufverfahren nicht erforderlich, über den Grunddatenbestand (§ 28 Abs. 1 MeldeG) hinaus den Zugang zu den teilweise recht zahlreichen darüber hinausgehenden Datenfeldern

[75] vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2003“, S. 27
[76] GVBl. 2003, S. 514

zu eröffnen. Das ist auch mit dem Grundsatz der Erhebung von Daten bei dem Betroffenen selbst nicht vereinbar. Um die Daten bei dem Betroffenen erheben zu können, muss er für die öffentlichen Stellen erreichbar sein. Das wird durch die insofern beschränkte Zugriffsmöglichkeit auf die aktuelle Wohnanschrift sichergestellt. Sollte das im Einzelfall nicht ausreichend sein, bleibt eine Anfrage nach § 25 MeldeG davon selbstverständlich unberührt. Ähnliches gilt für die regelmäßige Datenübermittlung. Mehr als der Anlass für die regelmäßige Übermittlung und die aktuelle Wohnanschrift ist für die Erreichbarkeit des Betroffenen nicht erforderlich. Sollten für die anlassbezogene Bearbeitung weitere Daten erforderlich sein, können sie nach dem Grundsatz der Erhebung bei dem Betroffenen beschafft werden.

Nach alledem haben wir empfohlen, den Umfang der Daten, die regelmäßig übermittelt werden sollen bzw. auf die zugegriffen werden kann, auf den Grunddatenbestand zu beschränken. Dem hat sich der Senat nicht angeschlossen und die Verordnung vielmehr im Wesentlichen unverändert in Kraft gesetzt, obgleich der Unterausschuss „Datenschutz und Informationsfreiheit“ des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses von Berlin noch Gesprächsbedarf angemeldet hatte.

Der schreibunkundige Personalausweisinhaber

> *Ein Bürger hat uns seinen maschinenlesbaren Personalausweis vorgelegt, der auf der Rückseite den gesiegelten handschriftlichen Vermerk „Ausweisinhaber lt. eigenen Angaben nicht mehr schreibfähig“ enthielt.*

Die Personalausweisbehörde hat eingeräumt, dass die Anbringung eines handschriftlichen oder wie auch immer gearteten Vermerkes zur Schreibfähigkeit des Dokumenteninhabers unzulässig ist.

Der Antragsteller ist verpflichtet, die erforderlichen Unterschriften in der für die Ausstellung des Ausweises notwendigen Form zu leisten (§ 4 Abs. 4 Landespersonalausweisgesetz (LPAuswG)). Nach den allgemeinen Vorschriften zur Durchführung des Passgesetzes (PassVwV), die analog auch für das Verfahren bei Personalausweisanträgen anzuwenden sind, hat die Passbehörde bei schreibunkundigen oder schreibunfähigen Passbewerbern in das Unterschriftsfeld einen waagerechten Strich zu setzen (Ziff. 6.2.4 PassVwV). Üblicherweise wird lediglich auf dem Antragsformular, das bei der Behörde verbleibt, notiert, ob die Unterschrift wegen Schreibunfähigkeit oder -unkundigkeit unterbleibt; ein Vermerk auf dem Dokument hat grundsätzlich zu unterbleiben, weil das Gesetz über Personalausweise abschließend regelt,

welche Einträge zur Person vorzunehmen sind. Die Feststellung der Schreibunfähigkeit erfolgt regelmäßig durch den Augenschein oder durch nachvollziehbare Erklärungen des Ausweisbewerbers. Aufgrund des Auftretens des Bürgers bei seinem Besuch war eine körperliche Beeinträchtigung, die die Unterschriftsleistung hätte betreffen können, nicht offensichtlich. So soll er nicht davon gesprochen haben, schreibunfähig zu sein, sondern nicht unterschreiben zu wollen. Das hätte die Folge haben müssen, den Ausweis nicht auszustellen, weil der Bewerber seinen gesetzlichen Mitwirkungspflichten nicht nachkommen wollte. Der Leiter der Dienststelle hat dennoch entschieden, dass der Ausweis ohne Unterschriftsleistung auszustellen sei.

Diskretion im Bürgeramt

Der Besucher eines Bürgeramtes berichtete uns davon, dass in der Wand zwischen dem Warteraum und dem Büro selbst eine große Öffnung sei, die ein müheloses Mithören der dort geführten Gespräche ermöglichen würde.

Bei einer Ortsbesichtigung konnten wir uns davon überzeugen, dass der Sachverhalt zutreffend war. Im Beratungsraum selbst standen drei paarweise angeordnete Schreibtische, an denen auf der einen Seite die Mitarbeiter sitzen; ihnen gegenüber konnten Besucher Platz nehmen. Die Monitore der PCs waren so aufgestellt, dass zunächst nur die Beschäftigten die Daten zur Kenntnis nehmen konnten. Lediglich der Eingabeblock für die elektronische Bezahlung von Gebühren usw. war in Griffweite der Besucher aufgestellt. Sofern beide Besucherplätze belegt waren, war ein Mithören nicht nur nicht ausgeschlossen, sondern zwangsläufig.

Nach dem BlnDSG (§ 5 Abs. 2 i. V. m. § 5 Abs. 4) sind bei der Datenverarbeitung Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit). Das war hier nicht der Fall.

Die Umsetzung der gesetzlichen Vorgabe ist angesichts der finanziellen und räumlichen Möglichkeiten nicht immer einfach. Nach intensiven Gesprächen haben wir mit dem Bezirksamt folgende einvernehmliche Lösung gefunden:

- Die bisher vorhandenen Doppelarbeitsplätze werden – soweit räumlich und technisch möglich – abgeschafft. Wegen der dafür benötigten weiteren Räume hat das Bezirksamt einen Beschluss gefasst.

- Daneben werden zusätzliche optische Trennwände beschafft und dort aufgestellt, wo eine Verbesserung der Diskretion zu erwarten ist.

- Im Bereich der Warteräume wird ein deutlicher schriftlicher Hinweis angebracht, in dem eine vertrauliche Gesprächsumgebung angeboten wird.

- In allen Standorten wird darüber hinaus sichergestellt, dass bei Bedarf ein Einzelberatungsraum genutzt werden kann.

- In den Bereichen, in denen eine Abschaffung der Doppelarbeitsplätze nicht möglich ist, wird zukünftig durch interne dienstliche Organisation zugesichert, dass Mitarbeiter auf freie Arbeitsplätze so umgesetzt werden, dass der größtmögliche Abstand zwischen dem zu bedienenden Publikum hergestellt wird.

4.2.2 Straßen- und Verkehrsverwaltung

Die große Versuchung von Kennzeichenlesegeräten

Zunehmend wird der Einsatz der Videotechnik zusammen mit geeigneter Software zur Erfassung und Identifizierung von Kfz-Kennzeichen diskutiert und geplant. Dabei ist die Bandbreite der möglichen Einsatzbereiche und der verfolgten Ziele groß.

So wurde die Firma Toll Collect – nachdem das Bundeskabinett am 15. August 2001 die Einführung einer LKW-Maut auf Autobahnen beschlossen hat – damit beauftragt, im Jahr 2003 ein automatisches System aufzubauen, mit dem eine streckenbezogene Autobahnbenutzungsgebühr für Lastkraftwagen erhoben werden kann. Inwieweit dabei die Forderungen der Datenschutzbeauftragten des Bundes und der Länder[77] für eine datenschutzgerechte Ausgestaltung der LKW-Maut berücksichtigt werden, bleibt abzuwarten. In jedem Fall soll bei dem Vorhaben neben dem Satellitennavigationssystem GPS und der Mobilfunktechnologie auch eine umfangreiche Videotechnik zum Einsatz kommen. Vorgesehen ist, dass Videoanlagen an den Bundesautobahnen installiert werden, die alle vorbeifahrenden Fahrzeuge zu Kontrollzwecken erfassen. Mit Hilfe einer Software werden die Fahrzeuge im System nach bestimmten Merkmalen (z. B. Größe, Anzahl der Achsen) sortiert und die erfassten LKW-Kennzeichen gespeichert.

[77] Entschließung der 62. Konferenz vom 24.-26. Oktober 2001, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2001“, S. 33

In Brandenburg wird seit Anfang Dezember 2003 auf den Autobahnen der Abstand zwischen den Fahrzeugen gemessen. An 12 eingerichteten Messstellen dokumentieren Kameras sämtliche Fahrvorgänge, die in bereitstehenden Fahrzeugen von der Polizei auf Monitoren überwacht werden. Eine zweite Kamera ermöglicht die Identifizierung der Fahrer und Fahrzeuge. Somit ließen sich auch Verstöße gegen die Anschnallpflicht und das Telefonieren am Steuer feststellen[78].

In Hessen hat die Polizei den Einsatz der Videokameras zur Autokennzeichenerfassung getestet. Dabei soll es sich nur um einen Funktionstest gehandelt haben; Daten seien weder gesammelt noch gespeichert worden. Dem Landtag liegt ein Entwurf zur Änderung des Polizeigesetzes vor[79], die den Einsatz ermöglichen soll.

In Thüringen kam der Innenminister in Bedrängnis, weil er den Innenausschuss des Landtages nicht rechtzeitig über die installierten Kameras am Rennsteigtunnel informiert hat. Dabei soll es sich um ein Pilotprojekt gehandelt haben, bei dem die Installationsfirma Tests durchgeführt hat, bei denen nur Polizeifahrzeuge erfasst wurden. Durch eine technische Panne sind im September aber auch über 600 Kennzeichen von Privatautos erfasst worden[80].

In einem Modellversuch wurden in Bayern die automatische Aufnahme und der abschließende Abgleich von Autokennzeichen mit Fahndungserkenntnissen zum einen bei Verkehrsverstößen und zum anderen an zwei Grenzübergängen erprobt. Bei den Verkehrsverstößen wird lediglich ein Vorgang automatisiert, der zuvor bereits zur Routinearbeit der Polizei gehörte. Nach bayerischem Polizeirecht dürfen bei festgestellten Verkehrsverstößen die Kennzeichen mit dem Fahndungsbestand abgeglichen werden. Bei den Grenzübergängen wurde jedes Kennzeichen bei der Einreise abgelesen und mit der Fahndungsliste abgeglichen. Um diese Erfassungsmethode einsetzen zu können, muss aber das Polizeiaufgabengesetz geändert werden[81].

Dem AK II der Innenministerkonferenz liegt ein Konzept der Polizei vor, wie mit der Erfassung der Autokennzeichen mit Videokameras wirksame Kontrollen durchgeführt werden können. An zentralen Verkehrspunkten wie beispielsweise Autobahnen, Tunnels oder stark befahrenen Bundesstraßen sollen bundesweit die Kennzeichen aller vorüberfahrenden Autos digitalisiert und anschließend mit dem Fahndungsbestand abgeglichen werden. Bei einem „Treffer“ (beispielsweise gestohlenes Kfz, gefälschtes Kennzeichen oder gesuchter Halter) muss die Polizei

[78] Berliner Zeitung, 6. Januar 2004, S. 20
[79] Der Tagesspiegel, 31. Dezember 2003/1. Januar 2004, S. 6
[80] Neues Deutschland, 23. Dezember 2003, S. 5
[81] Frankfurter Allgemeine Zeitung, 30. Dezember 2003, S. 4

nur noch den Wagen anhalten. Die Innenministerkonferenz wird das Thema voraussichtlich auf der Frühjahrskonferenz 2004 erörtern.

Trotz anders lautender Pressemeldungen[82] ist der Berliner Innensenator zurückhaltend[83]. Er verwies auf ein Projekt zur Lenkzeitmessung, bei dem wir unter bestimmten technischen Voraussetzungen den Einsatz für möglich hielten[84]. Im Übrigen soll – entsprechende Rechtsgrundlagen vorausgesetzt – der Einsatz ausschließlich anlassbezogen erfolgen.

Die flächendeckende Erfassung von Autokennzeichen mit dem Ziel des Fahndungsabgleiches ist sehr umstritten. Sicherheitskreise halten das für ein geeignetes Mittel, um einerseits Straftaten aufzuklären und andererseits mit dem Abschreckungseffekt künftigen Straftaten vorzubeugen. Wir halten dagegen die flächendeckende Erfassung und Auswertung aller Kennzeichen von Kraftfahrzeugen, die zufällig eine bestimmte Strecke passieren, für nicht mit dem Verhältnismäßigkeitsgrundsatz vereinbar. Grundsätzlich werden zunächst alle für verdächtig gehalten; erst im zweiten Schritt erfolgt die Aussortierung der Unbescholtenen. Die Maßnahme gesellt sich damit zu der Reihe anderer Instrumente wie die Speicherung von Telekommunikationsdaten oder von DNA-Analysen, bei denen das rechtsstaatliche Prinzip der Unschuldsvermutung umgekehrt wird. Einvernehmen besteht mit der Senatsverwaltung für Inneres darüber, dass für den präventiv-polizeilichen Einsatz dieser Überwachungskameras zur flächendeckenden Erfassung der Kfz-Kennzeichen und der sich anschließenden Auswertung keine gesetzliche Grundlage vorhanden ist.

„Korridorinitiative Holland – Berlin“

> *Im Rahmen des Projektes „Korridorinitiative Holland – Berlin“ war geplant, Fahrzeuge, die im Güterfernverkehr von Holland nach Berlin fahren, daraufhin zu kontrollieren, ob von den Fahrzeugführern die vorgeschriebenen Lenk- und Ruhezeiten eingehalten werden. Erreicht werden sollte dies durch einen automatisierten Abgleich der Abfahrtzeiten der Fahrzeuge in Holland und deren Ankunftszeiten in Berlin.*

Das Verfahren sah vor, dass sämtliche an einem Kontrollpunkt an der deutsch-holländischen Grenze vorbeifahrenden Fahrzeuge von einer mobilen Videokamera mit angeschlossenem Bedienrechner erfasst werden. Durch die eingesetzte Software sollte das amtliche Kennzeichen aus dem vorderen Umriss der gespeicherten Fahrzeuge herausgelesen, als Videoaus-

[82] Berliner Morgenpost, 6. Januar 2004, S. 14
[83] taz, 20. Januar 2004, S. 21

schnitt für das polizeiliche Bedienpersonal sichtbar auf einem Kontrollmonitor abgebildet und gleichzeitig mittels einer OCR-Erkennungssoftware in ein PC-lesbares ASCI II Zeichen umgewandelt werden. Danach war anhand des Videobildes zu entscheiden, ob das aufgezeichnete Kfz-Kennzeichen einem Fahrzeug der gesuchten Zielgruppe (LKW im Güterfernverkehr) zugeordnet werden kann. Bei Fahrzeugen mit holländischen Kennzeichen sollte dies automatisiert von der eingesetzten Software erkannt werden. Konnte das vorbeifahrende Fahrzeug der Zielgruppe zugeordnet werden, sollte das Kfz-Kennzeichen gespeichert und per E-Mail an den Polizeipräsident in Berlin übermittelt werden.

In Berlin sollte der beschriebene Vorgang - zeitversetzt – an einer weiteren Kontrollstelle wiederholt werden. Sofern die vorausberechneten Routenzeiten unterschritten wurden, sollte dies vom Bedienrechner akustisch und optisch angezeigt und bei den betroffenen Fahrzeugen eine Verkehrskontrolle nach § 36 Abs. 5 StVO zur Feststellung der Lenk- und Ruhezeiten durchgeführt werden.

Alle diese Daten dürfen vom Polizeipräsidenten in Berlin - unabhängig davon, ob die Verarbeitung hier auf § 18 Abs. 1 ASOG oder als vorbereitende Handlung zur Durchführung einer Verkehrskontrolle auf § 36 Abs. 5 StVO gestützt werden kann – nur unter Berücksichtigung des Erforderlichkeitsgrundsatzes (§ 9 Abs. 1 BlnDSG) verarbeitet werden. Die Verarbeitung der Kennzeichendaten ist in jedem Fall nur dann zulässig, wenn sie für den angestrebten Zweck der Maßnahme – Durchführung einer Verkehrskontrolle zur Feststellung der Lenk- und Ruhezeiten im Güterfernverkehr – erforderlich ist.

Alle an den Kontrollstellen vorbeifahrende Fahrzeuge sollten von der Videoanlage erfasst und deren Kfz-Kennzeichen erhoben werden. Erst danach sollte eine Differenzierung danach erfolgen, ob das Fahrzeug der gesuchten Zielgruppe zuzuordnen ist. Dies hätte bedeutet, dass zunächst auch Fahrzeuge von der Maßnahme erfasst werden, die nicht in die definierte und gesuchte Zielgruppe (LKW im Güterfernverkehr) gehören. Die Speicherung der Kfz-Kennzeichen dieser Fahrzeuge wäre in jedem Fall unzulässig, da die betroffenen Fahrer keine Lenk- und Ruhezeiten einzuhalten haben.

Aber auch wenn das vorbeifahrende Fahrzeug der gesuchten Zielgruppe hätte zugeordnet werden können, wäre ein Abgleich der Kennzeichen nur bei den Fahrzeugen möglich, die beide Kontrollstellen passieren. Ist dies nicht der Fall (z. B. bei Fahrzeugen, die von Holland nach München oder Hamburg fahren) wäre die Datenerhebung zur Vorbereitung einer Ver-

---

[84] vgl. nächsten Abschnitt

kehrskontrolle nach § 36 Abs. 5 StVO ungeeignet und nicht erforderlich. Auch die Verarbeitung dieser Kfz-Kennzeichen an der deutsch-holländischen Grenze wäre unzulässig.

Da die Zielsetzung der Maßnahme, nämlich die Kontrolle der Lenkzeiten, selbstverständlich gerechtfertigt ist, wäre zu überlegen gewesen, ob der Einsatz geeigneter Verschlüsselungstechniken dem Mangel abgeholfen hätte.

Wegen der Haushaltslage des Landes Berlin wurde das Projekt nicht realisiert.

Bereinigung der Fahrerlaubnisakten

Durch die am 1. Januar 1999 in Kraft getretenen straßenverkehrsrechtlichen Bestimmungen wurden die Vernichtungsfristen für bestimmte Unterlagen in den Führerscheinakten geändert. Die Bereinigung der Unterlagen wird seither auf der Grundlage einer vom Landeseinwohneramt Berlin (LEA) erlassenen Arbeitsanweisung für die Führerscheinstelle[85] durchgeführt. Um sicherzustellen, dass die Aktenbereinigung innerhalb der von der Senatsverwaltung für Stadtentwicklung zugesagten Zehn-Jahres-Frist abgeschlossen ist, erstellt diese jährlich einen Bericht über den Fortgang der Arbeiten.

Im Bericht von 2003 teilt die Senatsverwaltung mit, dass die Arbeitsanweisung kontinuierlich umgesetzt wird. Neben der anlassbezogenen Bearbeitung sind in den zwölf Monaten des Berichtszeitraums Sonderaktionen zur Aktenbereinigung durchgeführt worden, um die erforderlichen Jahresfallzahlen zu erreichen. Der gesamte Fahrerlaubnisaktenbestand hat sich seit Beginn der Aktion von 370.427 (= 100 %) durch Aussonderung und Bereinigung um 163.888 (rd. 44,2 %) auf einen Anteil von 206.539 (rd. 55,8 %) noch zu bereinigenden Akten verringert.

Danach ist davon auszugehen, dass die Bereinigung der Fahrerlaubnisakten wie vorgesehen bis zum 31. Dezember 2008 und damit innerhalb der vom Gesetzgeber eingeräumten Frist abgeschlossen werden kann.

[85] JB 1999, 4.2.4

4.3. Justiz und Finanzen

4.3.1 Justiz

Elektronischer Rechtsverkehr

Der Senat von Berlin hat 2003 ein Gesetz zur Anpassung verwaltungsverfahrensrechtlicher Vorschriften an den elektronischen Rechtsverkehr in das Abgeordnetenhaus eingebracht[86]. Durch das Gesetz wird der Einsatz der elektronischen qualifizierten Signatur nach dem Signaturgesetz in den Fällen geregelt, in denen ein Gesetz die Schriftform angeordnet hat. Das Gesetz zur elektronischen Signatur regelt die Möglichkeit des Einsatzes der elektronischen Signatur durch Änderung des Senatorengesetzes, des Landesbeamtengesetzes, des Berliner Wassergesetzes sowie des Berliner Datenschutzgesetzes. Nunmehr kann nach dem Berliner Datenschutzgesetz der Hinweis, dass die datenschutzrechtliche Einwilligungserklärung auch zusammen mit anderen Erklärungen erteilt werden kann, elektronisch erfolgen. Die Einwilligung selbst kann dagegen nicht elektronisch erteilt werden. Durch die Anpassung der verwaltungsverfahrensrechtlichen Vorschriften an den elektronischen Rechtsverkehr entfällt nunmehr das Gesetz zur Erprobung der elektronischen Signatur in der Berliner Verwaltung.

Friedman – auch ein Fall für den Datenschutz

> *In der Presse wurde in ausführlicher Form über ein gegen den Fernsehmoderator Michel Friedman eingeleitetes strafrechtliches Ermittlungsverfahren wegen des Verdachts des Betäubungsmittelmissbrauchs berichtet. Bei den veröffentlichten Details stellte sich aus datenschutzrechtlicher Sicht die Frage, ob unzulässigerweise Daten von der Polizei, die die Ermittlungen durchgeführt hatte, oder der für das Verfahren zuständigen Staatsanwaltschaft erfolgt waren. Insbesondere waren Informationen aus einer in einem anderen Ermittlungsverfahren durchgeführten Telefonüberwachungsmaßnahme an die Öffentlichkeit gelangt.*

Weder die Polizei noch die Staatsanwaltschaft haben nach einer von uns durchgeführten Prüfung unzulässigerweise Daten aus dem Verfahren an Dritte übermittelt. Interessant ist an dem Fall Friedman aus datenschutzrechtlicher Sicht, dass das Verfahren aufgrund von Erkenntnissen aus einer Telefonüberwachungsmaßnahme in einem Ermittlungsverfahren we-

[86] Abghs.-Drs. 15/1699

gen Menschenhandels und anderer Delikte eingeleitet worden war. Aus den Protokollierungen der überwachten Telefongespräche hatten sich Hinweise auf die Person Friedman ergeben, obwohl sich das Ermittlungsverfahren nicht gegen ihn richtete. Er war beim Abhören der Gespräche auch an seiner Stimme erkannt worden. Wie die Erkenntnisse aus den durchgeführten Telefonüberwachsmaßnahmen an die Öffentlichkeit geraten sind, bleibt ungeklärt. Es stellt sich jedoch aus datenschutzrechtlicher Sicht die Frage: Wie geschützt ist eine Telefonüberwachungsmaßnahme? Das Risiko, dass Daten unbefugt übermittelt werden, wird sich nie ausschließen lassen; aber Betroffener einer Telefonüberwachungsmaßnahme kann jede Person sein. Mit der steigenden Zahl von Telefonüberwachungsmaßnahmen steigt auch das Risiko für jedermann, dass er in Strafverfahren verwickelt werden kann.

Datenschutz in der Zwangsvollstreckung

Auch in diesem Berichtszeitraum hat sich gezeigt, dass der informationellen Selbstbestimmung bei Zwangsvollstreckungsmaßnahmen nicht hinreichend Beachtung geschenkt wird[87].

> *Ein Hauseigentümer, gegen den die Zwangsverwaltung seiner Immobilie angeordnet worden war, beschwerte sich darüber, dass der gerichtlich bestellte Zwangsverwalter allen Mietern den vollständigen Beschluss des Amtsgerichts zugesandt hatte. Daraus war die Höhe der Belastung und angefallenen Zinskosten ersichtlich. Der Enkel des Petenten wurde einige Zeit später von einem Mitschüler darauf angesprochen und zur Herausgabe seines Besitzes genötigt.*

Zwar müssen die Mieter über die Zwangsverwaltung benachrichtigt werden, da ihnen der Zwangsverwalter nunmehr als neuer Gläubiger gegenübersteht. Die Kenntnis der Belastung des Mietgrundstücks ist aber hierfür nicht erforderlich (§ 9 BlnDSG). Der Zwangsverwalter verwies darauf, dass nach § 9 Nr. 2 Zwangsversteigerungsgesetz (ZVG) der Mieter Beteiligter am Zwangsverwaltungs- und auch am Zwangsversteigerungsverfahren ist und er damit ohnehin ein Recht zur Einsicht in das Grundbuch habe. Die Übersendung des vollständigen Beschlusses sei bei ihm seit Jahrzehnten Praxis.

Dem ist entgegenzuhalten, dass ein Recht auf Akteneinsicht nicht die Befugnis einräumt, allen Personen, denen dieses Recht unter gewissen Umständen zusteht, sämtliche Unterlagen unaufgefordert zuzusenden. Vielmehr setzt § 9 Nr. 2 ZVG voraus, dass das Mietrecht beim Vollstreckungsgericht angemeldet ist, was die wenigsten Mieter tun werden. Hinzu

[87] vgl. auch JB 2002, 4.3.1 sowie unten 4.3.2

kommt, dass die Einsichtnahme in das Grundbuch ein berechtigtes Interesse voraussetzt (§ 12 Grundbuchordnung), das z. B. erst dann vorliegt, wenn ein Mieter das Grundstück ersteigern will. Langjährige Praxis ist schon gar keine Rechtfertigung für Verstöße gegen den Datenschutz. Die Übersendung des vollständigen Beschlusses, der zwangsläufig die Belastungen enthält, ist damit unzulässig.

> *Eine Bürgerin beschwerte sich bei uns darüber, dass ein Gerichtsvollzieher im Rahmen der Zustellung einer Ladung auf dem Briefumschlag vermerkt hatte, dass es sich um die Ladung zur Abgabe einer eidesstattlichen Versicherung handelte. Sie bat uns, die Zulässigkeit einer solchen Offenbarung des Inhaltes der Zustellung zu prüfen.*

Der Direktor des für den Gerichtsvollzieher zuständigen Amtsgerichts teilte uns daraufhin mit, dass eine derartige Kennzeichnung des benutzten Briefumschlages nicht zulässig und der Gerichtsvollzieher hierüber auch in Kenntnis gesetzt worden sei. Wir hoffen, dass es sich bei dieser Form der Zustellung nur um einen Einzelfall gehandelt hat.

Rechtswirklichkeit der Telefonüberwachung in Deutschland

Die Überwachung von Telefonanschlüssen in Deutschland nimmt weiter drastisch zu. Die Zahl der Ermittlungsverfahren, in denen TKÜ-Anordnungen erfolgten, hat sich im Zeitraum von 1996 bis 2001 um 80 % erhöht; die Gesamtzahl der TKÜ-Anordnungen pro Jahr im Zeitraum von 1990 bis 2000 ist um das Sechsfache auf 15.741 gestiegen. Dabei wurden in 21 % der Anordnungen zwischen 1.000 und 5.000 Gespräche, in 8 % der Anordnungen sogar mehr als 5.000 Gespräche abgehört. Zudem werden richterliche Anordnungen einer Überwachungsmaßnahme in vielen Fällen nur allgemein und ohne hinreichenden Einzelfallbezug begründet. Die gesetzliche Pflicht, die Betroffenen nachträglich zu informieren, wird nur in einer geringen Zahl von Fällen befolgt. Zu diesen Ergebnissen kommt ein im Auftrag des Bundesministeriums für Justiz erstelltes Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht in Freiburg, das im Mai 2003 vorgelegt wurde[88]. Die erheblichen Defizite bei der richterlichen Kontrolle werden auch durch eine Studie der Rechtsprofessoren Backes und Gusy von der Universität Bielefeld belegt, der zufolge nur ein Viertel der untersuchten Telefonüberwachungen entsprechend den Verfahrensvorschriften angeordnet wurde[89].

---

[88] „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO und anderer verdeckter Ermittlungsmaßnahmen“

[89] Backes, Otto; Gusy, Christoph u. a.: Wirksamkeitsbedingungen von Richtervorbehalten bei Telefonüberwachungen. Universität Bielefeld, Dezember 2002

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung[90] den Anstieg der Zahl der Verfahren, in denen Telefonüberwachungen angeordnet werden, äußerst kritisch bewertet und darauf hingewiesen, dass damit gravierende Eingriffe in das Persönlichkeitsrecht der Betroffenen, zu denen auch unbeteiligte Dritte gehören, verbunden sind. Telefonüberwachungen müssen daher ultima ratio bleiben. Wir hoffen, dass die Bundesregierung aus den Gutachten die erforderlichen Konsequenzen zieht und zügig Maßnahmen zur Beseitigung der strukturellen Mängel ergreift.

4.3.2 Finanzen

Datenschutz in der Abgabenordnung

Im Herbst dieses Jahres hat erneut die gemeinsame Arbeitsgruppe mit Mitgliedern des Bundesfinanzministeriums, der Länderfinanzverwaltungen und der Datenschutzbeauftragten getagt, um über die Aufnahme datenschutzrechtlicher Vorschriften in die Abgabenordnung zu beraten. Es bestand Einigkeit darüber, dass so schnell wie möglich versucht werden soll, diejenigen Regelungen in ein Gesetzgebungsverfahren aufzunehmen, bei denen zwischen den Arbeitsgruppenmitgliedern bereits Einvernehmen erzielt worden ist. Bei anderen von den Arbeitsgruppenmitgliedern als erforderlich angesehenen Regelungen bedarf es noch verfassungsrechtlicher Prüfungen der Gesetzgebungskompetenz, die im Steuerbereich aus historischen Gründen nur für die verfahrensrechtlichen Regelungen, nicht jedoch für organisatorische Regelungen bei dem Bundesgesetzgeber liegen.

Steueränderungsgesetz 2003

Das Steueränderungsgesetz 2003[91] schafft die gesetzlichen Grundlagen für die Einführung der elektronischen Lohnsteuerkarte und damit eines vereinfachten Lohnsteuerabzugsverfahrens (§ 41 b EStG-E). Bei diesem Verfahren übermittelt der Arbeitgeber erstmals elektronisch die Daten der bisherigen Lohnsteuerkarte an die Finanzverwaltung. Dadurch wird der Erfassungsaufwand des Finanzamtes verringert. Zum Zwecke der Datenübertragung erhält

[90] Entschließung der 66. Konferenz vom 25./26. September 2003 „Konsequenzen aus der Untersuchung des Max-Planck-Instituts über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation“, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2003“, S. 40

[91] BGBl. I, S. 2645

jeder Steuerpflichtige ein Ordnungsmerkmal, das nach einer amtlichen Vergabe aus dem Namen, Vornamen und Geburtsdatum gebildet wird. Das Ordnungsmerkmal darf nur für Zwecke des Besteuerungsverfahrens gebildet oder verarbeitet werden. Die Datenschutzbeauftragten haben kritisiert, dass bei der Bildung des Ordnungsmerkmals (E-Tin) eine Mehrfachvergabe nicht hingenommen werden kann. Bei der hier vorgesehenen Bildung des Ordnungsmerkmals nimmt das Bundesfinanzministerium ein wenn auch geringes Restrisiko an Mehrfachvergabe von etwa 0,053 % hin. Abhilfe könnte hier ein weiteres Ordnungsmerkmal schaffen, das bei der Bildung der E-Tin hinzukommen könnte.

Nachdem die Bundesregierung in dem eingebrachten Entwurf des Gesetzes zunächst darauf verzichtet hatte, in der Abgabenordnung ein Identifikationsmerkmal für jeden Steuerpflichtigen einzuführen, haben die Fraktionen von SPD und Bündnis 90/Die Grünen einen Änderungsantrag eingebracht, mit dem dieses doch eingeführt werden soll. Nach § 139 a soll das Bundesamt für Finanzen jedem Steuerpflichtigen für Zwecke seiner eindeutigen Identifizierung im Besteuerungsverfahren ein einheitliches dauerhaftes Merkmal zuteilen. Die Zuteilung des Identifikationsmerkmals soll dem Steuerpflichtigen unverzüglich mitgeteilt werden.

Das Bundesamt für Finanzen soll zu den natürlichen Personen die Identifikations- und gegebenenfalls auch die Wirtschaftsidentifikationsnummer, die personenbezogenen Daten wie den vollständigen Namen, Titel, Geburtsort und Geburtsdatum sowie Geschlecht, gegenwärtige und letzte bekannte Anschrift, Sterbetag und die zuständigen Finanzämter speichern. Die Meldebehörden sollen dem Bundesamt für Finanzen in Zukunft für jeden Bürger mit Hauptwohnsitz die entsprechenden Daten aus dem Melderegister melden. Die Mitteilung erfolgt schon bei der ersten Speicherung der Daten im Melderegister nach der Geburt eines Menschen. Es ist vorgesehen, dass durch eine Änderung des Melderechtsrahmengesetzes die Meldebehörden in Zukunft für Zwecke der eindeutigen Identifizierung des Einwohners im Besteuerungsverfahren die Identifikationsnummer im Melderegister speichern müssen.

Die Speicherung der Identifikationsmerkmale beim Bundesamt für Finanzen führt dazu, dass das Bundesamt für Finanzen ein vollständiges Register aller Einwohner der Bundesrepublik Deutschland erhält. Bei der Frage, wer steuerpflichtig ist, wird in der Begründung zu den Gesetzesvorschlägen darauf hingewiesen, dass es nur darauf ankommt, dass eine Steuerpflicht besteht, nicht aber, dass eine Steuer tatsächlich geschuldet wird. Deshalb sollen auch schon Neugeborene in der Datei gespeichert werden. Die Datenschutzbeauftragten haben ein zentrales Melderegister immer abgelehnt. Die Einführung eines zentralen Melderegisters durch die Hintertür kann daran nichts ändern. Die mit einem zentralen Register verbundenen Risiken sind weitaus höher als bei regional geführten Registern.

Selbst wenn ein zentrales Register für den Steuerbereich erforderlich sein sollte, ist eine Speicherung bereits Neugeborener, d. h. aller Kinder ohne eine konkrete Steuerpflicht dieser Kinder, nicht erforderlich und damit unverhältnismäßig. Eine automatische Übermittlung der Meldedaten an das Bundesamt für Finanzen durch die Meldebehörden ist aus diesem Grund aus datenschutzrechtlicher Sicht ebenfalls nicht erforderlich.

Die im Gesetzentwurf vorgesehene Speicherung der steuerlichen Identifikationsnummer im Melderegister dient nicht der Aufgabenerfüllung der Meldebehörden. Da die im Melderegister aufgeführten personenbezogenen Daten von bestimmten öffentlichen Stellen auch online abgerufen werden können, bestehen erhebliche datenschutzrechtliche Bedenken gegen die Speicherung der Identifikationsnummer bei den Meldestellen. Die Identifikationsnummer stellt einen großen Schritt zu einem Personenkennzeichen dar, vor dem die Datenschützer immer eindringlich gewarnt haben. Der nächste Schritt ist dann ein zentrales Melderegister für die gesamte Bundesrepublik Deutschland. Hiervor können die Datenschutzbeauftragten nur warnen.

Der Bundesbeauftragte für den Datenschutz hat im Gesetzgebungsverfahren zumindest erreicht, dass eine strikte Zweckbindungsregelung für die Verwendung der beim Bundesamt für Finanzen vorgesehenen Datenbank in das Gesetz aufgenommen wird. Damit wird ausgeschlossen, dass das Bundesamt für Finanzen Auskünfte an andere öffentliche und nichtöffentliche Stellen erteilen darf.

Das Mittelalter kehrt zurück – die Parkkralle oder der moderne Pranger

> *Durch Presseveröffentlichungen wurden wir darauf aufmerksam, dass die Finanzverwaltung den Einsatz einer Parkkralle zum Eintreiben säumiger Kraftfahrzeugsteuer testen wolle.*

Der Einsatz der Parkkralle erfolgt im Zusammenhang mit einem gegen den säumigen Kraftfahrzeugschuldner durchgeführten Vollstreckungsverfahren. Der Steuerschuldner wird zunächst schriftlich gemahnt und auf die möglichen Vollstreckungsmaßnahmen hingewiesen. Dabei wird er auch auf den Einsatz der Parkkralle hingewiesen. Wird die Vollstreckung tatsächlich durchgeführt, wird an dem Fahrzeug das Pfandsiegel angebracht und am vorderen linken Reifen die gelb leuchtende Parkkralle als Wegfahrsperre. Das Fahrzeug erhält einen Aufkleber mit der Telefonnummer des zuständigen Finanzamtes. In einem gleichzeitigen

Schreiben wird der Steuerschuldner darauf hingewiesen, dass er drei Tage Zeit hat, den rückständigen Steuerbetrag zu entrichten, ansonsten würde sein Fahrzeug verwertet.

Wir haben den Einsatz der Parkkralle gegenüber der Senatsverwaltung für Finanzen beanstandet. Der Einsatz der Parkkralle stellt aus datenschutzrechtlicher Sicht eine Übermittlung personenbezogener oder personenbeziehbarer Daten an Dritte dar, für die es nach § 13 BlnDSG einer Rechtsgrundlage bedarf. Auch nach § 30 Abs. 4 AO bedarf es einer Rechtsgrundlage für die Offenbarung steuerlicher Daten an Dritte.

Die Finanzverwaltung geht davon aus, dass § 286 Abs. 1 AO eine Rechtsgrundlage darstellt. Diese Bestimmung setzt voraus, dass der Vollziehungsbeamte den Vollstreckungsgegenstand in Besitz nimmt. Wenn die Befriedigung dadurch nicht gefährdet wird, kann er die Sache auch im Besitz des Schuldners lassen, muss sie aber dafür durch das Pfandsiegel oder in sonstiger Weise kenntlich machen.

Der Einsatz der Parkkralle erfolgt neben der Anbringung des Pfandsiegels. Er dient allein dazu, Druck auf den Vollstreckungsschuldner auszuüben, die Steuerschuld nunmehr zu bezahlen. Beim Einsatz der Parkkralle wird deshalb auch immer wieder von Druckpfändung gesprochen.

Bereits das Anbringen des Pfandsiegels stellt eine Offenbarung von Steuerdaten dar, durch die Handlungsdruck auf den Schuldner ausgeübt wird. Für das Anbringen des Pfandsiegels gibt es allerdings eine gesetzliche Grundlage. Die nicht gesetzlich geregelte große gelbe Parkkralle stellt dagegen den Schuldner in unverhältnismäßiger Weise an den Pranger, da sie durch ihre Größe und Signalwirkung in der Farbe kaum zu übersehen ist. Sie dient allein dem Zweck, Druck auf den Schuldner auszuüben. Von der Oberfinanzdirektion Berlin wurde die Parkkralle auch schon als Wunderwaffe und modernes Folterinstrument bezeichnet. Leider lässt sich die Parkkralle nicht an tiefergelegten Fahrzeugen oder Fahrzeugen mit extra breiten Reifen anlegen, so dass der Druck auf den säumigen Steuerschuldner nicht bei jedem Fahrzeug ausgeübt werden kann. Ob dies im Sinne der Steuergerechtigkeit ist, wagen wir zu bezweifeln.

4.4 Sozialordnung

4.4.1 Personaldatenschutz

Das Stellenpoolgesetz

> *Mit dem Gesetz zur Einrichtung eines zentralen Personalüberhangmanagements (Stellenpool)[92] wurden die gesetzlichen Grundlagen geschaffen für die Einrichtung eines zentralen Stellenpools des Landes Berlin. Der Stellenpool soll alle Personalüberhangkräfte des Landes Berlin aufnehmen und sich für eine schnellere und effizientere Vermittlung von Personalüberhangkräften sowie deren Qualifizierung einsetzen.*

Mit der Vermittlung von Personalüberhangkräften in freie Stellen oder als Aushilfskräfte zum Zweck der Qualifizierung durch das zentrale Personalüberhangmanagement sind immer auch Datenübermittlungen zwischen den beteiligten Stellen verbunden. Das zentrale Personalüberhangmanagement benötigt für seine Tätigkeit zahlreiche Personaldaten, die bisher nur die Personalverwaltungen gespeichert hatten. Hierfür bedarf es klarer gesetzlicher Regelungen.

Der in das Abgeordnetenhaus eingebrachte Entwurf des Gesetzes enthielt zunächst nur eine sehr allgemeine Datenverarbeitungsregelung sowie eine nicht abschließende Aufgabenregelung für den Stellenpool. Alles Nähere sollte in einer Rechtsverordnung geregelt werden. Die datenschutzrechtlichen Regelungen des Gesetzentwurfs waren im Vorfeld nicht mit uns abgestimmt worden.

Aus datenschutzrechtlicher Sicht ist es wichtig, die Aufgaben der neuen Behörde abschließend zu regeln, da die Rechtmäßigkeit der Datenverarbeitung an die gesetzlichen Aufgaben der Behörde anknüpft. Da es sich bei der personalaktenführenden Stelle und der vermittelnden und qualifizierenden Stelle um unterschiedliche Stellen handelt, muss sich dies auch an den datenschutzrechtlichen Regelungen erkennen lassen. Für die Personalaktenführung gilt das Landesbeamtengesetz. Die Datenverarbeitung des Personalüberhangmanagements war dagegen klar im Gesetz zu regeln.

Gemeinsam mit der Senatsverwaltung für Finanzen haben wir nach der Anhörung unserer Behörde die datenschutzrechtlichen Regelungen des Gesetzentwurfs überarbeitet. Das Gesetz hat nun eine klare und abschließende Aufgabenbeschreibung der Aufgaben des zentra-

---

[92] GVBl. 2003, S. 589

len Personalüberhangmanagements erhalten. In der überarbeiteten Datenverarbeitungsvorschrift (§ 4) werden die Datenverarbeitungsstufen im Einzelnen geregelt. Die Art der personenbezogenen Daten, die das zentrale Personalüberhangmanagement speichern darf, ist nunmehr aufgelistet (§ 4 Abs. 1). Die erforderlichen Datenübermittlungen an andere Stellen des Landes Berlin oder von diesen an das Personalüberhangmanagement sind jetzt ebenfalls gesetzlich geregelt. Außerdem ist eine klarstellende Löschungsregelung in das Gesetz aufgenommen worden.

Übermittlung amtsärztlicher Gutachten

> *Der Bedienstete einer Justizvollzugsanstalt beschwerte sich darüber, die Anstaltsleitung habe bei der Suche nach einer anderen dienstlichen Einsatzmöglichkeit für ihn ein Schreiben an 30 Behörden/Einrichtungen verschickt, in dem auszugsweise aus einem amtsärztlichen Gutachten zitiert wird. Das besagte Rundschreiben enthielt zwar nicht seinen konkreten Namen, wohl aber dessen Amtsbezeichnung, Besoldungsgruppe, Geburtsjahr, Zuständigkeit, Ausbildung sowie den Beginn seiner Tätigkeit im Berliner Strafvollzug.*

Der Anstaltsleiter sowie die Senatsverwaltung für Justiz teilten mit, den datenschutzrechtlichen Belangen des Petenten sei durch die anonymisierte Form der Sachverhaltsdarstellung und der nur auszugsweisen Datenübermittlung hinreichend Rechnung getragen worden. Ein Personenbezug sei nur mit besonderer Kenntnis der Personalstruktur in seiner Einrichtung möglich, über die in den angeschriebenen Behörden regelmäßig niemand verfügen dürfte.

Über das ITVB-Telefonverzeichnis der Berliner Verwaltung konnten wir bei entsprechender Sucheingabe der jeweiligen Zuständigkeit des Mitarbeiters die betreffenden Mitarbeiterinnen und Mitarbeiter der Justizvollzugsanstalt aufrufen. Wer darüber hinaus Kenntnis über Ausbildung und Tätigkeit im Berliner Justizvollzugsdienst hatte, hätte ohne weiteres einen Personenbezug herstellen können.

Die Datenübermittlung verstieß gegen § 81 a Abs. 2 Satz 2 Landesbeamtengesetz (LBG), wonach die übermittelten Daten nur für die nach § 77 Abs. 3, § 78 Abs. 2 und §§ 79 bis 81 zu treffende Entscheidung verarbeitet oder genutzt werden dürfen.

Auch § 56 d Abs. 1 Satz 4 i. V. m. Satz 1 bis 3 LBG konnte als Rechtsgrundlage für die Datenübermittlung nicht herangezogen werden. Danach dürfen Auskünfte aus der Personalakte

ohne Einwilligung des Betroffenen für Zwecke der Personalverwaltung oder Personalwirtschaft der obersten Dienstbehörde oder einer im Rahmen der Dienstaufsicht weisungsbefugten Behörde erteilt werden. Dies war im vorliegenden Fall ausschließlich die Senatsverwaltung für Justiz, nicht aber die übrigen im Verteiler des Schreibens der JVA Heiligensee angegebenen Behörden.

Beihilfeanträge von Versorgungsempfängern

Ein Versorgungsempfänger hatte sich mit der Beschwerde an uns gewandt, Beihilfeanträge, die von Versorgungsempfängern des Landes Berlin per Post zum Landesverwaltungsamt geschickt oder im dortigen Hausbriefkasten eingeworfen werden, würden in der dortigen Poststelle geöffnet und weitergeleitet werden. Damit könne ein großer, nicht abgrenzbarer und für die unmittelbare Bearbeitung nicht zuständiger Personenkreis von personenbezogenen medizinischen Daten der Antragsteller Kenntnis erlangen.

In der Anleitung zum Ausfüllen von Beihilfeanträgen befindet sich der Hinweis, dass die Zusammenstellung der Aufwendungen und die Belege in einem besonderen verschlossenen Umschlag dem Beihilfeantrag beigefügt werden können, um sicherzustellen, dass die Belege nur der Beihilfestelle zur Kenntnis gelangen. Dagegen enthielt der Anleitungsbogen keine Hinweise, wie mit Brief- bzw. Postanträgen verfahren wird, deren Briefumschläge nicht den Zusatz „Vertraulich“, „Persönlich“ oder „Eigenhändig“ aufweisen.

Nach unserer Mangelfeststellung wurde die Anleitung um folgenden Punkt ergänzt:

„Behandlung der Eingänge: mit dem Zusatz ‚Vertraulich’, ‚Persönlich’ oder ‚Eigenhändig’ versehene Eingänge werden ungeöffnet an die/den betreffende/n Beihilfebearbeiterin/-bearbeiter weitergeleitet. Sofern der Zusatz nicht vermerkt wird, erfolgt die Öffnung der Eingänge in der Verteilungsstelle des Landesverwaltungsamtes Berlin, die diese an die Zentrale Beihilfestelle weiterleitet. Die Zusammenstellung der Aufwendungen und die Belege (Arztrechnungen, ärztliche Verordnungen und dergleichen) können auch in einem besonderen verschlossenen Umschlag, auf dem ‚Anlage zum Beihilfeantrag des ... (Name, Personal- bzw. Versorgungsnummer)’ zu vermerken ist, dem Beihilfeantrag beigefügt werden. Damit stellen Sie sicher, dass diese Unterlagen ausschließlich der/m Beihilfebearbeiterin/-bearbeiter zu Kenntnis gelangen.“ Der letzte Absatz von Abschnitt C Nr.7 wurde dagegen ersatzlos gestrichen.

Mitteilung über arbeitsrechtliche Maßnahmen gegenüber Dritten

> *Ein Mitarbeiter eines Einrichtungsmarktes war zweimal aufgrund einer Kundenbeschwerde schriftlich abgemahnt worden. In der Folgezeit nahm er wahr, wie der Filialleiter in einem Telefongespräch offenbar eine Kundin über die Abmahnung informiert hatte.*

Abmahnungen sind Vorgänge, die in die jeweiligen Personalakten der Beschäftigten aufgenommen werden und damit dem Personalaktengeheimnis unterfallen. Wegen ihrer besonderen Sensibilität unterliegen sie einer gesteigerten Fürsorgepflicht des Arbeitgebers.

Hier wollte der Filialleiter der verärgerten Kundin offensichtlich signalisieren, dass ihre Beschwerde ernst genommen wurde und zu arbeitsrechtlichen Konsequenzen geführt hat. Dies ist für sich gesehen nicht zu beanstanden, sondern liegt im berechtigten Interesse des Arbeitgebers am Erhalt seines Kundenstammes.

Nicht erforderlich dagegen war die Präzisierung der arbeitsrechtlichen Konsequenz als „Abmahnung“, zumal ein Anhörungsrecht des Betroffenen vor Aufnahme des Abmahnungsvorgangs in die Personalakte besteht.

Entbindung von der Schweigepflicht gegenüber Arbeitgeber

> *Eine Arbeitnehmerin wurde von ihrem Arbeitgeber aufgefordert, ihren Arzt von der Schweigepflicht zu befreien, damit Auskünfte über die Prognose zu ihrer Arbeitsunfähigkeit eingeholt werden können. Sie sandte daraufhin dem Arbeitgeber ein Attest der Ärztin zu, aus dem hervorging, dass die Arbeitsunfähigkeit weiter bestünde und eine Prognose zu diesem Zeitpunkt nicht möglich sei. Der Bitte des Arbeitgebers, die Ärztin von der Schweigepflicht zu befreien, war die Arbeitnehmerin jedoch nicht nachgekommen. Da das Arbeitsverhältnis krankheitsbedingt gekündigt wurde, bat die Arbeitnehmerin um datenschutzrechtliche Prüfung.*

Die Zulässigkeit der Erhebung von Gesundheitsdaten des Arbeitnehmers durch den Arbeitgeber richtet sich – soweit keine speziellen tarifrechtlichen oder vertraglichen Regelungen gelten – nach § 28 Abs. 1 Nr. 1 i. V. m. Abs. 6 Nr. 3 BDSG. Danach ist das Erheben, Verar-

beiten und Nutzen von besonderen personenbezogenen Daten 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.

Grundsätzlich ist ein Arbeitnehmer nicht verpflichtet, sich auf Wunsch des Arbeitgebers durch einen Arzt untersuchen zu lassen. Lässt sich der Arbeitnehmer durch einen Arzt untersuchen, so liegt hierin zunächst die Einwilligung in die Erhebung der für das Arbeitsverhältnis relevanten Gesundheitsdaten, nicht dagegen eine Einwilligung in die Weiterleitung der Befunddaten an den Arbeitgeber. Diese bleiben weiterhin im Gewahrsam des Arztes und dürfen nur in absoluten Ausnahmefällen bei Vorliegen einer entsprechenden Schweigepflichtentbindung an den Arbeitgeber übermittelt werden.

Im vorliegenden Fall wurde die Petentin durch den Arbeitgeber gebeten, eine ungefähre Prognose über die voraussichtliche Dauer Ihrer Erkrankung mit einer entsprechenden ärztlichen Bescheinigung mitzuteilen. Nur für den Fall, dass eine solche Prognose nicht möglich sein sollte, wurde sie ferner gebeten, ihren behandelnden Arzt von der Schweigepflicht zu entbinden, um die voraussichtliche Dauer bis zu der Genesung mitzuteilen.

Dieser Bitte war die Arbeitnehmerin nachgekommen, indem sie dem Arbeitgeber ein Attest ihrer Ärztin zusandte, aus dem hervorging, dass die Arbeitsunfähigkeit weiter bestehe und eine Prognose zu diesem Zeitpunkt nicht möglich sei. Insoweit hatte der Arbeitgeber die gewünschte Mitteilung der Ärztin erhalten. Eine weitergehende Entbindung von der ärztlichen Schweigepflicht war daher nicht erforderlich, die Aufforderung des Arbeitgebers war unzulässig.

Erhebung und Nutzung von E-Mail-Adressen zu Werbezwecken

> *Der betriebliche Datenschutzbeauftragte eines Unternehmens war an uns mit der Mitteilung herangetreten, nahezu alle Mitarbeiter hätten unaufgefordert eine Informations- und Werbe-E-Mail vom ver.di-Bundesvorsitzenden erhalten.*

Die Gewerkschaft teilte zur Herkunft der Daten mit, die bei der E-Mail-Aktion genutzten Adressen seien ihr von Mitgliedern übermittelt worden. Die weitere Nutzung sei der notwendigen Kommunikation einer Gewerkschaft mit ihren Mitgliedern und den Beschäftigten in einem Betrieb geschuldet, die zum gesetzlich geschützten Kernbereich einer Gewerkschaft

gehören. Um diese Aufgabe effektiv wahrnehmen zu können, könne oftmals auf die Nutzung der modernen Kommunikationsmittel nicht verzichtet werden.

Die Nutzung der Namen entsprach nicht der Zweckbindung und entbehrte somit einer rechtlichen Grundlage, zumal eine vorherige Einwilligung der Betroffenen ebenfalls nicht vorlag. Zwar gehört die Kommunikation einer Gewerkschaft, insbesondere mit ihren Mitgliedern, zu den gesetzlich geschützten Aufgaben, nicht dagegen die offensive Bewerbung und ungefragte Nutzung personenbezogener Daten von Nichtmitgliedern.

4.4.2 Gesundheit

Gesundheitsmodernisierungsgesetz – Sieg oder Niederlage des Datenschutzes?

Mit dem Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GMG)[93] wurde vom Bundestag im November 2003 nicht nur eines der größten Reformwerke im Gesundheitswesen seit Einführung der gesetzlichen Krankenversicherung vollendet; auch aus datenschutzrechtlicher Sicht enthält dieses Gesetz bahnbrechende, wenn auch teilweise mit Skepsis zu betrachtende Vorschriften. Zwei Aspekte sind dabei von besonderer Bedeutung: Die Kommunikation der verschiedensten Leistungserbringer untereinander sowie mit den Patientinnen und Patienten soll sich künftig primär elektronischer Mittel bedienen. Zum anderen werden völlig neue Verfahren der Transparenzmachung sowie der Kontrolle des Gesundheitswesens eingeführt.

Grundsatz ist, dass die papiergebundene Kommunikation „sobald und so umfassend wie möglich durch die elektronische und maschinell verwertbare Übermittlung ersetzt werden soll“ (§ 67 SGB V neu). Diese Zielsetzung wird ergänzt durch die Zielsetzung, zur Verbesserung der Qualität und der Wirtschaftlichkeit der Versorgung eine „persönliche elektronische Gesundheitsakte“ einzuführen, zu deren Finanzierung die Krankenkassen ermächtigt werden (§ 68 SGB V neu). Beide Bestimmungen haben zwar zunächst nur programmatischen und haushaltsrechtlichen Charakter, sie werden aber sicherlich die Zukunft der Kommunikationsbeziehungen im Gesundheitswesen stark beeinflussen.

[93] BGBl. I S. 2190-2259, vgl. auch Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003 „Datenschutzrechtliche Rahmenbedingungen zur Modernisierung des Systems der gesetzlichen Krankenversicherung“, Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2003“, S. 24

Eine zentrale Rolle im künftigen Gesundheitswesen soll offensichtlich die elektronische Gesundheitskarte spielen, die die bisher eingeführte Krankenversichertenkarte um eine ganze Reihe von Daten ergänzt (§ 291 a SGB V neu). Zusätzlich zu den bisher gebräuchlichen Verwaltungsdaten sollen in der Chipkarte Bereiche enthalten sein, die die Übermittlung ärztlicher Verordnungen in elektronischer und maschinell verwertbarer Form ermöglichen (elektronisches Rezept) und die als Berechtigungsnachweis für die Inanspruchnahme von Gesundheitsleistungen europaweit nach den europäischen Rechtsvorschriften dienen. Die elektronische Gesundheitskarte soll ferner so ausgestaltet sein, dass sie Notfalldaten, Daten für die Kommunikation unter den Ärzten (elektronischer Arztbrief), Daten einer Arzneimitteldokumentation, Daten im Sinne einer elektronischen Patientenakte, vom Patienten selbst angegebene Daten sowie Daten über in Anspruch genommene Leistungen enthält – mithin eine Karte, die ein umfassendes Bild über die gesundheitlichen Verhältnisse der einzelnen Versicherten darstellt. Die über die Verwaltungsdaten hinausgehenden Daten dürfen nur mit Einwilligung der Betroffenen aufgenommen werden, die jederzeit widerrufen werden kann. Dies entspricht einer Forderung, die die Datenschutzbeauftragten seit Jahren erhoben haben[94]. Bemerkenswert ist, dass zum ersten Mal in einem Gesetz auf die Bestimmungen des § 6 c BDSG Bezug genommen wird, der Rahmenbedingungen für den Einsatz von Chipkarten enthält.

Begleitet werden diese Maßnahmen durch die Einführung einer bundeseinheitlichen Krankenversichertennummer (§ 290 SGB V). Diese Krankenversichertennummer darf zwar nicht mit der Rentenversicherungsnummer identisch sein, stellt aber wegen ihrer bundesweiten Vereinheitlichung eine weitere Initiative zur Schaffung einer Personenkennziffer dar[95].

Diese auf die Durchsetzung von E-Government orientierten Bestimmungen sind eingebettet in eine Vielzahl von Vorschriften, die die Kontrolle sämtlicher Leistungen des Gesundheitswesens deutlich intensivieren. So werden Stellen zur Bekämpfung von Fehlverhalten im Gesundheitswesen (§ 81 a SGB V), Prüfungs- und Beschwerdeausschüsse (§ 105 SGB V), Stellen zur Bekämpfung von Fehlverhalten im Gesundheitswesen (§ 197 a SGB V) und eine Arbeitsgemeinschaft für Aufgaben der Datentransparenz eingeführt, deren Aufgabe der sektorenübergreifende Datenaustausch in der Krankenversicherung ist (§ 303 a ff. SGB V). Die Rechte des bereits vorhandenen medizinischen Dienstes werden ausgedehnt. Alle diese Stellen erhalten in unterschiedlichem Umfang Zugriff auf Datenbestände aus der Krankenversorgung. Dies geschieht allerdings nicht in beliebigem Umfang und personenbezogener

[94] zuletzt: Entschließung der 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. September 2003 zum Gesundheitsmodernisierungsgesetz, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2003“, S. 39

[95] vgl. 4.2.1

Form. Vielmehr enthält das Gesetz komplizierte Verfahren zur Stichprobenbildung, Anonymisierung und Pseudonymisierung.

Insbesondere die Einrichtungen zur Herstellung der Datentransparenz werden einem Pseudonymisierungsverfahren unterworfen, das bislang in der Gesetzgebung einmalig ist und erstmals in großem Umfang das Prinzip der Datenvermeidung und Datensparsamkeit (§ 3 a BSDG) umsetzt. Das Zusammenspiel zwischen einer Vertrauensstelle, die personenbezogene Daten erhält und pseudonymisiert,und einer Datenaufbereitungsstelle, die die pseudonymisierten (und damit für die verschiedenen Nutzungsberechtigten anonymen) Datenbestände generiert und verwaltet, entspricht Modellen, die von den Datenschutzbeauftragten seit Jahrzehnten für Verfahren vorgeschlagen worden sind, bei denen Einzelangaben benötigt werden, der Personenbezug aber nicht erforderlich ist.

Die Konsequenzen all dieser Vorschriften sind noch nicht überschaubar. Es wird in den nächsten Jahren eine große Aufgabe der Datenschutzbeauftragten sein zu beobachten, zu welchen Auswirkungen diese erstmals in diesem Umfang eingeführten Verfahren der elektronischen Kommunikation und der darauf gestützten Kontrollverfahren mit dem informationellen Selbstbestimmungsrecht vereinbar sind.

Hetzjagd auf Blaumacher und ihre Ärzte

> *Die Presse meldete, Krankenkassen verdächtigten über 200 Berliner Ärzte, ihre Patienten unnötig krank zu schreiben[96]. Die Betriebskrankenkasse des Landes Berlin (BKK) beabsichtige, so genannte „schwarze Listen" von Ärzten an Arbeitgeber zu versenden, damit diese anhand ihrer Krankschreibungen „schwarze Schafe" unter den Mitarbeitern und Ärzten aufspüren könnten. Die Berliner BKK wolle damit dem Beispiel der Hamburger BKK folgen, die eine solche „schwarze Liste" mit zehn auffälligen Arztpraxen bereits an mehr als 2000 Firmenchefs in der Hansestadt abgesandt habe. Der Hamburger BKK-Chef habe die Arbeitgeber aufgefordert, die verdächtigen „Blaumacher" in der Mitarbeiterschaft zu melden.*

Bei den Daten der Ärzte handelt es sich um Sozialdaten nach § 67 Abs. 1 Sozialgesetzbuch X (SGB X). Schon aus der Tatsache, dass ein Arzt die Arbeitsunfähigkeitsbescheinigung seines Patienten, die „Sozialdaten" im Sinne des § 67 SGB X enthält, ausstellen und unterschreiben muss, lässt sich erkennen, dass auch der Name des Arztes selbst ein Sozialdatum

[96] Der Tagesspiegel, 30. März 2003, S. 12

ist. Die Anwendbarkeit der Vorschriften des Sozialgesetzbuches lässt sich nicht mit dem Argument ausschließen, dass es sich hier nur um eine „abstrakt erstellte“ Liste der Ärzte handele, die einen besonderen Bezug zu einzelnen Patienten nicht aufweise. Die bekundete Absicht, die Ärzteliste an Arbeitgeber zu versenden mit dem Zweck, „Blaumacher aufzuspüren und zu melden“, zeigt, dass es ja gerade darum ging oder gehen sollte, den Personenbezug zum Patienten herzustellen. Durch die Versendung der Ärzteliste wäre praktisch jeder Patient, der zufällig von einem dort verzeichneten Arzt krankgeschrieben wurde, dem Verdacht ausgesetzt worden, ein „Blaumacher“ zu sein. Eine solche Stigmatisierung hätte also auch solche Arbeitnehmer getroffen, die wirklich erkrankt waren. Eine Rechtsgrundlage für die Übersendung einer solchen Ärzteliste gibt es nicht.

Nach Erörterungen der Rechtslage und nach Einbeziehung der Senatsverwaltung für Gesundheit, Soziales und Verbraucherschutz wurde entschieden, dass von der Berliner BKK keine „schwarzen Listen“ versendet werden würden.

Direktanfrage bei Versicherten

> *Eine in der BKK Berlin versicherte Patientin überreichte uns mit der Bitte um Prüfung einen Fragebogen, den die BKK direkt an sie geschickt hatte. Dort wurde im Zusammenhang mit der Arbeitsunfähigkeit der Patientin detailliert nach der Krankheit und den Beschwerden sowie sonstigen Befindlichkeiten gefragt wie z. B. nach dem bisherigen Krankheitsverlauf, nach der derzeitigen und geplanten Therapie, nach den festgestellten Befunden, nach dem täglichen Nikotin- oder Alkoholgenuss, nach sportlichen Initiativen, der Länge der wöchentlichen Arbeitszeit, der Berufstätigkeit, den aufgesuchten Fachärzten, nach Veränderungen des Lebensstils. Der Fragebogen umfasste knapp drei Seiten.*

Auf unsere Frage nach den rechtlichen Grundlagen dieser Befragung verwies die BKK darauf, dass Arztanfragen im Gegensatz zu dieser Patientenbefragung erst nach drei Monaten vorgesehen seien. Innerhalb dieser Zeit sei jedoch bereits die Chronifizierung der Krankheiten zu befürchten, und dies sei kaum noch rückführbar. Deshalb habe sich die BKK für die direkte Versichertenanfrage entschieden. Sie bezog sich auf den Mitwirkungsgrundsatz nach § 60 SGB I und darauf, dass Erfahrungen gezeigt hätten, dass durch rechtzeitiges Aufgreifen der Erkrankungen Therapien eingeleitet und Krankenhauseinweisungen vermieden werden könnten.

Mit dem Versenden des Fragebogens hatte die BKK ihre Versicherten aufgefordert, Fragen zu ihrem Krankheitsverlauf zu beantworten, die nach dem gesetzlichen Leistungssystem des SGB V nur vom Medizinischen Dienst der Krankenkassen (MDK) zu klären waren (§ 275 ff. SGB V). Es handelte sich dabei um eine Erhebung von Sozialdaten, zu deren Erhebung der Gesetzgeber nur den MDK berechtigt hat. Nach § 275 Abs. 1 Nr. 3 a SGB V ist die Krankenkasse verpflichtet, zur Sicherung des Behandlungserfolgs, insbesondere zur Einleitung von Maßnahmen der Leistungsträger für die Wiederherstellung der Arbeitsfähigkeit, den MDK einzubeziehen. Wir haben dies der BKK mitgeteilt. Unsere Auffassung wird von der für die BKK zuständigen Aufsichtsbehörde geteilt.

Patienteninformation für die Verordnung von Heil- und Hilfsmitteln

> *Eine Patientin war nach einer Operation auf den Gebrauch eines im Handel befindlichen Hilfsmittels angewiesen, welches ihr als gesetzliche Versicherungsleistung vom Arzt, ihrem persönlichen Bedarf entsprechend, verordnet worden war. Sie wurde unvermutet von einer privaten Firma, die dieses Hilfsmittel auf dem Markt anbietet, angerufen und erhielt von der dortigen Mitarbeiterin die Mitteilung, dass die Firma sie fortan mit dem von ihr benötigten Hilfsmittel beliefern würde und dass die Firma für zukünftige Hilfsmittelbestellungen ihre Ansprechpartnerin sein werde. Auf Nachfrage, woher sie die Personal- und Krankheitsdaten habe, unterrichtete sie die Mitarbeiterin, dass die BKK die Patientendaten an die Firma übermittelt habe.*

Für das Vorgehen der gesetzlichen Krankenversicherungen, ohne Einverständnis des Versicherten personenbezogene Stammdaten sowie Daten zur medizinischen Versorgung mit Heil- und Hilfsmitteln an Leistungsbringer unmittelbar zu übermitteln, gibt es keine gesetzliche Grundlage. Aufgrund des § 302 Abs. 2 SGB V sind „Richtlinien über die Verordnung von Hilfsmitteln in der vertragsärztlichen Versorgung“ (Hilfsmittelrichtlinie) des Bundesausschusses der Ärzte und Krankenkassen ergangen. In der Fassung vom 17. Juni 1992[97] wurde unter Ziffer 27 geregelt, dass die Versicherten Anspruch auf eine zweckmäßige und ausreichende Versorgung mit Hilfsmitteln haben. Es besteht nach dieser Vorschrift jedoch kein Anspruch auf Leistungen, die nicht notwendig oder unwirtschaftlich sind. Nach Ziffer 28 der Richtlinie soll der Vertragsarzt die Versicherten auf die in diesen Richtlinien genannten Beschränkungen hinweisen.

[97] Beilage zum BAnz Nr. 183

Diese Richtlinien konkretisieren lediglich die im Sozialgesetzbuch, insbesondere in den Vorschriften der §§ 12, 126, 127 sowie 128 SGB V, definierten Leistungskategorien. Insbesondere aus § 127 Abs. 3 SGB V ergibt sich, dass die Krankenkassen bei den Leistungserbringern Preisvergleiche über Hilfsmittel durchführen und die Versicherten und Ärzte über preisgünstige Versorgungsmöglichkeiten und über Leistungserbringer, die bereit sind, zum Festbetrag zu liefern, informieren können. Die Krankenkassen können Preisvergleiche auch durch regionale Arbeitsgemeinschaften oder in Zusammenarbeit mit Verbraucherverbänden durchführen. Nach § 128 SGB V können Hilfsmittelverzeichnisse mit Festbeträgen erstellt werden. Auch bedürfen die Leistungserbringer nach §§ 124 bis 126 SGB V einer Zulassung.

Daraus ergibt sich, dass im Rahmen der Verhältnismäßigkeit im Sinne der Nr. 28 Hilfsmittelrichtlinie die Versicherten durchaus – wenn auch nur im vorgegebenen Rahmen – eine Wahlfreiheit haben, ob und von wem sie Hilfsmittel in Anspruch nehmen wollen. Mit seiner ärztlichen Verordnung nach § 33 SGB V für ein Hilfsmittel wendet sich der Patient somit zunächst an seine Krankenkasse und hat dann die Wahl, allerdings nur im Rahmen der Kassenleistung, d. h. nur in dem Umfang, wie auch sein Anspruch auf die Versorgung mit Hilfsmitteln nach § 2 sowie § 12 i. V. m. § 33 Abs. 2 SGB V entstanden ist. Diese Rechtsauffassung wird auch durch ein Urteil des Sozialgerichtes Gießen vom 28. April 2003 gestützt[98]. Wir haben unsere Rechtsauffassung, die von der Senatsverwaltung für Gesundheit, Soziales und Verbraucherschutz geteilt wird, der BKK mitgeteilt.

Die Blankovollmacht

> *Das Universitätsklinikum Benjamin Franklin (UKBF) legte seinen Patienten eine „Erklärung zum Datenschutz“ vor, die uns von Patienten wiederholt zur Prüfung weitergereicht wurde. Die Erklärung umfasste eine DIN-A4-Seite kleingedruckter rechtlicher Verzichtserklärungen, die apodiktisch jeweils mit Worten eingeleitet wurden wie: „Ich habe zur Kenntnis genommen ...“, „Mir ist bekannt ...“, „Mir ist bekannt gegeben worden ...“, „Ich bin davon unterrichtet worden ...“. Dies hatte eine unangebrachte Abschreckungswirkung auf Patienten.*

In diesem Kleingedruckten wurden Dinge angesprochen, die sich teilweise von selbst verstanden, weil sie Gegenstand geltender gesetzlicher Regelungen sind und einer vertragsrechtlichen Vereinbarung nicht mehr bedürfen. Ferner wurden Einverständniserklärungen verlangt, die in keinem Zusammenhang mit einem etwaigen Behandlungsziel stehen.

[98] Az.: S-21/9/KR 251/02

Wir haben dem Krankenhaus empfohlen, diese Erklärung nicht mehr zu verwenden. Das öffentliche Gesundheitsversorgungssystem ist im Sozialgesetzbuch geregelt. Soweit der Gesetzgeber Regelungen geschaffen hat, bedarf es vertragsrechtlicher Erklärungen nicht mehr. Nur in Ausnahmefällen kann mitunter eine Überprüfung sinnvoll sein, ob eine gesetzliche Regelung vertragsrechtlich modifiziert werden kann oder darf. Einem Patienten darf daher nicht zugemutet werden, wenn er erkrankt und ins Krankenhaus eingewiesen wird, einen derart aufwändigen Verhandlungstext lesen zu müssen. Nach langwierigen Verhandlungen ist es gelungen, das UKBF hiervon zu überzeugen und eine Überarbeitung der Erklärung einzuleiten. Eine Abänderung wurde vom UKBF zwar zugesagt, jedoch befindet sich eine Neufassung, die sich auf das unbedingt Notwendige reduziert, noch in Arbeit.

Fälschungssichere Hunde für Berlin?

> *Seit März 1999 beschäftigt sich Berlin mit dem Entwurf einer gesetzlichen Regelung zum Halten und Führen von Hunden in Berlin. Uns sind im Laufe der Jahre wechselnde Entwürfe vorgelegt worden, wobei die Aktivität des Gesetzgebers und der Verwaltung immer dann zunahm, wenn wieder einmal ein hilfloser Mensch von einem Kampfhund angefallen wurde. Auch dieses Jahr wurde laut einer Pressemeldung[99] ein Kind angefallen. In der Pressemeldung hieß es: „Nach der Kampfhundattacke auf den kleinen Dennis einigt sich die Koalition auf ein neues Hundegesetz."*

Wir hatten zu vergangenen Entwürfen immer wieder Stellung genommen und wesentliche datenschutzrechtliche Verbesserungen erreicht. Doch diesmal ließ man sich etwas Besonderes einfallen: Hunde sollen durch Implantation eines fälschungssicheren Chips gekennzeichnet werden. Im Entwurf heißt es dazu lapidar: Hunde sind mit einem Chip nach ISO-Norm fälschungssicher zu kennzeichnen. Die Kennzeichnung ist der zuständigen Behörde unter Angabe der Chipnummer auf Verlangen mitzuteilen (§ 1 Abs. 5).

Die Idee einer fälschungssicheren Kennzeichnung des Hundes durch Implantation eines Chips wirft Probleme im Hinblick auf die Geeignetheit der Maßnahme wie auch deren Durchsetzbarkeit und Aufrechterhaltung im Verlauf der Lebenszeit eines Hundes auf. Die fälschungssichere Kennzeichnung bewahrt die Öffentlichkeit nicht vor den Gefahren, die von einem gefährlichen Hund ausgehen. Und sie könnte nur bedingt den Zugriff auf den verantwortlichen Halter ermöglichen.

---

[99] Der Tagesspiegel, 19. September 2003, S. 13

Fraglich ist schon, ob „Fälschungssicherheit“ überhaupt erreichbar wäre oder ob der Chip nicht mit neuen Daten geladen werden kann. Ungeklärt ist auch, wie gewährleistet werden soll, dass das Implantat – selbst wenn es fälschungssicher sein sollte – nicht ausgetauscht werden kann.

Hinzu kommt die Frage nach der Verhältnismäßigkeit des Eigentumseingriffes, da insbesondere Hunde betroffen sind, die nicht gefährlich sind – also der weitaus überwiegende Teil. Während die Halsbandkapsel mit den Daten des Eigentümers nur umgelegt werden muss, sofern der Hund das befriedete Besitztum des Hundehalters verlässt, muss die Implantation nach dem Gesetzeswortlaut bei jedem Hund erfolgen, auch wenn der Hund das befriedete Besitztum nicht verlassen soll.

Unklar ist, wie die Auslesung des implantierten Chips erfolgen soll, wer über solche Lesegeräte verfügen und wer zu welchen Anlässen die Chip-Nummer erheben darf.

Unzureichend sind auch die Regelungen zum Halterwechsel. Ungeregelt bleibt, wer den neuen Halter zu melden hat, ob dies der alte oder der neue Halter für sich selbst sein soll. Nicht geregelt ist, wie mit den Daten des vorherigen Halters oder mehrerer vorheriger Halter verfahren werden soll. Ungeklärt ist auch die Frage, was im Falle des unwiederbringlichen Entlaufens eines Hundes mit dem Chip und den Daten des Hundehalters geschehen soll.

All diese Punkte zeigen, dass erhebliche Zweifel an der Verhältnismäßigkeit der Einführung eines fälschungssicheren Chips bestehen.

4.4.3 Sozial- und Jugendverwaltung

BAföG-Schwindel

> *Zu erstaunlichen Ergebnissen führte in den Bundesländern der Abgleich der Daten von Studierenden, die Ausbildungsförderung (BAföG) beziehen, mit den Datenbeständen des Bundesamtes für Finanzen zu Freistellungsaufträgen von der Quellbesteuerung bei Spareinnahmen. In jedem zehnten Fall wurden falsche Angaben zum Vermögen gemacht*[100]*. Berlin hat an der Aktion teilgenommen.*

[100] Der Tagesspiegel, 19. August 2003, S. 1

Die Senatsverwaltung für Wissenschaft, Forschung und Kultur teilte dazu mit, dass die Bundes- und Landesministerien in § 45 d EStG eine im Sinne des § 67 a Abs. 2 Satz 2 Nr. 2 SGB X hinreichende gesetzliche Grundlage sähen. Diese Bestimmung lässt zu, dass die Daten aus den Freistellungsaufträgen zur Vermögensüberprüfung verwendet werden dürfen – aber selbstverständlich nur durch die Finanzbehörden, nicht durch andere Stellen. Im Sozialgesetzbuch ist eine Übermittlung von Sozialdaten nur zulässig, soweit sie in den Vorschriften des § 67 ff. SGB X gesetzlich angeordnet ist oder die Zustimmung der Betroffenen vorliegt. Von der Zustimmung der Betroffenen konnte hier nicht ausgegangen werden. Eine gesetzliche Regelung des Datenabgleichs im SGB ist also erforderlich. Inzwischen zeichnet sich auf der Bundes- bzw. Landesebene ab, die erforderlichen bereichsspezifischen gesetzlichen Regelungen für das BAföG ins Auge zu fassen.

Ein ähnlicher Datenabgleich wurde von der Senatsverwaltung für Bildung, Jugend und Sport für Leistungen nach dem Unterhaltsvorschussgesetz geplant. Es wurde die Auffassung vertreten, wenn der Datenabgleich der BAföG-Ämter nach § 45 d EStG zulässig sei, dann müsse er auch für die Unterhaltsvorschussstellen gestattet sein. Unverzichtbar ist jedoch auch hier eine gesetzliche Regelung.

Vorlage der Kontoauszüge bei Wohngeld und Sozialhilfe

> *Ein Bürger teilte mit, dass er Wohngeld beantragt habe und das Wohngeldamt Einsicht in Kontoauszüge verlangte und davon Kopien in der Wohngeldakte abheftete. Er wollte wissen, ob die Kontoauszüge zumindest teilweise geschwärzt werden dürfen und ob das Wohngeldamt überhaupt berechtigt ist, sich Kontoauszüge vorlegen zu lassen und abzuheften. Er war der Auffassung, mit der Vorlage seines Einkommensnachweises habe er das Seinige für die Leistungsbewilligung getan.*

Eine Verletzung von Datenschutzvorschriften durch die Vorlagepflicht und Abheftung ungeschwärzter Kontoauszüge in der Wohngeldakte konnten wir in dem hier zu prüfenden Fall nicht feststellen. Das zuständige Bezirksamt (Wohngeldstelle) hatte korrekt gehandelt. Antragsteller auf Wohngeld nach dem Wohngeldgesetz müssen ihre Einkommensverhältnisse vollständig nachweisen. Die Rechtsprechung geht davon aus, dass in den Fällen, in denen Einkünfte (deutlich) unterhalb des sozialhilferechtlichen Existenzminimums behauptet werden, Zweifel an der Darlegung der Einkommensverhältnisse gerechtfertigt sind. Das Oberverwaltungsgericht Berlin hatte bereits 1996[101] entschieden, dass ein Antragsteller glaubhaft

[101] Beschluss vom 21. Oktober 1996, Az.: 3 S 9.96

zu machen hat, wie er mit den angegebenen geringen Mitteln, die nicht nur den sozialhilferechtlichen Regelbedarf, sondern auch den Mindestbedarf deutlich unterschreiten, auskommt. Hierzu sei erforderlich, dass er im Einzelnen die Kosten seiner Lebenshaltung durch Angaben und Belege über regelmäßige Aufwendungen darlegt. Es sei nämlich nicht Aufgabe der Leistungsbehörde, dem Antragsteller nachzuweisen, dass er weitere Einnahmen oder sonstige Mittel hat, sondern es sei Sache des Antragstellers, die berechtigten Zweifel an der Vollständigkeit seiner Einkommensangaben zu entkräften. Für den Petenten war schwer nachvollziehbar, dass der strenge Maßstab zur Glaubhaftmachung gerade durch die Geringfügigkeit seiner Einkünfte bedingt war. Es reichte also nicht, für den Bezug von Wohngeld einen Einkommensnachweis über geringe Einkünfte vorzulegen, sondern gerade bei Unterschreiten des sozialhilferechtlichen Mindestbedarfes waren weitere Angaben bzw. Prüfungen durch die Behörde angezeigt. Diese Überprüfung konnte auch durch Vorlage bzw. Anforderung von Kontoauszügen erfolgen.

Wohngemeinschaft und Datenschutz

> *Eine Tochter entschloss sich, mit ihrem Freund zusammen zu wohnen. Da sie noch zur Schule ging und der Unterhalt der Eltern nicht reichte, beantragte sie mit ihrem Freund beim Sozialamt Hilfe zum Lebensunterhalt. Im Antragsverfahren schickte das Sozialamt an die unterhaltspflichtigen Eltern der Tochter eine Berechnung, in der alle Einkünfte und Angaben zu den Vermögensverhältnissen des Freundes der Tochter enthalten waren. Das Sozialamt ging nämlich davon aus, dass die Tochter mit ihrem Freund in eheähnlicher Gemeinschaft lebe und nicht besser gestellt werden dürfe als unterhaltspflichtige Ehegatten. Daher seien die Einkünfte, einschließlich des Unterhaltes, ihrem sozialhilferechtlichen Anspruch gegenüberzustellen und nur durch die ergänzende Hilfe zum Lebensunterhalt auszugleichen.*

Nur Unterhaltsverpflichtete haben ihre Vermögensverhältnisse gegenseitig offen zu legen. Für uns war nicht nachvollziehbar, warum das Sozialamt die Einkommensunterlagen des in Wirtschaftsgemeinschaft mit der Tochter lebenden Freundes an die unterhaltsverpflichteten Eltern der Tochter weiterleitete. Es war zwar vom Sozialamt für die Leistungsbemessung das Bestehen einer Wirtschaftsgemeinschaft zwischen der Tochter und ihrem Freund zu berücksichtigen. Jedoch hatte die Tochter keine Unterhaltsansprüche gegen den Freund, mit dem sie in dieser Wirtschaftsgemeinschaft lebte, so dass dieser auch nicht verpflichtet war, seiner Mitbewohnerin Auskunft über seine Vermögensverhältnisse zu geben. Erst recht konnte keine Verpflichtung bestehen, die Eltern der Tochter über seine Vermögensverhältnisse zu informieren. Für die Bedürftigkeitsfeststellung bei der Tochter war die Übermittlung der Ver-

mögensverhältnisse ihres Freundes an die Eltern der Tochter nicht erforderlich. Die Bedürftigkeit war vielmehr ausgehend von dem unstrittigen Tatbestand einer Wirtschaftsgemeinschaft in der gemeinsamen Wohnung feststellbar. Die durch das Bestehen einer Wirtschaftsgemeinschaft begründete Minderung des Bedarfs reichte bereits für sich aus, um den Leistungsanspruch der Tochter angemessen zu berechnen.

IT-Sicherheit im Verfahren BASIS I

Das Verfahren BASIS I (Berliner Automatisiertes Sozialhilfe Interaktionssystem) bildet die elektronische Grundlage für die Bearbeitung von Sozial- und Jugendhilfeangelegenheiten in den Bezirken und dem Landesamt für Gesundheit und Soziales. Es wird bereits seit 1994 in den Berliner Bezirken eingesetzt. Das Verfahren teilt sich in einzelne Softwarekomponenten auf, die nach dem Namen des Herstellers, des PROSOZ-Instituts Herten, auch unter dem Begriff PROSOZ zusammengefasst werden. Die seinerzeit für die Sicherheit des Verfahrens vorgesehene Konzeption hatten wir akzeptiert.

Das BASIS-I-Verfahren wurde ursprünglich für die Verwendung unter dem Betriebssystem MS-DOS oder einem dazu kompatiblen Betriebssystem konzipiert. Diese Betriebssysteme können – anders als z. B. Betriebssysteme wie UNIX oder MS Windows NT den parallelen Ablauf von mehreren Programmen (Multitasking, Multithreading) nicht unterstützen. Das Sicherheitskonzept wurde daher auch speziell für den Betrieb in einer DOS-Umgebung entwickelt und durch uns begleitet. Grundlegender Ansatz war eine dezentrale Verfahrensorganisation, die dazu führte, das jeder Bezirk PROSOZ eigenverantwortlich betrieb.

Durch die Einführung von MS Windows 3.11 bzw. Windows NT in den Sozialämtern entstanden neue Sicherheitsproblematiken. Bereits 1999 stellten wir bei diversen Kontrollen fest, dass es einen Handlungsbedarf zur Schließung neuer Sicherheitslücken gibt[102].

Ende der neunziger Jahre stellte Microsoft die Unterstützung für seine Betriebssysteme MS-DOS und Windows 3.x ein. In diesem Zusammenhang wurde der Betrieb einer DOS-basierenden Anwendung immer schwieriger, so dass bald nach der Einführung von PROSOZ mit der Entwicklung eines neuen moderneren Verfahrens begonnen wurde. Das neue Verfahren sollte eine Client-Server-Datenbank nutzen.

[102] JB 1999, 4.4.3

Dieses nachfolgende IT-Verfahren BASIS II bzw. BASIS 3000 der Berliner Sozialverwaltung sollte Ende 1999 in Betrieb gehen. Das auch von politischer Seite geforderte Nachfolgeverfahren sollte die funktionalen Defizite und softwareergonomischen Mängel beheben, die die Arbeit mit dem veralteten Verfahren erschwerten. Im Laufe der Zeit verzögerte sich der zunächst für Ende 1999 vorgesehene Fertigstellungstermin bis Ende 2003, ein Termin, an dem für das alte Verfahren keine Unterstützungsgarantie von dem Softwareherstellern mehr gegeben wurde. Das Projekt wurde schließlich wegen des unverhältnismäßigen zeitlichen Verzuges, für den je nach Position unterschiedliche Gründe angegeben wurden, aufgegeben.

Als Übergangslösung bis zum Einsatz eines modernen Verfahrens wurde PROSOZ/S für Windows von den Bezirken vorgesehen. Die wesentlichen Änderungen betreffen die Benutzeroberfläche und einige fachliche Belange. Sicherheitstechnisch benutzt dieses Verfahren jedoch die gleichen technischen Grundlagen wie schon die DOS-Version. Die bereits im Jahresbericht 1999 angesprochenen Sicherheitsprobleme wurden mit der neuen Lösung daher nicht gelöst. Mittlerweile ist die Migration von PROSOZ auf eine 32-BIT-Software abgeschlossen worden.

Durch die Umstellung des Betriebssystems auf den Arbeitsplatzsystemen sind die Bezirke angehalten, ihre Sicherheitskonzepte anzupassen. Schon für BASIS I war die Erstellung eines Sicherheitskonzepts durch den Verfahrensbetreiber (Bezirke) zwingend. In der Praxis wurden leider jedoch nur in den wenigsten Fällen Sicherheitskonzepte erstellt. Viele Bezirke warteten auf zentrale Vorgaben, übersahen dabei jedoch, dass jeder Bezirk eine unterschiedliche, individuelle Infrastruktur sowie eigene organisatorische Regelungen hat, die in ein Sicherheitskonzept einfließen müssen. Jede Risikoanalyse ist auf die jeweils vorhandene Situation abzustimmen. Betrachtet man den zunehmenden Vernetzungsgrad, so ist umso wichtiger, die Sicherheitsanforderungen in das ganze bezirkliche Sicherheitskonzept einzubeziehen.

Die Notwendigkeit eines Sicherheitskonzepts leitet sich bereits aus der 1999 beschlossenen IT-Sicherheitsrichtlinie her. Spätestens seit der 2001 erfolgten Novellierung des Berliner Datenschutzgesetzes wird durch § 5 Abs. 3 gesetzlich vorgeschrieben, dass Sicherheitskonzepte von Altverfahren neu zu entwickeln sind, wenn die Verfahren wesentliche Änderungen erfahren.

Die oben erwähnten kritischen Kontrollergebnisse aus dem Jahre 1999 waren auf eine unzureichende Umsetzung der von der BASIS-Geschäftsstelle herausgegebenen Anweisungen zur Schließung einer Sicherheitslücke des Verfahrens zurückzuführen. Mit der Umstellung

auf modernere Betriebssysteme sind jedoch nicht einmal die früheren Vorgaben mehr anwendbar, ohne dass die Sicherheitslücke kleiner geworden ist.

Die immer wieder beklagten Sicherheitsdefizite veranlassten die Betreiber jetzt zur Erstellung eines neuen Sicherheitskonzepts. Mit der Erstellung wurde der LIT unter Einbeziehung einer Unternehmensberatung beauftragt. Erfreulicherweise wurde uns noch 2003 ein Ergebnis vorgelegt, das auf Grundlage des Sicherheitshandbuchs und des Grundschutzhandbuchs des BSI erstellt wurde[103]. Im Ergebnis wurden unsere Bedenken bestätigt und weitreichende Vorschläge zur Verbesserung der Sicherheit unterbreitet, die aber sowohl tief greifende organisatorische Anforderungen als auch grundlegende Änderungen des Dateihaltungskonzepts verlangen.

4.4.4 Bauen, Wohnen und Umwelt

Anzeige von Baumängeln wird an Vermieter weitergeleitet

Ein Mieter hatte aufgrund eines beschädigten Hausdachs einen Wasserdurchlaufschaden an seiner Wohnungsdecke. Da der Vermieter den Schaden nicht beseitigte, wurde dieser vom Mieter unter Beifügung von Fotos vom Dachboden beim zuständigen Wohnungsaufsichtsamt angezeigt. Das Amt informierte den Vermieter über die Anzeige und führte in dessen Beisein eine Besichtigung des Dachbodens durch, um die Ursachen und Auswirkungen des Schadens zu ermitteln. Der Mieter beschwerte sich darüber, dass die Daten aus seiner Anzeige beim Wohnungsaufsichtsamt dem Vermieter bekannt gegeben worden waren.

Nach § 45 Abs. 1 Nr. 1 ASOG können Ordnungsbehörden personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs übermitteln, soweit das zur Erfüllung ordnungsbehördlicher Aufgaben erforderlich ist. Auch nach § 9 Abs. 1 BlnDSG ist die Verarbeitung (z. B. Übermittlung) von personenbezogenen Daten durch eine Behörde an Dritte nur zulässig, wenn dies zur rechtmäßigen Erfüllung der durch Gesetz der Daten verarbeitenden Stelle zugewiesenen Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist. Das Wohnungsaufsichtsamt hat nach § 1 Abs. 1 Wohnungsaufsichtsgesetz (WoAufGBln) die Beseitigung von Wohnmissständen, die Verbesserung von Wohnungsverhältnissen usw. sicherzustellen. Zu diesem Zweck kann es nach § 3 Abs. 1 WoAufGBln an-

[103] vgl. 3.5

ordnen, dass der Verfügungsberechtigte (Hauseigentümer) bestimmte Arbeiten an der Wohnsache durchführt bzw. nachholt.

Die Vorgehensweise und der Umfang der ordnungsrechtlichen Prüfung ergibt sich bei Beschwerden von betroffenen Mietern aus deren Angaben über Art, Ort und genaue Lage des Mangels. Unabhängig davon unterliegen die Verfügungsberechtigten, Besitzer und Bewohner von Wohnraum zur Beseitigung der angezeigten Mängel bestimmten Mitwirkungs- und Duldungspflichten. Nach § 10 Abs. 1 WoAufGBln haben sie zu ermöglichen, dass Mitarbeiter der Wohnungsaufsicht Gebäude, Wohnungen und Wohnräume betreten können. Ferner haben Sie der Wohnungsaufsichtsbehörde die erforderlichen Auskünfte zu geben und die hierfür erforderlichen Unterlagen vorzulegen. Danach kann die Mängelanzeige vom Aufsichtsamt nur dann umfassend bearbeitet werden und eine Verfügung zur Abhilfe an den Verfügungsberechtigten (Hauseigentümer) ergehen, wenn dieser vom Wohnungsaufsichtsamt über den Inhalt des Beschwerdeschreibens und über die Identität des Anzeigenerstatters regelmäßig informiert wird.

Die Übermittlung der Daten aus der Mangelanzeige des Mieters an den Verfügungsberechtigten ist danach zur Aufgabenerfüllung des Wohnungsaufsichtsamtes erforderlich und zulässig. Eine anonyme Bearbeitung der Anzeige gegenüber dem Verfügungsberechtigten ist nur in Ausnahmefällen – bei Vorliegen besonderer Umstände – möglich. Derartige Umstände hat der Anzeigende bei der Anzeigenerstattung darzulegen.

Milieuschutzrechtliches Genehmigungsverfahren

> *Ein Hauseigentümer beschwerte sich darüber, dass das Stadtplanungsamt Einzelheiten aus dem von ihm beantragten milieuschutzrechtlichen Genehmigungsverfahren – insbesondere den Stand des Baugenehmigungsverfahrens – an eine private Mieterberatungsfirma übermittelt hatte.*

Im milieuschutzrechtlichen Genehmigungsverfahren sind grundsätzlich zwei Varianten möglich: Beantragt der Eigentümer des Objektes lediglich kleinere Sanierungsmaßnahmen (z. B. im Sanitärbereich), wird das milieuschutzrechtliche Genehmigungsverfahren ausschließlich vom Stadtplanungsamt durchgeführt. Geht es jedoch um ein größeres Bauvorhaben (z. B. den Anbau von Balkonen), ist eine Baugenehmigung erforderlich, die beim zuständigen Bauamt zu beantragen ist. In diesem Fall wird das milieuschutzrechtliche Verfahren ein Teil des Baugenehmigungsverfahrens.

Nach § 173 Abs. 3 Satz 2 Baugesetzbuch (BauGB) hat die Genehmigungsbehörde die Mieter, Pächter und sonstige Nutzungsberechtigte in jedem Fall vor der Entscheidung über den Genehmigungsantrag anzuhören. Die Behörde ist mithin zur Kontaktaufnahme mit den Mietern verpflichtet und hat diese im Rahmen der Anhörung über das geplante Vorhaben und die Inhalte des Genehmigungsbescheides zu informieren.

Zur Durchführung der Anhörung und der damit verbundenen Mieterberatung bedient sich die Genehmigungsbehörde zumeist – so auch in dem Beschwerdefall – privatrechtlicher Mieterberatungsfirmen. Die genannten Aufgaben werden den Firmen vertraglich übertragen. Die Mieterberatungsfirmen erhalten damit Einblick in die Antrags- und Verfahrensunterlagen, informieren die Mieter über die sie betreffenden Inhalte des Genehmigungsbescheides und beraten sie über ihre Rechte und Pflichten. Durch die Mieterberatung erhalten die Mieter somit zwangsläufig Kenntnis von der Beantragung einer Baugenehmigung und Informationen über den Stand des Verfahrens.

Datenschutzrechtlich handelt es sich um eine Datenverarbeitung durch die Mieterberatungsfirma im Auftrag der Genehmigungsbehörde (§ 3 Abs. 1 Satz 1 BlnDSG). Die damit verbundene Weitergabe von personenbezogenen Daten des Eigentümers und Antragstellers an die Mieter kann auf § 13 BlnDSG i. V. m. den §§ 172 Abs. 4, 5 und 173 Abs. 3 Satz 2 BauGB gestützt werden und ist grundsätzlich zulässig.

In dem konkreten Einzelfall des Beschwerdeführers ergaben sich keine Anhaltpunkte dafür, dass die Mieterberatungsfirma personenbezogene Daten über den konkreten Auftrag hinaus verarbeitet (an die Mieter übermittelt) hat. Ein Verstoß gegen datenschutzrechtliche Bestimmungen konnte nicht festgestellt werden.

Herausgabe des Haustürschlüssels nur gegen Kopie des Personalausweises

Eine Hausverwaltung ließ in die Eingangstür eines Mietshauses ein neues Schloss einbauen. Vor Übergabe der neuen Schlüssel an die Mieter sollten diese jeweils ihren Personalausweis oder ein sonstiges amtliches Lichtbilddokument vorlegen. Die Vermieterin beabsichtigte, von den Unterlagen Kopien zu fertigen und zu den jeweiligen Mietverträgen zu nehmen.

Auch Akten und Aktensammlungen können dem Dateibegriff in § 3 Abs. 2 Satz 2 BDSG unterfallen. Dies ist dann der Fall, wenn diese nach bestimmten Merkmalen (z. B. Objekt, Wohnungsnummer usw.) geordnet und nach der Betreffangabe oder dem Namen (z. B. des Mieters) umgeordnet werden können. Mietverträge lassen sich nach den genannten Merkmalen ordnen bzw. umordnen. Dass dies nicht automatisiert erfolgt, ist für die datenschutzrechtliche Bewertung unerheblich. Ungeachtet dessen ergibt eine lebensnahe Betrachtung, dass ein Vermieter zur Verwaltung der Mieterdaten entweder – z. B. zur Berechnung der Betriebskosten, Führung der Mietkonten, zum Schriftwechsel mit den Vertragspartnern – einen Computer einsetzt oder die Mieterakten zumindest systematisch ordnet. Insofern sind die Bestimmungen des BDSG bei der Verarbeitung von Mieterdaten durch den Vermieter anzuwenden.

Bei der Speicherung von Daten aus den Personalausweisen der Mieter in den Mieterakten handelt es sich um die Verarbeitung von personenbezogenen Daten innerhalb eines Mietvertragsverhältnisses. Diese Datenverarbeitung ist nur zulässig, wenn es der Zweckbestimmung des Vertragsverhältnisses mit dem Betroffenen dient (§ 28 Abs. 1 Nr. 1 BDSG).

Die zweifelsfreie Feststellung der Identität des Vertragspartners dient der Zweckbestimmung des Vertragsverhältnisses. Insofern hat jeder Vermieter ein berechtigtes Interesse daran zu erfahren, von welchen Personen die Wohnungen tatsächlich bewohnt werden, bzw. die Schlüssel nur an diejenigen herauszugeben, die zur Entgegennahme vertraglich berechtigt sind.

Zur Feststellung der Identität ist es jedoch ausreichend, dass sich der Vermieter beim Vertragsabschluss oder – wie im vorliegenden Fall – bei der Schlüsselübergabe den Personalausweis bzw. ein anderes amtliches Lichtbilddokument des Abholers zur Einsichtnahme und Überprüfung vorlegen lässt. Die Anfertigung einer Kopie des Dokumentes für die Mieterakte und damit eine Speicherung der Daten ist für diesen bzw. jeden anderen mietvertraglichen Zweck nicht erforderlich und damit unzulässig.

Datenabgleich bei Besuchern des Reaktorbereichs im Hahn-Meitner-Institut

> *Kurzbesucher mit Zugang zum Sicherheitsbereich von Reaktoranlagen, für die keine Zuverlässigkeitsüberprüfung nach § 12 Atomgesetz (AtomG) durchgeführt wurde, sollen nach den Vorgaben des Bundesministeriums für Umwelt, Naturschutz und Reaktorsicherheit unter Abgleich polizeilicher Datensammlungen kurzfristig überprüft werden. In Berlin betrifft dies jährlich ca. 120 Besucher (z. B. Wissenschaftler) des Hahn-*

Meitner-Institutes, die in kleinen Gruppen durch die sensitiven Bereiche des Forschungsreaktors BER II geführt werden. Von der Senatsverwaltung für Stadtentwicklung wurden wir gebeten zu prüfen, unter welchen datenschutzrechtlichen Voraussetzungen diese Personen überprüft werden können.

In Ermangelung einer Rechtsgrundlage sowohl im AtomG wie auch im ASOG ist die Übermittlung von Daten aus den polizeilichen Datensammlungen durch den Polizeipräsidenten in Berlin an die Senatsverwaltung für Stadtentwicklung nur mit Einwilligung der betroffenen Besucher zulässig. Die Einwilligung bedarf grundsätzlich der Schriftform (§ 6 Abs. 4 BlnDSG), und der Betroffene ist zuvor über die Bedeutung der Einwilligung, den Verwendungszweck der Daten und die Rechtsfolgen einer Verweigerung der Einwilligung aufzuklären (§ 6 Abs. 3 BlnDSG).

Derzeit erfolgt mit Einwilligung der Betroffenen innerhalb von 24 Stunden nach Anmeldung des Besuches ein Datenabgleich in den bundesweiten Dateien INPOL und APIS. Die dafür erforderliche Einwilligungserklärung der Betroffenen wurde inhaltlich mit uns abgestimmt. Von dem Landeskriminalamt Berlin und der Senatsverwaltung für Inneres wurde jedoch angeregt, den Datenabgleich mit Einwilligung der Betroffenen um eine Abfrage des Datenbestandes im ISVB zu erweitern.

Die Einwilligung des Betroffenen in die Datenverarbeitung kann in keinem Fall bestehende gesetzliche Einschränkungen der Datenverarbeitung umgehen bzw. außer Kraft setzen. Die Verarbeitung von personenbezogenen Daten ist daher – auch wenn sie auf die Einwilligung des Betroffenen gestützt wird – nur zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Gesetz der Daten verarbeitenden Stelle zugewiesenen Aufgabe und für den jeweils damit verbundenen Zweck erforderlich ist (§ 9 Abs. 1 BlnDSG).

Entscheidend für die datenschutzrechtliche Zulässigkeit eines Datenabgleichs mit dem ISVB und die Übermittlung von Erkenntnissen an die Senatsverwaltung für Stadtentwicklung ist somit – unter Beachtung des Erforderlichkeitsgrundsatzes – die Ausgestaltung des Verfahrens. Das ISVB als zentrales Vorgangsverwaltungssystem des Polizeipräsidenten in Berlin enthält Datensätze über eine Vielzahl von Personen – egal, ob diese lediglich eine Anzeige erstattet haben oder selbst Täter, Opfer oder Zeuge einer Straftat oder Ordnungswidrigkeit sind. Eine ungefilterte Übermittlung dieser polizeilichen Erkenntnisse an die Senatsverwaltung für Stadtentwicklung wäre unzulässig. Für die Sicherheitsüberprüfung der Kurzbesucher des HMI sind nur die Daten im ISVB relevant, die Aufschluss über ein mögliches Gefährdungspotenzial, das von dem Besucher ausgeht, geben. Die entsprechende Analyse hat

unter Berücksichtigung sicherheitsbehördlicher Erkenntnisse und Erfahrungen zu erfolgen und kann nur von der Polizei – in keinem Fall von der Senatsverwaltung für Stadtentwicklung – durchgeführt werden. Nur das Ergebnis dieser Analyse und die dafür relevanten Daten dürfen – gestützt auf die vorherige Einwilligung des Betroffenen – an die Senatsverwaltung für Stadtentwicklung übermittelt werden. Die Übermittlung weiterer, anderer Daten aus dem ISVB oder von Daten zu Delikten, aus denen sich kein Gefährdungspotenzial ergibt, ist für die Sicherheitsüberprüfung und somit für die Erfüllung der Aufgaben nicht erforderlich und damit unzulässig.

4.5 Wissen und Bildung

4.5.1 Wissenschaft und Forschung

Medizinische Forschungsnetze – erste Früchte der Mühen

Im Jahresbericht 2002 erläuterten wir die nunmehr abschließend vorgelegten generischen Modelle der Telematikplattform „Medizinische Forschungsnetze“[104]. Nunmehr ergab sich ein großer Beratungsbedarf bei der Erarbeitung einer Datenschutzpolice einschließlich der Formulierung datenschutzrechtlicher Rahmenbedingungen und Muster für Patienteneinwilligungserklärungen bei der Nutzung pseudonymisierter Patientendaten. Diese beiden „Handwerkszeuge“ für den Aufbau medizinischer Forschungsdatennetze wurden einer ausführlichen Prüfung unterzogen.

Die Datenschutzpolice enthält jeweils Musterbeispiele für die Satzung eines eingetragenen Vereins als Träger des Kompetenznetzes, für die Geschäftsordnung des Vorstandes und der Datenschutzkommission, für die Verträge mit den Ärzten, für die Patienteninformation, für die Zertifizierung des Pseudonymisierungsdienstes und der Transportverschlüsselung, für Nutzerordnungen der verschiedenen Dienste, für Nutzungsoptionen von Smart-Cards und das Verfahren bei auftretenden Fehlern oder des Verlustes bzw. der Kompromittierung von geheimen Informationen.

Die erarbeiteten Rahmenbedingungen für die Patienteneinwilligungserklärungen enthalten in Form einer Scheckliste fast 70 Bausteine und die dazugehörigen Fragestellungen, die für das jeweilige Projekt abzuklären sind. Diese zunächst sehr aufwendigen Vorarbeiten haben sich gelohnt. Die von uns zu prüfende Patienteninformation nebst Einwilligungserklärung

[104] JB 2002, 4.5.1

zum Kompetenznetz „Herzinsuffizienz“, die sich an diesem Rahmen orientiert hatte, wies eine hohe Qualität auf.

Ausgehend von den erarbeiteten generischen Modellen wurde uns auch das Pflichtenheft zur Erstellung eines Pseudonymisierungsdienstes zur datenschutzrechtlichen Prüfung vorgelegt. Hier ist der Ansatz ebenfalls modular, so dass die aufzubauenden Pseudonymisierungsdienste entsprechend den spezifischen Anforderungen der Kompetenznetze gestaltet werden können.

Unter den durch unsere Behörde zu betreuenden Forschungs- und Behandlungsregistern[105] erhielt das Kompetenznetz „Angeborene Hörfehler“ mit seinem zentralen Patientenregister Mitte 2003 die Förderung durch das Bundesministerium für Bildung und Forschung bewilligt. Als Träger des Registers wurde zwischenzeitlich auch ein Verein gegründet. Die Gründung der Vereine ist datenschutzrechtlich wichtig, da nur so auch bei reduzierter oder ausbleibender Förderung durch Bundesmittel die Kontinuität der Rahmenbedingungen für die Speicherung von Patientendaten gesichert werden kann. Es wird damit vermieden, dass bei Beendigung von Forschungsvorhaben oder ausbleibender Förderung Patientendaten faktisch herrenlos werden.

Neukonzeption der Qualitätssicherung in der Nierenersatztherapie (QuaSi-Niere)

Im vergangenen Jahr diskutierten wir mit den Vertretern von QuaSi-Niere gGmbH, dem Bundes- und den Landesbeauftragten für den Datenschutz als auch Vertretern des Bundesausschusses der Ärzte und der Krankenkassen, Fragen einer Neukonzeptionierung der Qualitätssicherung in der Nierenersatztherapie. Ausgangspunkt hierfür ist die Neuordnung der Versorgung chronisch niereninsuffizienter Patienten, die auch ein regelmäßig standardisiertes Qualitätsmonitoring nach § 136 a SGB V einschließen soll. Beim Projekt QuaSi-Niere ist seit 1994 die Beteiligung sowohl der Patienten als auch der Behandlungseinrichtungen freiwillig. Es beteiligen sich derzeit von den über 1100 Behandlungseinrichtungen etwa 90 % und von den über 60.000 Patienten in der Nierenersatztherapie etwa 60 %. Nunmehr sollen aufgrund einer Richtlinie des Bundesausschusses der Ärzte und Krankenkassen alle Behandlungseinrichtungen verpflichtet werden, sich an der Qualitätssicherungsmaßnahme zu beteiligen. Die Rechtsgrundlage dafür ist die Verpflichtung nach dem Gesundheitsmodernisierungsgesetz. Eine flächendeckende Qualitätssicherung ist nur mit den medizinischen Daten aller Patienten möglich. Inwieweit bei einer verpflichtenden Teilnahme der Behandlungs-

[105] JB 2002, 4.5.1

einrichtungen auch eine verpflichtende Teilnahme der Patienten geregelt werden kann, wird gegenwärtig diskutiert.

Übereinstimmung besteht jetzt darin, dass Patienten- und Einrichtungsdaten nur pseudonymisiert nach wissenschaftlichen Kriterien für die Qualitätssicherung analysiert werden dürfen und ein Datentreuhänder Klarnamen und Pseudonyme gegen unberechtigte Zugriffe sichert.

Das Gesamtkonzept soll so verfasst werden, dass es den Anforderungen zur Datentransparenz des Gesundheitsmodernisierungsgesetzes (§§ 303 a bis f und § 304 GMG) voll entspricht. Dies gilt auch für die Integration der QuaSi-Niere Patientenchipkarte in das Gesamtprojekt der Elektronischen Gesundheitskarte nach § 291a GMG[106].

Datenschutzgerechte Forschung

Es hat schon Tradition, in den Jahresberichten eine Auswahl von Forschungsprojekten kurz vorzustellen, 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 u. a.:

- Drogenabhängige für eine Evaluation der Substitutionsbehandlung, insbesondere der Suche nach Modellen „guter Praxis“,
- Schüler der Klassenstufe sieben bis zehn zum Thema „Alkohol und Schule“,
- Schüler und Lehrer über die Wirksamkeit von Schulstationen,
- Viertklässler russlanddeutscher Herkunft hinsichtlich der Mehrsprachigkeit und des Leseverständnisses,
- Opfer und Täter häuslicher Gewalt zur Evaluation des Gewaltschutzgesetzes,
- Berliner Haus- und Kinderärzte zu Kompetenzen in der Prävention und bei der Versorgung von Kindern mit Gewalterfahrungen,
- deutsche und türkische Jugendliche sowie deren Eltern zu einem Vergleich der Kultur der Erziehung,
- im Justizvollzug befindliche Frauen zur Funktion und Praxis der Sozialtherapie,
- Schüler zu ihrem Wissen und ihrer Meinung über Homosexualität,
- Schüler, ob sportvereinsgebundene Jugendliche seltener straffällig werden,

[106] vgl. 4.4.2

- Mieter in Sanierungsgebieten zwecks Fortschreibung der Mietobergrenzen,
- Aussiedler zur Wirksamkeit von Integrationsverträgen.

Akteneinsicht nahmen Forscher in

- Auszüge aus dem Bundeszentralregister und dem Erziehungsregister zur Beurteilung von Möglichkeiten präventiver und therapeutischer Strategien zum Zwecke der Verhinderung sexueller Übergriffe,
- Akten NS-belasteter Richter, Staatsanwälte und anderer Justizbediensteter, denen Anfang der 60er Jahre nach § 116 Richtergesetz die Möglichkeit des vorzeitigen Wechsels in den Ruhestand bei voller Aufrechterhaltung ihrer Bezüge gegeben wurde,
- polizeiliche Ermittlungsakten bei der Verfolgung von sexuellem Missbrauch Schutzbefohlener,
- Akten der Rechtsanwaltskammer zur Geschichte der Juristinnen in Deutschland im 20. Jahrhundert.

Darüber hinaus wurden Forscher zu folgenden Themen beraten:

- zur Durchführung der DESI-Hauptuntersuchung (Deutsch-Englisch-Schulleistungsvergleich), bei der es u. a. um die Fragebögen, die Einwilligungserklärung, aber auch die Durchführung einer Videostudie bei ausgewählten Englischlehrkräften ging,
- zur vergleichenden Untersuchung des Lese- und Mathematikverständnisses in den vierten bis sechsten Klassen an Berliner Schulen (Studie ELEMENT),
- zur Entwicklung von Vergleichsarbeiten an Berliner Grundschulen (VERA),
- zur Erfassungsintensität bei meldepflichtigen Krankheiten,
- zur Durchführung einer Videostudie zum Chemieunterricht, die auch als Lehrfilm für Ausbildungszwecke genutzt werden soll,
- zu den Möglichkeiten, aus Daten der Einwohnerregister Informationen für eine Kontaktaufnahme mit Zwillingen zum Zweck eines Forschungsregisters über Zwillinge zu erhalten,
- zur Durchführung einer Gesamterhebung der Schülerpopulation in Schulen für Sprachbehinderte, insbesondere unter dem Aspekt des Gewichts von Schülern nichtdeutscher Herkunftssprache.

Hohe Anforderungen an eine sichere Pseudonymisierung in der pharmakogenetischen Forschung – Schering AG

Besonders hohe Anforderungen an Datenschutzmaßnahmen ergeben sich beim Aufbau von Gendatenbanken, d. h. Sammlungen von Proben und genetischen Daten zu noch unbestimmten, allgemeinen Forschungszwecken. Ausführlich haben wir dazu im Jahresbericht 2001[107] unsere Anforderungen, insbesondere auch an Forschungsregelungen in einem Gentestgesetz, formuliert. Da eben bei solchen Untersuchungen nicht von einer strikten Zweckbindung an ein konkret definiertes Forschungsvorhaben ausgegangen werden kann, sind zum Ausgleich andere Maßnahmen, insbesondere auch die sichere Pseudonymisierung, umzusetzen. Die Schering AG möchte zur Durchführung pharmakogenetischer Studien Daten aus Blut- oder Gewebeproben mit den im Rahmen der klinischen Studien gewonnenen medizinischen Daten zusammenführen und abgleichen. Das Projekt „GENOMatch“ beinhaltet den Aufbau einer pharmakogenetischen Biobank (Probensammlung) sowie die Generierung und sichere Speicherung von pseudonymisierten, genetischen und klinischen Daten und die statistische Analyse der Daten durch eine Zusammenführung („Data-Matching“). Für die datenschutzkonforme Sammlung von Blut- und Gewebeproben beauftragte die Schering AG das Institut für Informatik und praktische Mathematik der Christian-Albrecht-Universität zu Kiel damit, ein sicheres Pseudonymisierungsprojekt zu erarbeiten. Für das Projekt wurde vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein nach § 43 Abs. 2 Landesdatenschutzgesetz Schleswig-Holstein ein Gütesiegel erteilt. Gegenwärtig wird vom betrieblichen Datenschutzbeauftragten der Schering AG die Vorabkontrolle des Verfahrens vorbereitet.

Pseudonymisierung in der pharmakologischen Forschung

Im Jahresbericht 2002[108] stellten wir fest, dass von einer Umsetzung des Gebots der Anonymisierung und Pseudonymisierung nach § 3 a BDSG bei der pharmakologischen Forschung und den vom Arzneimittelgesetz vorgeschriebenen Tests nicht auszugehen ist, wenn medizinische Probandendaten unter Nutzung der Namensinitialen, des vollständigen Geburtsdatums und des Geschlechts gespeichert und an die forschenden Pharmaunternehmen übermittelt werden. Der Arbeitskreis Wissenschaft der Datenschutzbeauftragten ist einvernehmlich der Auffassung, dass zumindest bei der Übermittlung von den Prüfärzten an die forschenden Pharmaunternehmen auf den Geburtstag und den Geburtsmonat zu verzichten ist.

[107] JB 2001, 3.2
[108] JB 2002, 4.5.1

Im forschenden Unternehmen sollte dann ein echtes Pseudonym vergeben werden. Im August 2003 einigten sich die Berliner Medizinischen Ethikkommissionen darüber, bei Studien das vollständige Geburtsdatum auf das Geburtsjahr zu verkürzen und statt der Namensinitialen eine Codenummer oder Dummyinitialen zu verwenden. Diesen Vorschlag, ergänzt um Forderungen nach Verbesserung der Transparenz der Datenschutz- und Einwilligungserklärungen, brachten sie auf die Tagesordnung der Jahrestagung des Arbeitskreises Medizinischer Ethikkommissionen in der Bundesrepublik Deutschland. Ein Votum liegt hierzu noch nicht vor.

4.5.2 Statistik

Forschungsdatenzentren

Vor zwei Jahren informierten wir über die Vorschläge der „Kommission zur Verbesserung der informationellen Infrastruktur zwischen Wissenschaft und Statistik“. Dort wurde die Empfehlung gegeben, in den Statistischen Ämtern, aber auch bei der Bundesanstalt für Arbeit so genannte Forschungsdatenzentren einzurichten. Im Statistischen Bundesamt und in der Bundesanstalt für Arbeit ist dies bereits geschehen. Dort haben Wissenschaftler die Möglichkeit, faktisch anonymisierte Einzeldaten in kontrollierter Umgebung für ihre Berechnungen selbst zu nutzen oder die Berechnungen durchführen zu lassen. Die Statistiker überwachen diese Arbeiten und prüfen insbesondere die Ergebnisse auf die Einhaltung der statistischen Geheimhaltung.

Auch die statistischen Landesämter wollten auf diesem Weg ihre Daten für die Wissenschaft besser nutzbar machen. Dabei sollte sich jedes statistische Landesamt auf bestimmte Statistiken spezialisieren und die Einzeldatensätze der anderen Landesämter in deren Auftrag übernehmen sowie diese zusammenführen. Das spezialisierte Landesamt (Serveramt) sollte dann auch die Daten für die Forscher bereitstellen und die Ergebnisse sowie die Arbeiten selbst auf die Einhaltung der statistischen Geheimhaltung prüfen.

Diese Arbeiten können jedoch nicht als Auftragsdatenverarbeitung gefasst werden, da das jeweilige Landesamt inhaltlich selbstständig tätig wird. In den Arbeitskreisen Wissenschaft und Statistik der Datenschutzbeauftragten von Bund und Ländern wurden die rechtlichen Möglichkeiten intensiv diskutiert. Übereinstimmung bestand darin, dass der beste Weg, diesen Datenaustausch zu legitimieren, eine explizite Befugnisnorm im Bundesstatistikgesetz wäre. Gleichwohl vertreten wir die Auffassung, dass die Softwareinstrumente der Forschungsdatenzentren im Vorgriff auf eine rechtliche Legitimierung geschaffen, erprobt und

auch schon genutzt werden können. Dabei sollten die Daten beim Serveramt bis zum Eingang konkreter Anfragen verschlüsselt gespeichert werden und die Möglichkeit, Zusatzwissen zuzuspielen, für die Nutzer ausgeschlossen sein. Auch ist es möglich, dass die übermittelten Einzeldaten vor der Übermittlung eine weitere Stufe der Anonymisierung durchlaufen, z. B. durch Vergröberung der Schlüssel und regionalen Zuordnungen. Leider konnte auf der Konferenz der Datenschutzbeauftragten von Bund und Ländern im Herbst des Berichtsjahres kein Konsens erzielt werden.

Personalstrukturstatistik des unmittelbaren Landesdienstes

Mit Hochdruck wurde im vergangenen Jahr am Gesetzentwurf für ein Landesstatistikgesetz über die Personalstruktur in der Senatsverwaltung für Finanzen gearbeitet[109] Parallel dazu wurde im Frühsommer durch Dienstanweisung des Senators eine organisatorisch, personell und räumlich abgeschottete Statistikstelle geschaffen. Leider konnte dieser Statistikstelle erst zum Jahresende ein Fachstatistiker zugeordnet werden, so dass sich die von uns als grundlegend für die Arbeit einer Statistikstelle außerhalb eines abgeschotteten statistischen Amtes geforderten Arbeiten zur Sicherung der statistischen Geheimhaltung verzögerten. Auch die Aufbereitung von Altdaten für den Personalstandsbericht 2002 konnte somit nicht begonnen werden.

Der Gesetzentwurf selbst wurde mehrfach überarbeitet. So soll nun neben der Personalstandsstatistik auch eine Versorgungs- und eine Beihilfestatistik geführt werden. Dabei wurde der vom Hauptpersonalrat und von uns vorgebrachten Forderung einer strikten technischen und organisatorischen Trennung dieser drei Statistiken sowohl im vorliegenden Gesetzentwurf als auch bei den vorbereitenden Arbeiten am künftigen IT-Verfahren PuSta entsprochen.

4.5.3 Schule

Mehr Datenschutz im neuen Schulgesetz

Unter dieser Überschrift erläuterten wir im Jahresbericht 2002[110] die datenschutzrechtlichen Ergänzungen und Neuerungen. Zunächst noch offene Probleme wie die Ausdehnung der

[109] JB 2002, 4.5.3
[110] JB 2002, 4.5.2

Datenschutzregelungen auch auf die Privatschulen und die Aufgaben des Schulpsychologischen Dienstes sind einvernehmlich mit der Senatsverwaltung für Bildung, Jugend und Sport geklärt und in den Gesetzentwurf aufgenommen worden.

Schule nunmehr auch rechtssicherer im Internet

Die Nutzung des Internets in der Berliner Schule ist mittlerweile zum Normalfall geworden. Die Ausstattung der Schulen hat sich erheblich verbessert. Gleichwohl tauchen immer Fragen auf sowohl zur Nutzung des Internets für Unterrichtszwecke, zum Aufbau von eigenen Angeboten und Veröffentlichungen der Berliner Schulen sowie zu den Möglichkeiten, über den Rahmen des Unterrichts hinaus auch in der Freizeit den Schülern Nutzungen anzubieten. Die Senatsverwaltung für Bildung, Jugend und Sport hat daher unsere Hinweise aus den Jahresberichten 1999, 2000 und 2001[111] aufgegriffen und angekündigt, unter Nutzung der rechtlichen Hinweise, die im Auftrag der Kultusministerkonferenz erarbeitet wurden, ein Rundschreiben zur Regelung der rechtssicheren Nutzung des Internets zu erlassen. Dies dürfte die Rechtssicherheit an den Schulen erheblich verbessern, insbesondere da neben der Erörterung der rechtlichen Probleme auch der Entwurf einer Musternutzerordnung beigefügt wurde.

Das Gegenteil von gut ist gut gemeint – das Ende der Lernmittelfreiheit

Im April 2003 erfuhren wir von der Senatsverwaltung für Bildung, Jugend und Sport von der Absicht, durch Änderung des Schulgesetzes die Lernmittelfreiheit abzuschaffen und eine finanzielle Selbstbeteiligung der Erziehungsberechtigten vorzuschreiben.

Kurz vor Erlass des § 18 a des Schulgesetzes für Berlin entnahmen wir der Presse, dass die Empfänger von Sozialhilfe, Wohngeld oder BAföG sowie Asylbewerber, die staatliche Zuwendungen erhalten, vom Eigenanteil befreit werden sollten. Die Eltern sollen dies durch den entsprechenden amtlichen Bescheid nachweisen. Der Bescheid sollte der Schulleitung vorgelegt werden. Dadurch waren die Schülerinnen und Schüler gezwungen, der Schule gegenüber die Bedürftigkeit ihrer Eltern nachzuweisen. Diese Prangerwirkung löste landesweit eine heftige Diskussion aus.

[111] jeweils 4.5.2

Anfang Juni, d. h. noch vor Erlass der Lernmittelverordnung, erhielten wir erste Hinweise und Eingaben von betroffenen Eltern in der Angelegenheit; insbesondere wurde auf ein Rundschreiben der Senatsverwaltung für Bildung, Jugend und Sport vom Mai 2003 verwiesen. Dieses Rundschreiben war uns von der Senatsverwaltung vorab nicht zur Kenntnis gegeben worden. Das Rundschreiben selbst stellte nur eine Art „Vorinformationen der Schule“ dar, da weder eine Änderung des Schulgesetzes bis zu diesem Datum erfolgt noch die vorgesehene Rechtsverordnung zur Schulgesetzänderung in Kraft getreten war.

Aus den Eingaben und Anfragen entnahmen wir, dass dieses Rundschreiben zu einer erheblichen Verwirrung an den Schulen geführt hatte. So seien insbesondere an einigen Grundschulen die Nachweise offen über die Lehrer an die Schulleitung weitergeleitet und erst nach mehreren Tagen zurückgegeben worden. Um dieser unhaltbaren Situation ein Ende zu setzen, nahmen wir Ende Mai, also unmittelbar nach den ersten Pressemeldungen, mit der Senatsverwaltung für Schule, Jugend uns Sport Kontakt auf, die zusicherte, dass der Entwurf der Lernmittelverordnung uns rechtzeitig vorgelegt wird. Wir regten zur Entschärfung der Situation an den Schulen an, diesen einen Vordruck zum Kopieren zukommen zu lassen, der das Vorlegen der Originalbescheide erübrigt hätte. Dieser Vorschlag eines Vordrucks sollte lediglich die vier Kategorien von gesetzlichen Unterstützungsleistungen enthalten, deren Richtigkeit durch das betreffende Leistungsamt durch Stempel und Unterschrift zu quittieren wäre. Leider wurde dieser Vorschlag nicht aufgegriffen, wovon wir allerdings erst Mitte Juni Kenntnis erhielten. Zwischenzeitlich teilten wir den Schulen auf Anfrage mit, dass ein die Bearbeitung vereinfachendes Formular per Rundschreiben an die Schulen gesendet werden sollte.

Nachdem sich auch der Unterausschuss „Datenschutz und Informationsfreiheit“ des Abgeordnetenhauses mit dem Verfahren befasst hatte, erhielten wir von der Senatsverwaltung einen überarbeiteten Entwurf der Lernmittelverordnung. In dem Entwurf wurde zwar geregelt, dass Nachweise vorzulegen sind und lediglich die Schulleitung oder eine von ihr zu bestimmende Person diese zur Kenntnis nehmen darf. Hinreichende Klarheit über das Verfahren war damit jedoch nicht gegeben.

Kurz nach Beginn der Sommerferien berieten wir die Angelegenheit nochmals mit der Senatsverwaltung. Dabei wurde festgestellt, dass für die laufende Lernmittelbeschaffung kaum noch ein geregeltes Verfahren durchsetzbar sei, jedoch eine grundsätzliche Lösung für das Schuljahr 2004/2005 gefunden werden muss. Dazu wurde ein Gutscheinverfahren skizziert, das weder die Art der Sozialleistung noch das die Sozialleistung gewährende Amt erkennbar werden lässt. Die Lernmittelverordnung war zu diesem Zeitpunkt bereits erlassen worden.

Mit einem Ende Juli erlassenen Rundschreiben hob die Senatsverwaltung das datenschutzrechtlich unzulängliche Rundschreiben vom Mai 2003 auf.

Für die Zukunft haben wir folgendes Verfahren vorgeschlagen: Die leistungsgewährenden Stellen erhalten lediglich einen nummerierten Vordruck als Durchschreibesatz. Die Ämter geben das Original und die erste Durchschrift an die betroffenen Bedürftigen aus. Die zweite Durchschrift verbleibt beim die entsprechende Sozialleistung gewährenden Amt. In das Formular wird lediglich der Name des Kindes und die Unterschrift des ausgebenden Mitarbeiters eingesetzt. Eine Kennzeichnung des Amtes auch durch Stempel erfolgt nicht. Die betroffenen Eltern übergeben das Original des Vordrucks an die zu bestimmenden Personen in der Schule und behalten die erste Durchschrift. Die Schulen verwahren dann für das laufende Schuljahr die „Gutscheinbögen“ und können damit den Anschaffungsbedarf planen. Durch die Nummerierung der Bögen ist auch eine Kontrollmöglichkeit über die Senatsverwaltung gegeben.

4.6 Wirtschaft

4.6.1 Banken

Due-Diligence-Verfahren bei der Bankgesellschaft Berlin

> *Das Land Berlin beabsichtigte, das Aktienpaket an der Bankgesellschaft Berlin an einen Investor zu verkaufen. Da Großinvestoren nicht bereit sind, „die Katze im Sack“ zu kaufen, muss ihnen während des Bieterverfahrens Gelegenheit gegeben werden, sich über die finanzielle Situation des potenziellen Kaufobjekts zu informieren (Due-Diligence-Verfahren). Von besonderer Bedeutung war bei dem Verkauf der Bankgesellschaft das Kreditportefeuille insbesondere der Berlin Hyp.*

Während des Due-Diligence-Verfahrens werden die für den Investor entscheidungserheblichen Unterlagen in einen so genannten „Grünen Raum“ und einen „Roten Raum“ gebracht. Die Akten des „Roten Raumes“ enthalten personenbezogene Daten. Zu diesem Raum haben nur unter einer besonderen Schweigepflicht stehende Wirtschaftsprüfer Zutritt. Die Akten des „Grünen Raumes“ sollen demgegenüber keine personenbezogenen Daten enthalten. Akten aus dem „Roten Raum“ dürfen erst nach einer Anonymisierung aller personenbezogenen Daten in den „Grünen Raum“ transferiert werden. Zu den Akten des „Grünen Raumes“ haben die Kaufinteressenten der Bankgesellschaft Berlin direkt Zugang.

Ein amerikanischer Interessent forderte von der Bankgesellschaft Berlin Einsicht in Akten aus dem „Roten Raum“. Es handelte sich dabei um personenbezogene Daten von Kunden der Berlin Hyp, der Investor wollte zu allen großen Grundstücksengagements der Bank die Kreditunterlagen einsehen. Der Name des Investors müsse nicht mitgeteilt werden, wohl aber die Adresse des Objektes. Außerdem sollten die Mietkonditionen der einzelnen Objekte offen gelegt werden. Eine Einwilligung der Betroffenen lag nicht vor. Die Bankgesellschaft Berlin bat uns um Auskunft, ob Bedenken gegen die von dem Investor geforderte Datenübermittlung bestehen würden.

Es erscheint zweifelhaft, ob die Bankgesellschaft als verantwortliche Stelle ein berechtigtes Interesse an der Offenbarung nach § 28 Abs. 1 Nr. 2 BDSG hat, ebenso ob der Investor die angeforderten Daten zur Wahrung berechtigter Interessen benötigt (§ 28 Abs. 3 Nr. 1 BDSG). Berechtigte Interessen werden definiert als ein nach vernünftiger Erwägung durch die Sachlage gerechtfertigtes, also ein tatsächliches Interesse, das wirtschaftlicher oder ideeller Natur sein kann. Ein berechtigtes Interesse des Investors wäre nur dann gegeben, wenn dieser ohne die angeforderten Daten keine abgewogene Entscheidung über den Kauf des Aktienpakets treffen könnte. Dies ist allerdings nicht der Fall, da die Möglichkeit bestünde, sich aggregierte und anonymisierte Daten zu beschaffen und ein Wirtschaftsprüfungsunternehmen zu beauftragen, die einzelnen Kreditengagements nach den jeweiligen Vorgaben des Investors zu analysieren und betriebswirtschaftlich zu bewerten. Ein berechtigtes Interesse kann auch dann nicht angenommen werden, wenn die Übermittlung der Informationen gegen Vorgaben des Aktiengesetzes, insbesondere gegen § 53 a Aktiengesetz (AktienG), verstoßen würde. Hier ist zweifelhaft, ob die detaillierte Information des Investors nicht gegen den in § 53 a AktienG konstituierten Gleichbehandlungsgrundsatz verstoßen würde.

Es konnte offen bleiben, ob berechtigte Interessen des Investors oder der Bankgesellschaft Berlin gegeben waren, da das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Datenübermittlung überwogen. Die Kreditnehmer der Bankgesellschaft Berlin, die das Bankgeheimnis beachten muss, müssen nicht damit rechnen, dass Einzelheiten ihres Kreditengagements an Kaufinteressenten übermittelt werden, zumal der Kaufinteressent selbst im Grundstücksgeschäft aktiv ist und nicht ausgeschlossen werden kann, dass der Betroffene möglicherweise bei anderen Projekten gerade mit diesem Investor in Verhandlungen tritt, ohne ihm Einzelheiten des Engagements bei der Bankgesellschaft Berlin mitteilen zu wollen. Der Kunde der Bankgesellschaft Berlin muss nur damit rechnen, dass Wirtschaftsprüfungsgesellschaften im Rahmen von Due-Diligence-Analysen einzelne Kreditengagements bewer-

ten. Die von dem Investor und dem Verkäufer des Aktienpakets gewünschte Datenübermittlung war rechtswidrig. Die Bankgesellschaft Berlin entsprach unseren Vorgaben.

Bei der Stichprobenkontrolle des „Grünen Raumes“ wurden - allerdings in geringem Umfang – Mängel der Anonymisierung festgestellt: Die Namen von Mitarbeitern der Bankgesellschaft Berlin wurden nicht geschwärzt. Es bestand keine Erforderlichkeit dafür, dass den Kaufinteressenten die Namen von Mitarbeitern, die nicht zum höheren Management gehören, wie Devisenhändler oder Kreditsachbearbeiter, mitgeteilt werden.

Bei der Aufstellung der Mieteinkünfte von Objekten, die im Eigentum der Bank stehen, wurden mindestens in zwei Fällen Mieternamen von Privatpersonen nicht geschwärzt. Bei diesen Mietern konnten die Adresse, die Quadratmeterzahl der gemieteten Wohnung, der Mietzins und die Mietvertragslaufzeit den Unterlagen entnommen werden.

Bei dem Verzeichnis der Großkreditkunden waren zwar der Name sowie die Hypothekendarlehen des belasteten Objekts „geschwärzt“, lesbar waren aber die Kontonummer, die Kreditnehmernummer sowie die Kundennummer. Zwar wird man annehmen können, dass man nur mit krimineller Energie mit Hilfe dieser Daten eine Personenbeziehbarkeit herstellen kann. Allerdings kann bei Großkreditkunden nicht ausgeschlossen werden, dass diese auch zu den Kaufinteressenten in Geschäftsbeziehung stehen und deshalb dem Kaufinteressenten die Bankverbindung des Kreditnehmers, die ein Unternehmen in normaler Geschäftspost mitteilt, bekannt ist. Die ungekürzte Übermittlung der drei Nummern, insbesondere aber der Kontonummer, hätte unterbleiben müssen.

Kundenbetreuungsprogramm

> *Die Berliner Bank und die Berliner Sparkasse haben insbesondere für die Betreuung vermögender Privatkunden ein Kundenbetreuungsprogramm (KBP) installiert, durch welches die Beratungsleistung der Kundenbetreuer erhöht werden soll. Außerdem sollen diesen Kunden möglichst maßgeschneiderte Angebote unterbreitet werden können. Zu jeder der betroffenen Personen wird im Rahmen des KBP ein umfangreicher Datensatz angelegt.*

Um eine gute Gesprächsatmosphäre mit dem Kunden sicherzustellen, sollten die Kundenberater Daten zu Ess- und Trinkgewohnheiten (Kaffee oder Tee) speichern; außerdem sollten Informationen zu möglichen einleitenden Gesprächsthemen wie Hobbys des Kunden (Golf,

Segeln etc.) festgehalten werden. Da die Speicherung derartiger Daten sich nicht im Rahmen der Zweckbestimmung des Vertragsverhältnisses mit dem Betroffenen bewegt, haben wir die beiden Banken aufgefordert, diesen Datensatz nicht mehr zu verwenden. Daraufhin wurden die Daten gesperrt.

In das Kundenbetreuungsprogramm werden auch Daten eingespeist, die nach dem Kreditwesengesetz oder nach Regelungen zur Zinsabschlagsteuer erhoben und gespeichert wurden. Während das Wertpapierhandelsgesetz einen gesetzlichen Rahmen zur Kundenbetreuung schafft, ist die Einspeisung von Daten, die ein Kunde nicht zur Verbesserung seiner Betreuung, sondern ausschließlich in Erfüllung gesetzlicher Vorgaben preisgegeben hat, rechtswidrig. Grundsätzlich muss ein Kunde nicht damit rechnen, dass die Daten, die aufgrund von gesetzlichen Vorgaben gespeichert werden, zur Kundenbetreuung verwendet werden. So sind Daten zu Freistellungsaufträgen, denen auch entnommen werden kann, dass der Kunde einem Wettbewerber Freistellungsaufträge erteilt hat, nicht für die Kundenberatung zu verwenden.

Der für die Mitarbeiter erstellte KBP-Leitfaden enthält den Hinweis, dass alle Personen, die zum Kundenhaushalt gehören, in einen Familienverbund aufzunehmen sind. Alle Kinder von Kunden werden generell als Interessenten angelegt. Sofern Ehepartner nach gesetzlichen Vorgaben (wie z. B. bei der Zinsabschlagsteuer) gemeinsam zu werten sind, bestehen gegen die Speicherung von Verbünden keine Bedenken, diese müssen sich allerdings im Rahmen der Zweckbestimmung der gesetzlichen Vorgabe bewegen. Soweit Volljährige ansonsten in ein „Datenverband“ aufgenommen werden, kann diese Verknüpfung nur mit Einwilligung *aller* Verbundteilnehmer erfolgen. Bei Jugendlichen ist die Einwilligung der Erziehungsberechtigten einzuholen. Wir haben beide Banken darauf hingewiesen, dass etwa eine Ehefrau nicht ohne ihr Einverständnis im Datenverbund ihres Mannes geführt werden darf; auch sollten Eltern die Einwilligung dazu geben, dass ihr Kind, welches möglicherweise gar kein Konto besitzt, im Datenverbund ihrer Bank geführt wird.

Wir haben beide Banken aufgefordert, ihr Kundenbetreuungssystem noch einmal zu überprüfen. Sichergestellt werden sollte dabei auch, dass ein Löschungskonzept vorhanden ist, das gewährleistet, dass Daten gelöscht werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist (§ 35 Abs. 2 Satz 2 Nr. 3 BDSG).

4.6.2 Verkehrsunternehmen

Nächtliche Ausweiskontrollen

Die Hilfsorganisation Pro Asyl e. V. bat zu prüfen, ob es zulässig ist, dass die Zugbegleiter in den Nachtzügen der DB AutoZug GmbH auf Verbindungen, bei denen Kontrollen durch die Grenzbehörden zu erwarten sind, die Pässe und Ausweisdokumente der Reisenden entgegennehmen und zur späteren Vorlage an den Bundesgrenzschutz in den Dienstabteilen verwahren.

Der Bundesgrenzschutz (BGS) führt im Rahmen des Schengener Durchführungsübereinkommens bei innereuropäischen Grenzübertritten „lageabhängige Kontrollen“ durch. Nach § 23 Abs. 1 Nr. 2 BGSG ist er berechtigt, personenbezogene Daten zur Identitätsfeststellung der Betroffenen zu erheben. Dabei handelt es sich um eine hoheitliche Maßnahme des BGS. Eine Beleihung der DB AG zur Vornahme dieser hoheitlichen Maßnahme ist nicht gegeben. Die Erhebung der personenbezogenen Ausweisdaten durch die DB AG kann somit nicht auf die Bestimmungen des BGSG gestützt werden.

Die Ausweise werden nach Angaben der DB AG eingesammelt und dem BGS zur Kontrolle übergeben, um den Fahrgästen eine ungestörte Nachtruhe zu ermöglichen. Auch wenn unterstellt werden kann, dass diese Serviceleistung im weitesten Sinne den Geschäftsinteressen und -zwecken der DB AG dient, ist dies für die damit verbundene Datenerhebung von Ausweisdaten der Fahrgäste selbst nicht der Fall. Damit scheidet § 28 BDSG als Rechtsgrundlage für die Datenverarbeitung aus.

Eine (eventuell durch Herausgabe der Pässe konkludente) Einwilligung der Betroffenen in die Datenerhebung liegt ebenfalls nicht vor. Eine Einwilligung muss auf einer freien Entscheidung des Betroffenen beruhen. Das setzt voraus, dass der Betroffene ausreichende Kenntnis über Art, Zweck und Umfang des Umgangs mit seinen Daten hat. Ihm muss bewusst sein, dass er sich anders entscheiden kann.

Pro Asyl e. V. erklärte dazu, dass das Auftreten und Verhalten der uniformierten Zugbegleiter beim Einsammeln der Dokumente für die Reisenden eine Pflicht zur Vorlage der Papiere implizieren würde. Insbesondere für nicht deutsch sprechende Reisende sei – wenn die Dokumente zusammen mit den Fahrkarten herausverlangt würden – nicht zu erkennen, dass es sich um einen freiwilligen „Service“ der DB AG handeln würde.

Wir haben empfohlen, die Betroffenen über ihre Rechte und Pflichten und über den Umstand aufzuklären, dass es sich bei dem Verfahren lediglich um eine Servicedienstleistung der DB AG handelt. Die Aufklärung kann z. B. durch Hinweisblätter vorgenommen werden. Die DB AG hat erklärt, dass unsere Empfehlungen zukünftig berücksichtigt werden.

Bonitätsprüfung bei der Mitnahme von Fahrrädern

Ein Bürger wollte über die Fahrrad-Hotline der DB AG eine telefonische Reservierung von Platzkarten zur Mitnahme von Fahrrädern vornehmen. Obwohl es sich um einen kostenlosen Service der DB AG handelt, habe die Mitarbeiterin der Hotline darauf bestanden, dass er seine Bankverbindung mitteilt. Zur Begründung sei darauf verwiesen worden, dass das verwendete Computersystem zur Vergabe einer Auftragsnummer zwingend die Eingabe der Kontonummer verlange. Nachdem die Abholung der Platzkarten am Automaten – trotz Eingabe der Auftragsnummer – gescheitert sei, sei ihm von der DB AG mitgeteilt worden, dass eine Reservierung nicht möglich sei, da der DB AG ein so genannter „Negativbrief" seines Kreditinstitutes vorliege.

Die DB AG hat dazu erklärt, dass den Kunden mit dem neuen Vertriebssystem die Möglichkeit gegeben werde, die von ihnen telefonisch gebuchten Leistungen auch am Ticket-Automaten abzuholen. Voraussetzung für eine Abholung der Fahrscheinunterlagen am Automaten sei die Zahlung der bestellten Leistungen. Diese könne per Kreditkarte oder per Lastschrift erfolgen. Voraussetzung einer Zahlung sei jedoch eine erfolgreiche Prüfung der Angaben des Kunden. Zu diesem Zweck werde eine „Bonitätsprüfung" bei der Firma InFoScore Consumer Data GmbH durchgeführt. In keinem Fall erhalte die DB AG im Rahmen der Bonitätsprüfung „Negativbriefe" der Kreditinstitute. Es liege lediglich die Information vor, dass die Bonitätsprüfung durch die Firma InFoScore Consumer Data GmbH negativ verlaufen sei. Die Gründe für die Ablehnung seien nur der Firma InFoScore Consumer Data GmbH bekannt und könnten dort nur durch den Kunden selbst erfragt werden. Die Bediensteten seien angewiesen worden, vor der Durchführung der Bonitätsprüfung den Kunden auf diese Umstände hinzuweisen.

Des Weiteren teilte die DB AG dazu mit, dass derartige Bonitätsprüfungen in der Vergangenheit bei der Erbringung aller Leistungen vorgenommen worden seien. Seit Anfang September 2003 könnten die Zahlungen bei kostenlosen Leistungen für die Buchungen im Computersystem simuliert werden. In diesen Fällen werde seitdem auf eine Bonitätsprüfung und die Erfassung von Zahlungsdaten verzichtet.

4.6.3 Detekteien und Auskunfteien

Organisationsmangel in einer Detektei

Eine Bürgerin machte gegenüber ihrer Reiserücktrittsversicherung geltend, dass der Versicherungsfall eingetreten sei, da sie aufgrund gesundheitlicher Probleme die geplante Reise (Wert: 20.000 €) nicht antreten konnte. Anstatt den geforderten Geldbetrag zu begleichen, beauftragte die Versicherung eine Detektei, die Umstände der Reise sowie das wirtschaftliche Umfeld der Betroffenen zu überprüfen. Die Ermittlungen der Auskunftei ergaben, dass sich die Versicherungsnehmerin eine derartig teure Reise nicht leisten konnte. Auch die Umstände der Reise, etwa dass sie mit dem ihr kaum bekannten Inhaber des Reisebüros verreisen wollte, deuteten darauf hin, dass die Versicherungsnehmerin beim Abschluss der Reiserücktrittsversicherung einen Betrug begehen wollte. Nach Erhalt des Ermittlungsergebnisses durch die Detektei hat die Versicherung die Auszahlung der Versicherungssumme verweigert und eine Strafanzeige erstattet.

Gegen die Beauftragung einer Detektei beim Verdacht des Versicherungsbetrugs bestehen keine datenschutzrechtlichen Bedenken. Allerdings enthält der Ermittlungsbericht der Detektei Informationen, bei denen man davon ausgehen muss, dass diese nicht auf rechtmäßige Weise erhoben wurden. So war der Detektei bekannt, dass die Versicherungsnehmerin in ihrer Zeit als Arbeitslose Probleme mit dem Arbeitsamt gehabt hatte, sie verfügte über Informationen, die offenbar aus dem Datenbestand der BfA stammen; sogar die besonderen Umstände ihres Arztbesuches, der schließlich zu der Erstellung des ärztlichen Attests führte, wurden durch die Detektei ermittelt. In einem Parallelfall, in dem ein Versicherter den Diebstahl eines Schmuckstücks bei einer Reise geltend machte, verfügte die Detektei sogar über genaue Kontodaten des Betroffenen. Der Datenbestand der Detektei enthält keine Informationen darüber, wie die personenbezogenen Daten erhoben wurden.

§ 34 Abs. 1 Nr. 1 BDSG gibt dem Betroffenen zwar einen Anspruch auf Auskunft über die Herkunft der Daten, dieser Anspruch besteht aber nur, wenn die verantwortliche Stelle die Herkunft der Daten gespeichert hat. Auch die Aufsichtsbehörde hat kaum die Möglichkeit, die Herkunft der Daten zu ermitteln, zumal die verantwortliche Stelle sich in der Regel auf ihr Auskunftsverweigerungsrecht nach § 38 Abs. 3 Satz 2 BDSG berufen kann.

Nach einer Entscheidung des Verwaltungsgerichts Hamburg[112] ist die Gefahr, dass einzelne Mitarbeiter in der verantwortlichen Stelle Verstöße gegen Datenschutzbestimmungen begehen, ohne dass diese Verstöße geahndet werden können, als Organisationsmangel nach der Anlage zu § 9 BDSG zu werten. Die innerbetriebliche Organisation sei so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Das Verwaltungsgericht räumt deshalb den Aufsichtsbehörden das Recht ein, 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. Wir haben der Detektei mitgeteilt, dass wir eine Anordnung nach § 38 Abs. 5 Satz 1 BDSG erlassen werden, sofern sie nicht freiwillig den Organisationsmangel behebt.

Durchgeroutete Auskünfte

> *Eine neu eröffnete Auskunftei stellte ihren Mitgliedsunternehmen zwei verschiedene Serviceangebote zur Verfügung, einen Neukundencheck sowie das Monitoring bei länger währender Geschäftsbeziehung. Der Informationsaustausch erfolgte über das Internet. Nach den Informationen des Unternehmens verfügt es für den Neukundencheck über Informationen von über 7 Mio. Personen mit 40 Mio. Negativmerkmalen sowie über fast eine ½ Mio. Unternehmen mit 1 Mio. Negativmerkmalen.*

Unsere Kontrolle ergab, dass die neu gegründete Auskunftei zur Durchführung des Neukundenchecks keine Daten gespeichert hatte, sie war nur selbst Kundin einer größeren Auskunftei und „routete“ die Bonitätsanfragen ihrer Mitglieder zu diesen durch. Die größere Auskunftei ging bei den Anfragen davon aus, dass diese durch die Auskunftei erfolgten, die Mitglieder der Auskunftei dachten, sie würden auf die Datenbank der von ihr beauftragten Auskunftei zugreifen. Da der Betreiber der Datenbank davon ausging, er würde die Daten an eine andere Auskunftei übermitteln, die bei weiterer Übermittlung der Daten das berechtigte Interesse ihrer Mitglieder überprüfen würde, diese aber die Daten nur an ihre Mitglieder durchroutete und sich nicht selbst als verantwortliche Stelle betrachtete, wurde von keiner der beiden beteiligten Auskunfteien das berechtigte Interesse der „Endverbraucher“ überprüft. Hierin ist ein Verstoß gegen § 29 Abs. 2 Nr. 1 a BDSG zu sehen. Danach hat der Dritte, dem Daten (von einer Auskunftei) übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft darzulegen. Da die Übermittlung im automatisierten Abrufverfahren erfolgte, hätten die Kunden die Verpflichtung gehabt, ihr berechtigtes Interesse aufzuzeichnen (vgl. § 29 Abs. 2 Satz 4 BDSG). Die überprüfte Auskunftei hat es versäumt, ihre Kunden entsprechend

[112] Urteil vom 21. November 2002, Az.: 22 VG 2830/99

zu unterrichten. Der Betreiber der Datenbank hat nach Aufklärung des Sachverhalts den Vertrag mit seiner Kundin aufgrund vertragswidrigen Verhaltens gekündigt.

Farbenlehre der Bonität

> *Bei der Bonitätsüberwachung (Monitoring) von Kunden während einer längerfristigen Geschäftsbeziehung, etwa einem größeren Bauvorhaben, melden die Mitglieder, die sich für diesen Kunden interessieren, selbst Daten über einen bestimmten Code ein. Bei der Abfrage zu diesem Kunden erhält das Mitglied den gesamten Datensatz, an der Verfärbung des Bildschirms kann das Mitglied erkennen, ob sein Kunde über gute, noch ausreichende oder schlechte Bonität (grün, gelb, rot) verfügt. Die Auskunftei reichert diese Information mit Daten aus öffentlich zugänglichen Quellen an. Die Geschäftskunden der Mitglieder haben sich mit einer Überprüfung ihrer Bonität durch die Auskunftei einverstanden erklärt.*

Die Informationen, die Auskunfteien über Betroffene speichern, sollen sich auf objektive Daten beziehen, aus denen auf die Zahlungsunwilligkeit bzw. Zahlungsunfähigkeit des Betroffenen geschlossen werden kann. Verschiedene von der Auskunftei verwendete Meldecodes erfüllten diese Voraussetzung nicht. So verleitet das Merkmal „Konkurs soll beantragt sein“ dazu, Gerüchte an die Auskunftei zu übermitteln. Merkmale wie „Kunde behauptet Mängel“ oder „Barzahler, da Bonität unbekannt“ sind ohne jeden Aussagewert und haben deshalb zu unterbleiben. Wir haben die Auskunftei aufgefordert, die Meldecodes völlig neu zu überarbeiten. Die Auskunftei konnte uns keine ausreichende Information darüber geben, nach welchen Parametern das Farbsystem arbeitet, so dass nicht davon ausgegangen werden kann, dass es eine objektive Beurteilung der Bonität des Betroffenen vornehmen kann. Auch hier haben wir die Auskunftei aufgefordert, das Verfahren nachzubessern.

Wir haben weiterhin beanstandet, dass die Auskunftei zwar Informationen aus öffentlich zugänglichen Quellen speichert, eine Vollständigkeit und insbesondere Aktualität der gespeicherten Daten aber nicht garantiert wird, und dass sie bei den Meldungen ihrer Mitglieder nicht feststellen kann, aufgrund welcher Tatsachen und aufgrund welchen Rechtsverhältnisses die Einmeldung erfolgt (Verifizierbarkeit der Einmeldung). Auch sollten die Mitglieder bei der Frage, wann etwas eingemeldet wird, keinen Ermessensspielraum haben, da hierdurch die Objektivität des Kreditinformationssystems leidet.

Die Auskunftei hat zugesagt, ihr Verhalten entsprechend unseren Vorgaben nachzubessern.

4.6.4 Was wir sonst noch geprüft haben ...

Ein überraschendes Angebot

> *Ein Ehepaar hatte in einer Zeitung eine Eigentumswohnung angeboten. Da zur Kontaktaufnahme für Interessenten nur eine Telefonnummer angegeben wurde, nicht jedoch Name und Adresse, waren sie überrascht, von einem Immobilienunternehmen einen Brief zu erhalten, in dem ihnen angeboten wurde, ihre Verkaufsbemühungen professionell zu unterstützen.*

Die Eheleute hatten einem Eintrag in ein elektronisches Telefonverzeichnis (Telefon-CDs) zugestimmt. Diese CDs selbst ermöglichen allerdings nicht die Zuordnung einer Rufnummer zu einer bzw. mehreren bestimmen Personen. Das Immobilienunternehmen verwendete allerdings eine zusätzliche Software, mit deren Hilfe anhand der Rufnummer der Name und die Adresse des Teilnehmers ermittelt werden kann (Inverssuche).

Wer in einer Zeitung eine Anzeige aufgibt und seine Telefonnummer hinterlässt, erklärt damit konkludent sein Einverständnis dafür, mittels Telefon Angebote zu erhalten. Er muss allerdings nicht damit rechnen, dass mittels Inverssuche Adressdaten ermittelt werden.

Sowohl die Auswertung als auch die weitere Nutzung der durch die Software erlangten Adressdaten sind rechtswidrig. Wegen der überwiegenden schutzwürdigen Interessen der Betroffenen kann die Inverssuche nicht auf § 28 Abs. 1 Satz 1 Nr. 3 BDSG gestützt werden. Die auf der Telefon-CD gespeicherten Daten sind zwar öffentlich zugänglich, jedoch nur soweit sie dem Funktionsumfang der CD und der gesetzgeberischen Wertung in § 14 Abs. 4 TDSV entsprechend abrufbar sind. Insbesondere lag keine Einwilligung der betroffenen Teilnehmer in die Inverssuche vor. Diese hatten zwar der Aufnahme ihrer Daten in die Telefon-CD zugestimmt, diese Einwilligung erstreckt sich aber lediglich auf die Aufnahme in ein Verzeichnis, mit dessen Hilfe anhand des Namens die Telefonnummer des Teilnehmers ermittelt werden kann.

Wir haben das Immobilienunternehmen aufgefordert, bei der Kundenakquise zukünftig auf das Hilfsmittel der Inverssuche zu verzichten.

Besucherdatei der Spielbank Berlin

> *Wer das „Große Spiel“ der Spielbank Berlin besuchen möchte, wird in einem Besucherverzeichnis erfasst. Dort werden Name, Anschrift, Geburtsdatum, Personalausweisnummer bzw. Passausweisnummer und das Besuchsdatum nebst Uhrzeit gespeichert. Die Daten werden nach zehn Jahren gelöscht.*

Eine Einwilligung in die Aufnahme der Daten in das Besucherverzeichnis wird von der Spielbank nicht eingeholt. Das Gesetz über die Zulassung öffentlicher Spielbanken in Berlin (Spielbankgesetz – SpBG) sieht zwar die Speicherung von Daten im Besucherverzeichnis vor, verweist aber bezüglich des Datensatzes auf die von der Aufsichtsbehörde zur Regelung des Spielbetriebs der Spielbanken zu erlassene Spielordnung (§ 10 Abs. 1 Satz 1 und Satz 2 Nr. 5 SpBG).

§ 5 der Spielordnung für die Spielbank Berlin vom 20. Dezember 2001 führt die Personalausweisnummer und die Uhrzeit nicht als zu speichernde Daten auf. Auch bei den in der Spielordnung erwähnten Daten ergibt sich die Rechtmäßigkeit der Speicherung nicht aus der Spielordnung. Da sie keine Rechtsvorschrift im Sinne des § 4 Abs. 1 BDSG darstellt, stellt sie keinen Erlaubnistatbestand dar.

Als Rechtsgrundlage für die Besucherdatei kommt somit insbesondere § 28 Abs. 1 Satz 1 Nr. 1 BDSG in Betracht. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient. Nach § 28 Abs. 1 Satz 2 BDSG sind bei der Erhebung personenbezogener Daten die Zwecke, für die die Daten verarbeitet oder genutzt werden, konkret (schriftlich) festzulegen. Die Spielbank hatte auf eine derartige konkrete Festlegung verzichtet, sah sich bisher auch nicht in der Lage, Gründe für die Datenspeicherung zu nennen. Auch blieb unklar, wieso die Daten in dem Besucherverzeichnis zehn Jahre aufbewahrt werden. Nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG sind personenbezogene Daten zu löschen, wenn sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.

Ein sammelwütiges Möbelhaus

Bei der Kontrolle eines Möbelhauses stellten wir fest, dass dieses Unternehmen zu viele Kundendaten speichert und die nicht mehr benötigten Daten zu spät löscht. Das Möbelhaus praktiziert das so genannte „wilde Lastschriftverfahren", bei dem der Kunde seine PIN-Nummer nicht eingeben muss. Die Kassierer des Möbelhauses notieren sich auf einem Zettel Namen, Anschrift und Geburtsdatum des Karteninhabers. Der Zettel wird der jeweiligen Kassenabrechnung beigefügt und mit dieser zusammen aufbewahrt. Nach zwei Jahren werden die Kassenabrechnungen und damit auch die im Zusammenhang mit der ec-Zahlung erhobenen Daten vernichtet.

Nur dann, wenn ein Kunde die Ware nicht sofort mitnimmt, wird ein schriftlicher Kaufvertrag abgeschlossen, also insbesondere dann, wenn sich der Kunde die Ware durch das Möbelhaus liefern lässt. In dem Vertrag sind Name, Anschrift, die gekaufte Ware sowie der Kaufpreis enthalten. Die Verträge werden von dem Möbelhaus dauerhaft gespeichert, eine Vernichtung der Vertragsunterlagen ist nicht vorgesehen.

Das Möbelhaus gibt auch eine eigene Kundenkarte heraus. Bei Käufen von Kundenkarteninhabern werden die gekauften Artikel, das Datum des Kaufs und die Rechnungssumme gespeichert, diese Daten können der jeweiligen Kundenkarte des Betroffenen zugeordnet werden.

Da bei dem wilden Lastschriftverfahren der Gläubiger bis zum Erhalt der Gutschrift in ein Vorleistungsverhältnis zu seinem Schuldner tritt, ist es hinzunehmen, dass die Betreiber derartiger Lastschriftverfahren sich den Namen und die Anschrift ihrer Kunden notieren. Für die Speicherung des Geburtsdatums besteht dagegen keine Notwendigkeit.

Die Speicherfrist von zwei Jahren für die auf dem Zettel erhobenen Daten ist rechtswidrig, da der Zahlungsvorgang in der Regel nach sechs Wochen abgeschlossen ist (§ 35 Abs. 2 Satz 2 Nr. 3 BDSG). Wir haben dem Unternehmen empfohlen, die bei dem ec-Kartenverfahren erhobenen Daten nach drei Monaten zu vernichten, sofern die Gutschrift eingelöst wurde.

Die unbegrenzte Speicherung der Vertragsunterlagen begründete das Unternehmen damit, man wolle den Kunden auch nach Ablauf der Gewährleistungsfristen nicht vom Kundenservice ausschließen. Außerdem möchte man die Daten eventuell für noch nicht festgelegte Zwecke verwenden. Die Speicherung für noch nicht festgelegte Zwecke stellt allerdings eine rechtswidrige Vorratsdatenverarbeitung dar (§ 28 Abs. 1 Satz 2 BDSG). Eine Datenspeiche-

rung zur Erbringung von Serviceleistungen nach Ablauf der Gewährleistungsfrist kann nur dann als Grund für eine fortdauernde Speicherung verwendet werden, wenn sich das Unternehmen in seinen allgemeinen Geschäftsbedingungen zu einem Kundenservice verpflichtet, der über die Vorgaben des Bürgerlichen Gesetzbuches hinausgeht. Derartige Verpflichtungen waren allerdings in den allgemeinen Geschäftsbedingungen des Möbelhauses nicht enthalten, auch war es schwer nachvollziehbar, warum man bei mündlichen Kaufverträgen keinerlei Kundendaten speichert, wäre die Speicherung dieser Daten für den Kundenservice erforderlich, würde dies bedeuten, dass Kunden, die keinen schriftlichen Vertrag abschließen, schlechter gestellt werden. Wir haben das Unternehmen aufgefordert, die schriftlichen Kaufverträge entsprechend den Vorgaben des § 35 Abs. 2 Satz 2 Nr. 3 BDSG zu vernichten.

Anders als bei anderen Rabattsystemen, bei denen die Speicherung einzelner Vertragsabschlüsse für die Zuordnung der jeweils vertraglich zugesagten Incentives erforderlich ist, gewährt das Möbelhaus den Kundenkarteninhabern keine bestimmten und vorab definierten Vorteile, für die die von dem Unternehmen durchgeführte Datenspeicherung von Geschäftstransaktionen der Kundenkarteninhaber erforderlich wäre. Wir haben das Unternehmen aufgefordert, die Speicherung der einzelnen Geschäftstransaktionen bei Kundenkarten zu beenden oder für die Kundenkarte neue rechtliche Rahmenbedingungen zu schaffen.

Videoüberwachung eines Kaufhauses

Im Jahresbericht 2002 hatten wir darüber berichtet, dass ein Berliner Kaufhaus rechtswidrigerweise öffentliches Straßenland überwachte[113]. Unsere Rechtsauffassung wurde nunmehr vom Amtsgericht Mitte bestätigt[114]. Das Gericht betont, das verfassungsmäßige Recht auf informationelle Selbstbestimmung verbürge das Recht des Einzelnen, sich insbesondere in der Öffentlichkeit frei und ungezwungen bewegen zu dürfen, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung gemacht zu werden. Bei der gebotenen Güterabwägung mit dem Eigentumsrecht bzw. dem Recht am eingerichteten und ausgeübten Gewerbebetrieb (Art. 12, 14 GG) würden im vorliegenden Fall die schutzwürdigen Interessen der Betroffenen überwiegen. Allerdings räumte das Gericht dem Kaufhaus das Recht ein, zum Schutz des Eigentums einen 1 Meter breiten Streifen entlang der Schaufensterseiten und der übrigen Hausfront zu überwachen.

[113] JB 2002, 4.6.5
[114] Urteil vom 18. Dezember 2003, Az 16 C 427/02

4.7 Europäischer und internationaler Datenschutz

4.7.1 Ergebnisse aus Brüssel

Angemessenheitsentscheidungen

Die Europäische Kommission hat weitere Entscheidungen zur Angemessenheit des Datenschutzniveaus in Drittländern nach Art. 25 Abs. 6 Europäische Datenschutzrichtlinie getroffen. Nach der Schweiz, Ungarn und Kanada[115] sind nunmehr zu Argentinien[116] und zur Kanalinsel Guernsey[117] entsprechende Feststellungen getroffen worden. Die Kanalinseln Guernsey, Jersey und Isle of Man unterstehen der britischen Krone, ohne zum Vereinigten Königreich zu gehören oder Kolonie zu sein, und genießen volle Unabhängigkeit. Deshalb gelten sie als Drittländer. Darüber hinaus werden von der Europäischen Kommission die neuen EU-Länder, deren Beitritt am 1. Mai 2004 wirksam wird, ohne besondere Feststellung für den Übergangszeitraum als Drittländer mit angemessenem Datenschutzniveau betrachtet. Es sind dies (Ungarn ausgenommen) Estland, Lettland, Litauen, Malta, Polen, Slowakei, Slowenien, Tschechien und Zypern. Datenübermittlungen in alle aufgeführten Länder sind fortan unter den gleichen vereinfachten Voraussetzungen möglich wie solche in Mitgliedstaaten des EWR (§ 4 b Abs. 2 BDSG).

Verbindliche Unternehmensregelungen

Wir haben im letzten Jahr ausführlich über die Bedeutung und den Inhalt von Unternehmensregelungen als Garantie für den Datenschutz in Drittstaaten berichtet[118]. Damals waren bereits Diskussionen auf europäischer Ebene im Gange, deren Ergebnisse schließlich in ein Arbeitsdokument WP 74 der Art. 29-Datenschutzgruppe[119] mündeten. Es werden Aussagen zur Rechtsnatur und zum wesentlichen Inhalt von verbindlichen Unternehmensregelungen getroffen. Für die Zusammenarbeit der nationalen Aufsichtsbehörden in den Fällen, in denen Unternehmensteile in mehreren EU-Mitgliedstaaten ansässig sind, wird ein Verfahren skizziert, das bei der Überprüfung der Unternehmensregelung greifen soll. Der gegenüber der

---

[115] ABl. EG vom 25. August 2000, L 215/1, L 215/4; ABl. EG vom 4. Januar 2002, L 2/13
[116] Entscheidung vom 30. Juni 2003, ABl. EG vom 5. Juli 2003, L168/19
[117] Entscheidung vom 21. November 2003, ABl. EG vom 25. November 2003, L 308/27
[118] JB 2002, 3.2 und 4.7.3
[119] Arbeitsdokument vom 3. Juni 2003: Übermittlung personenbezogener Daten in Drittländer: Anwendung von Art. 26 Abs. 2 der EU-Datenschutzrichtlinie auf verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2003“, S. 65

Entwurfsfassung deutlich abgespeckte Abschnitt über das koordinierte Verfahren der Aufsichtsbehörden sieht u. a. vor, dass Unternehmen, die an einer Genehmigung für ähnliche Arten des Datenexports aus verschiedenen Mitgliedstaaten interessiert sind, sich eines koordinierten Genehmigungsverfahrens bedienen können. Dem liegt die Hauptidee zugrunde, „dass Unternehmen nur *einen* Antrag auf Genehmigung bei einer Datenschutzbehörde eines Mitgliedstaats stellen können, der zur Erteilung von Genehmigungen durch alle Datenschutzbehörden der Mitgliedstaaten führt, in denen das Unternehmen tätig ist." Ob diese Hauptidee von allen Mitgliedern der Art. 29-Datenschutzgruppe verfolgt werden wird, ist zu bezweifeln. Bei den Verhandlungen über das Arbeitspapier hat sich ein deutliches Nord-Süd-Gefälle aufgetan. Insbesondere die Südeuropäer hatten grundsätzliche Bedenken gegen Unternehmensregelungen vorgetragen und die konsequente Anwendung der Standardverträge gefordert. Die Entscheidung eines anderen Mitgliedstaates sich zueigen zu machen, findet dort ebenfalls keinen großen Anklang. Dagegen haben Finnland, Großbritannien, Niederlande, Österreich und Deutschland vereinbart, das Kooperationsverfahren bei nächster Gelegenheit zu erproben.

Sogleich nach Verabschiedung des WP 74 hat die Art. 29-Datenschutzgruppe eine *öffentliche Umfrage* zu dem Arbeitsdokument eingeleitet. Dabei wurden Wirtschaftsunternehmen und Aufsichtsbehörden aufgefordert, ihre Erfahrungen im Umgang mit dem Arbeitsdokument mitzuteilen. Das zusammengetragene Material[120] soll Eingang finden in eine öffentliche Anhörung, die im ersten Halbjahr 2004 von der Europäischen Kommission veranstaltet wird. Einigkeit lässt sich aus deutscher Sicht zumindest in einem Punkt bereits erzielen: Unternehmensregelungen bieten bei Umsetzung der Vorgaben des WP 74 eine Alternative zu den Standardvertragsklauseln der Europäischen Kommission und erleichtern gerade multinationalen Unternehmen die Beachtung des Datenschutzes nach grenzüberschreitendem Datentransfer. Leider ist die Idee der Schaffung einer Musterunternehmensregelung, die von der Europäischen Kommission nach dem Vorbild ihrer Standardvertragsklauseln zu erarbeiten wäre, bislang nicht weiter gediehen: Der wissenschaftliche Dienst prüft noch, ob sich dies mit dem Wortlaut von Art. 26 Abs. 4 Europäische Datenschutzrichtlinie vereinbaren lässt.

Nicht zuletzt als Folge der Diskussion um ein koordiniertes Vorgehen der Aufsichtsbehörden in Europa bei Vorliegen von Unternehmensregelungen ist gefragt worden, auf welche Art und Weise Mitteilungen der Mitgliedstaaten nach Art. 26 Abs. 3 Europäische Datenschutzrichtlinie, also über erteilte Genehmigungen, gegenüber der Europäischen Kommission und anderen Mitgliedstaaten erfolgen müssen. Die Europäische Kommission selbst hat in einem veröf-

fentlichten Vermerk[121] Einzelheiten hierüber festgelegt. Leider enthält das Papier zwei elementare Mängel, die sich im Verfahren als sehr hinderlich erweisen werden: Die dreimonatige Frist, innerhalb der die Europäische Kommission Widersprüche anderer Mitgliedstaaten gegen die von einer Aufsichtsbehörde erteilte Genehmigung mitzuteilen gedenkt, ist nicht als Ausschlussfrist zu verstehen, obwohl dies aus Gründen der Rechtssicherheit für die Unternehmen, aber auch für die Aufsichtsbehörden sehr hilfreich wäre. Mit der Empfangsbestätigung sollen die übrigen Mitgliedstaaten über eine Genehmigung nach Art. 26 Abs. 3 Europäische Datenschutzrichtlinie von der Kommission informiert werden. Die Empfangsbestätigung beinhaltet einige Details zum Sachverhalt, aber nicht den Namen des Unternehmens. Damit ist es anderen Mitgliedstaaten unmöglich, zeitnah festzustellen, ob eine eigene Betroffenheit wegen einer Niederlassung des Unternehmens im eigenen Zuständigkeitsbereich und einer gleichartigen Datenübermittlung vorliegt. Es besteht die Hoffnung, dass eine Klärung dieser Punkte noch im Ausschuss nach Art. 31 Europäische Datenschutzrichtlinie herbeigeführt wird.

Erster Bericht über die Durchführung der Datenschutzrichtlinie

Die Europäische Kommission hat – wie in Art. 33 Europäische Datenschutzrichtlinie vorgesehen – dem Europäischen Parlament und dem Rat einen „Ersten Bericht über die Durchführung der Datenschutzrichtlinie“[122] vorgelegt. Sie ist der Auffassung, dass es aus verschiedenen Gründen nicht sinnvoll ist, in nächster Zukunft Vorschläge zu Änderung der Richtlinie zu unterbreiten. So seien die Erfahrungen mit der Durchführung der Richtlinie angesichts der von einigen Mitgliedstaaten versäumten fristgemäßen Umsetzung bisher sehr begrenzt. Auch könnten viele Schwierigkeiten, die bei der Überprüfung ermittelt wurden, ohne Änderung der Richtlinie behoben werden. In einigen Fällen seien Änderungen der innerstaatlichen Rechtsvorschriften erforderlich, die eine richtlinienkonforme Vorgehensweise verhinderten. Als einen Hauptkritikpunkt sieht die Kommission die Abweichungen, die die Mitgliedstaaten zur Umsetzung von Art. 25, 26 Europäische Datenschutzrichtlinie (Grundsätze und Ausnahmen zur Übermittlung personenbezogener Daten in Drittländer) erlassen haben. Der Bericht enthält daneben eine Aussage zu der (von den deutschen Aufsichtsbehörden seit längerem diskutierten) Frage, ob beim Vorliegen einer Unternehmensregelung die hierauf beruhende

---

[120] Art. 29-Datenschutzgruppe: Ergebnisse der öffentlichen Umfrage zum Thema verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer, Stand: 18. November 2003

[121] vom 21. August 2003: Mitteilungen der Mitgliedstaaten nach Artikel 26 Absatz 3 der Richtlinie und Austausch bewährter Verfahren

[122] Bericht vom 15. Mai 2003, KOM(2003) 265 endg.

Datenübermittlung genehmigungspflichtig oder genehmigungsfrei ist[123]. Für die Einordnung von Datenübermittlungen auf der Grundlage von Unternehmensregelungen in § 4 c Abs. 2 BDSG, also für die Genehmigungspflicht, haben sich mittlerweile außer uns die Aufsichtsbehörden in Brandenburg, Bremen, Hamburg, Nordrhein-Westfalen, Schleswig-Holstein sowie der Bundesbeauftragte für den Datenschutz ausgesprochen. Die „§ 4 b-Befürworter", die entgegen dem Wortlaut von § 4 c Abs. 2 BDSG eine Datenübermittlung auf der Grundlage von Unternehmensregelungen nach § 4 b Abs. 2 Satz 2 BDSG eingeordnet wissen wollen, haben nun durch die Europäische Kommission eine mehrfache Absage erhalten. So heißt es in dem „Ersten Bericht" unter 4.4.5:

„Der von einigen Mitgliedstaaten verfolgte Ansatz, bei dem die Beurteilung der Angemessenheit des vom Empfänger garantierten Schutzniveaus von dem für die Verarbeitung Verantwortlichen vorgenommen werden soll, die Kontrolle der Datenströme durch den Staat oder die nationale Kontrollstelle aber sehr begrenzt ist, entspricht offensichtlich nicht der Anforderung, die den Mitgliedstaaten in Art. 25 Abs. 1 auferlegt wird."

Diese Auffassung, nach der Unternehmensregelungen nicht unter Art. 25 Abs. 1, sondern unter Art. 26 Abs. 2 Europäischen Datenschutzrichtlinie fallen, was die Genehmigungspflicht der hierauf beruhenden Datenübermittlungen indiziert, liegt unzweifelhaft auch dem Vermerk der Europäischen Kommission über die „Mitteilungen der Mitgliedstaaten nach Art. 26 Abs. 3 der Richtlinie" sowie dem Arbeitspapier WP 74 der Art. 29-Datenschutzgruppe zugrunde.

Übermittlung von Flugpassagierdaten in die USA

Ein in der Öffentlichkeit heiß diskutiertes und nach Ende des Berichtszeitraums noch immer nicht abgeschlossenes Thema ist die Frage, unter welchen Voraussetzungen die Übermittlung von Flugpassagierdaten in die USA zulässig ist. Seit März sind die fünf größten europäischen Fluggesellschaften Air France, British Airways, Iberia, KLM und Lufthansa aufgrund der US-Antiterrorgesetzgebung verpflichtet, dem US-Zoll und den Sicherheitsbehörden die Reservierungsdaten zur Kenntnis zu geben. Bei Verweigerung wurde von US-Seite mit hohen finanziellen Strafen bis zum Entzug der Landeerlaubnis gedroht. Die Reservierungsdaten umfassen als PNR-Daten (Passenger Name Record) diejenigen Angaben, die Fluggesellschaften zur Abwicklung eines Fluges speichern. Die Daten können bis zu 60 verschiedene Informationen je Passagier beinhalten. Dazu können auch sensitive Daten[124] über die

[123] vgl. bereits JB 2002, 4.7.3
[124] JB 2002, 3.1

Gesundheit (z. B. Rollstuhlfahrer) oder über Essensgewohnheiten (z. B. koschere Mahlzeit) gehören, aus denen Rückschlüsse auf die religiöse Überzeugung gewonnen werden können. Der Zugriff durch das nach den Terroranschlägen vom 11. September 2001 neu gegründete Heimatschutzministerium der USA auf die begehrten Daten erfolgt über das europäische Reservierungssystem „AMADEUS“.

Aus deutscher Sicht ist die Datenübermittlung in die USA mangels freiwilliger Einwilligung und gesetzlicher Rechtsgrundlage nicht zulässig. Zwar ist das berechtigte kommerzielle Interesse der Lufthansa an der Datenübermittlung zur Abwehr von möglichen Sanktionen durch die US-Seite anzuerkennen (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG). Allerdings ist das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Übermittlung nicht nur wegen des fehlenden angemessenen Datenschutzniveaus in den USA höherwertig, sondern auch, weil mehr als die für die US-Behörden erforderlichen Daten dorthin übermittelt werden (sensitive Daten über den Gesundheitszustand und ethnische Zugehörigkeit, Daten über andere als USA-Flüge).

Angesichts der politischen und wirtschaftlichen Dimension ist die Europäische Kommission in Verhandlungen mit der US-amerikanischen Zoll- und Grenzschutzbehörde (US-Customs and Border Protection CBP) eingetreten, die in eine „Gemeinsame Erklärung“[125] mündeten. Die US-Seite hat hier Zusagen zum sachgerechten Umgang mit den Daten gemacht (z. B. keine Nutzung der sensitiven Daten). Das Verhandlungsergebnis wurde vom Europäischen Parlament als nicht sachgerecht angesehen und in einer Entschließung missbilligt[126]. Es wurde bezweifelt, dass die übermittelten Daten in den USA angemessen geschützt seien, und gefordert, das Abkommen auszusetzen. In einer weiteren Entschließung[127] hat das Europäische Parlament – offenbar angesichts nicht weiterführender Verhandlungen - sogar angedroht, die Europäische Kommission wegen Untätigkeit zu verklagen, wenn nicht bis zum Ende des Jahres ein zufriedenstellendes Ergebnis erzielt würde.

Rechtzeitig hat die Kommission in einer „Mitteilung an den Rat und das Parlament“[128] einen Bericht über den Verhandlungsstand erstattet. Hiernach haben die USA bestimmte Zusagen zum Datenschutz gegeben. Geklärt ist die Speicherfrist, die von den ursprünglich verlangten 50 Jahren auf dreieinhalb reduziert wurde. Die Zweckbestimmung der Datenverwendung wurde beschränkt auf die Bekämpfung des Terrorismus und anderer Verbrechen. Die Anzahl

---

[125] „Joint Statement“ vom 17./18. Februar 2003, Zusatzerklärung vom 4. März 2003
[126] vom 13. März 2003
[127] vom 9. Oktober 2003
[128] vom 16. Dezember 2003: Übermittlung von Fluggastdatensätzen (PNR).: Ein sektorübergreifendes EU-Konzept

der geforderten Datenelemente beträgt 34. Offen ist, ob und unter welchen Umständen von dem Verfahren abgerückt werden soll, nach dem die US-Behörden auf alle Reservierungsdaten zugreifen (so genannte Pull-Lösung). Die Übermittlung der benötigten Daten durch die Fluggesellschaften (so genannte Push-Lösung) wäre die datenschutzgerechte Alternative.

4.7.2 AG Internationaler Datenverkehr

Verbindliche Unternehmensregelungen

Wie im vergangenen Jahr[129] hat sich die Arbeitsgruppe „Internationaler Datenverkehr“ des „Düsseldorfer Kreises“ unter unserem Vorsitz vornehmlich mit dem Inhalt von verbindlichen Unternehmensregelungen (§ 4 c Abs. 2 BDSG) befasst. Zunächst hatte der Konzern General Electric (GE) Company eine „Verbindliche Unternehmensregelung für den Datenschutz von Mitarbeiterdaten“ zur Überprüfung auf ausreichende Garantien nach § 4 c Abs. 2 BDSG bei den Aufsichtsbehörden eingereicht. Die Schwierigkeit bestand zunächst darin, unter ihnen die Federführung bei der Beratung der Unternehmensregelung festzustellen. Aus der vom Unternehmen vorgelegten Übersicht ergab sich, dass allein in Deutschland etwa 200 Niederlassungen des US-Konzerns ansässig sind, ohne dass es hier einen Hauptsitz gibt. Da sich die meisten von ihnen in Nordrhein-Westfalen befinden, hat die dortige Aufsichtsbehörde die Federführung in den Beratungen mit dem Unternehmen übernommen. Der „Düsseldorfer Kreis“ hat die Regelung schließlich verabschiedet, so dass auf ihrer Grundlage Datenübermittlungen in Konzernteile in Drittländern vorgenommen werden dürfen. In Berlin konnte auf dieser Basis die von einer Niederlassung beantragte Genehmigung der Datenübermittlung in einen Konzernteil in den USA positiv beschieden werden.

Die Arbeitsgruppe hat sich darüber hinaus mit der „Leitlinie (Code of Conduct) zum Schutz der Persönlichkeitsrechte im Umgang mit personenbezogenen Daten in der Deutschen Telekom Gruppe“ befasst, die die Verarbeitung von Kunden-, Mitarbeiter- und Aktionärsdaten sowie von Daten über Geschäftspartner weltweit einheitlich regelt. Der „Düsseldorfer Kreis“ hat auch diese Regelung verabschiedet. Genehmigungen für die Datenübermittlung durch Konzerntöchter auf dieser Grundlage wurden noch nicht erteilt.

In den Beschlüssen des „Düsseldorfer Kreises“ zu den beiden Unternehmensregelungen findet sich angesichts des unter den Aufsichtsbehörden noch immer nicht beigelegten Streits

[129] JB 2002, 4.7.3

über die Genehmigungspflicht[130] der Vorbehalt, dass die für die einzelnen Unternehmen zuständige Aufsichtsbehörde im Einzelfall abschließend beurteilt, ob die Unternehmensregelung als Grundlage für Genehmigungen nach § 4 c BDSG bzw. als Grundlage für ein angemessenes Datenschutzniveau nach § 4 b BDSG anzusehen ist.

Der bereits im letzten Jahr schwelende Streit unter den Aufsichtsbehörden ist zwischenzeitlich von uns als diesjährigem Vorsitzland des „Düsseldorfer Kreises“ an die Europäische Kommission herangetragen worden[131]. Die Europäische Kommission hat in ihrer Antwort[132] zwar nicht ausdrücklich die Frage der Genehmigungspflicht bejaht. Sie hat aber entscheidend darauf abgehoben, dass das in Art. 26 Abs. 3 Europäische Datenschutzrichtlinie genannte Verfahren, nach dem die Entscheidungen der Mitgliedstaaten über erteilte Genehmigungen den übrigen Mitgliedstaaten und der Kommission mitzuteilen sind, eingehalten werden muss[133]. Dies setzt nach Auffassung der Kommission voraus, „dass die Datenschutzbehörden seitens der Unternehmen systematisch über in diesem Bereich existierende Regelungen informiert werden“. Dementsprechend lässt sich zumindest diejenige Tendenz unter den „§ 4 b-Befürwortern“ nicht halten, dass die Aufsichtsbehörde noch nicht einmal über in Kraft gesetzte Unternehmensregelungen informiert werden will. Auch lässt sich das in Art. 26 Abs. 3 der Richtlinie genannte und von der Europäischen Kommission für zwingend gehaltene Mitteilungsverfahren dann nicht durchführen, wenn mitzuteilende Genehmigungen grundsätzlich nicht erteilt werden. Deshalb muss „zwischen den Zeilen“ davon ausgegangen werden, dass die (diplomatisch gehaltene) Antwort auf unsere Anfrage als Unterstützung unserer Auffassung zur Genehmigungspflicht zu verstehen ist.

Bestärkt wird diese Ansicht durch eine das Antwortschreiben ergänzende Äußerung der Europäischen Kommission gegenüber den Teilnehmern der Arbeitsgruppe. Hiernach herrsche in der Kommission die einhellige Meinung, dass Art. 25 Abs. 1 Europäische Datenschutzrichtlinie (vgl. § 4 b Abs. 2 BDSG) immer dann anwendbar sei, wenn die datenexportierende Stelle bestimmte rechtliche Regelungen im Drittland bereits *vorfindet*. Dagegen sei Art. 26 Europäische Datenschutzrichtlinie anwendbar, wenn die exportierende Stelle erst Regelungen *erarbeitet*. Deshalb seien Unternehmensregelungen unzweifelhaft unter Art. 26 Abs. 2 (und damit unter § 4 c Abs. 2 BDSG) zu subsumieren. Die Europäische Kommission befürwortet also unsere Auffassung, die von den Aufsichtsbehörden in Brandenburg, Bremen, Hamburg, Nordrhein-Westfalen, Schleswig-Holstein sowie dem Bundesbeauftragten für den

[130] vgl. 4.7.1 sowie ausführlich JB 2002, 4.7.3
[131] Schreiben vom 21. Mai 2003
[132] vom 8. August 2003
[133] vgl. 4.7.1

Datenschutz geteilt wird, nach der Datenübermittlungen auf der Grundlage von Unternehmensregelungen genehmigungspflichtig sind[134].

Leider ist damit der Streit unter den Aufsichtsbehörden noch immer nicht beigelegt, was insbesondere für die Wirtschaftsunternehmen unbefriedigend ist. Hier bedarf es offenbar einer ausdrücklichen Feststellung der Europäischen Kommission, dass die Umsetzung von Art. 26 Abs. 2 Europäische Datenschutzrichtlinie in Gestalt des § 4 b Abs. 2 Satz 2 BDSG und die hierauf beruhende Praxis der „§ 4 b-Befürworter“ richtlinienwidrig sind.

Internationale Auftragsdatenverarbeitung

Immer wieder erreichen uns Anfragen, was zu beachten ist, wenn ein Unternehmen innerhalb oder außerhalb der EU Daten für einen Auftraggeber verarbeitet und seinerseits einen Unterauftragnehmer im Drittland einschaltet. Dabei ist fraglich, welches Recht überhaupt gilt (§ 1 Abs. 5 BDSG) und wer mit wem (bei Geltung deutschen Rechts) einen Vertrag zur Schaffung ausreichender Garantien nach § 4 c Abs. 2 BDSG schließen muss.

> *Ein medizinisches Forschungsunternehmen stellte die Frage, welche Datenschutzbestimmungen greifen, wenn ein anderes Unternehmen aus einem Mitgliedstaat der Europäischen Union in Berlin sensitive Daten sammelt (also erhebt) oder im Auftrag sammeln lässt, ohne hierfür eine Niederlassung in Berlin einzusetzen*.

Nach § 1 Abs. 5 Satz 1 BDSG, der vom Gedanken des europäischen Binnenmarktes geprägt ist, soll – auch in Fällen der Auftragsdatenverarbeitung – für die in Deutschland (ohne Niederlassung) erhobenen Daten nicht das BDSG, sondern das Recht des andernorts in der Europäischen Union befindlichen Unternehmens (hier: das Recht des Auftraggebers) gelten. Dies ist nach dem Wortlaut der Regelung auch dann der Fall, wenn der betroffene Mitgliedstaat die Europäische Datenschutzrichtlinie noch nicht in eigenes nationales Recht umgesetzt hat.

> *Mehrere Unternehmen mit Sitz in der Schweiz, Ungarn, der Tschechischen Republik und Indien lassen in Berlin sensitive Daten im Auftrag erheben.*

Nach § 1 Abs. 5 Satz 2 BDSG gilt nicht das Recht der im Drittland befindlichen Auftraggeber, sondern das BDSG für die in Deutschland im Auftrag erhobenen Daten. Die Unternehmen in

[134] vgl. 4.7.1

der Schweiz und in Ungarn (Drittländer mit angemessenem Datenschutzniveau) werden also nicht anders behandelt als das Unternehmen in der Tschechischen Republik, die – ebenso wie die übrigen EU-Beitrittskandidaten (Ungarn ausgenommen) – für den Übergangszeitraum bis zum Beitrittstermin am 1. Mai 2004 als Drittland mit angemessenem Datenschutzniveau anzusehen ist[135], oder als Indien (Drittland ohne angemessenes Datenschutzniveau).

> *Ein Unternehmen in Deutschland lässt Kundendaten von einem Unternehmen in Brasilien im Auftrag verarbeiten, das seinerseits für einen Teil der Auftragsdatenverarbeitung ein Unternehmen in Venezuela einschaltet. Das deutsche Unternehmen möchte wissen, welches Unternehmen mit welchem anderen welchen Standardvertrag der Europäischen Kommission (für Auftragsdatenverarbeitung oder für Eigenverarbeitung) schließen muss.*

In diesem Fall, in dem sich der *Auftraggeber in der EU* befindet, aber *Auftragnehmer und Unterauftragnehmer im Drittland* ansässig sind, muss bedacht werden, dass der Standardvertrag der Europäischen Kommission vom 27. Dezember 2001 (Auftragsdatenverarbeitung) im Gegensatz zum Standardvertrag vom 15. Juni 2001 (Eigenverarbeitung)[136] keine Regelung über die Weiterübermittlung der Daten an eine andere Stelle enthält. Offenbar ist die Weiterübermittlung der Daten durch den im Drittland befindlichen Auftragnehmer an den im Drittland befindlichen Unterauftragnehmer deshalb im Standardvertrag/Auftragsdatenverarbeitung nicht geregelt, weil die Entscheidung über die Weiterübermittlung an den Unterauftragnehmer (hier: in Venezuela) nicht im Drittland (hier: durch den Auftragnehmer in Brasilien), sondern im Binnenmarkt (nämlich durch den Auftraggeber in Deutschland) getroffen werden soll. Folgende Lösungen bieten sich an: Entweder muss der Auftraggeber in Deutschland einen weiteren Standardvertrag mit dem Unterauftragnehmer in Venezuela schließen oder der Unterauftragnehmer übernimmt selbst die Pflichten des Auftragnehmers in Brasilien, indem er (der Unterauftragnehmer) dem Vertrag zwischen dem Auftraggeber in Deutschland und dem Auftragnehmer in Brasilien beitritt.

> *Das deutsche Unternehmen lässt Kundendaten von einem Unternehmen (Rechenzentrum) in Spanien im Auftrag verarbeiten, das seinerseits ein Unternehmen in Venezuela einschaltet.*

Hier sind sowohl *Auftraggeber als auch Auftragnehmer in der EU* ansässig, nur der *Unterauftragnehmer* befindet sich *im Drittland*. Ein Vertrag zwischen dem Auftraggeber und dem Un-

---

[135] vgl. 4.7.1

[136] Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2001“, S. 37 ff.

terauftragnehmer erscheint zumindest in den Fällen nicht praktikabel, in denen der Auftragnehmer als Rechenzentrum im Auftrag einer Vielzahl von Auftraggebern Daten verarbeitet. Der Abschluss eines (Standard-)Vertrages zwischen dem Auftragnehmer in Spanien und dem Unterauftragnehmer in Venezuela ist deshalb nicht sachgerecht, weil der Auftragnehmer (anders als der Datenexporteur in den Standardverträgen) nicht verantwortliche Stelle ist. Deshalb ist es sachgerecht, dass der Auftragnehmer in Spanien im Auftrag des Auftraggebers in Deutschland einen (Standard-)Vertrag/Auftragsdatenverarbeitung mit dem Unterauftragnehmer in Venezuela abschließen muss. Dies erscheint insbesondere sinnvoll, weil damit der Auftraggeber in Deutschland als verantwortliche Stelle bei der Einschaltung eines Unterauftragnehmers in Venezuela durch den Auftragnehmer in Spanien nicht „außen vor" gelassen wird.

4.8 Organisation und Technik

4.8.1 Behördliche Datenschutzbeauftragte

Befragung zur Umsetzung des Berliner Datenschutzgesetzes 2001

Zwei Jahre nach In-Kraft-Treten des Berliner Datenschutzgesetzes von 2001 haben wir 176 öffentliche Stellen des Landes nach der Umsetzung der darin enthaltenen neuen Regelungen zur Organisation des Datenschutzes befragt, darunter alle Senatsverwaltungen, Bezirksämter und die großen nachgeordneten Behörden, aber auch kleinere Stellen wie Berufskammern und Stiftungen.

Die Rückläufe brachten viele Erkenntnisse darüber, wie ernst es die Behörden mit ihrer bereits seit 1979 bestehenden Pflicht nach § 28 BlnDSG nehmen, uns bei der Erfüllung unserer Aufgaben zu unterstützen. Nach dieser Vorschrift ist uns Auskunft zu unseren Fragen zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Die Beantwortung unserer Schreiben ist für die angeschriebenen Stellen gesetzliche Pflicht.

Wir mussten bei sehr vielen Stellen an die Beantwortung erinnern, da sie die gesetzten Fristen verstreichen ließen. Auf unsere Bitte um Beantwortung unseres Fragenkatalogs haben 25 Stellen (das sind ca. 15 % aller angeschriebenen Stellen) überhaupt nicht reagiert; die wichtigsten unter ihnen sind die Senatsverwaltungen für Stadtentwicklung, für Bildung, Jugend und Sport sowie für Wissenschaft, Forschung und Kultur sowie die drei großen Landesämter zur Regelung offener Vermögensfragen (LAROV), für Gesundheit und Soziales (LAGeSo) und für Arbeitsschutz, Gesundheitsschutz und technische Sicherheit (LAGetSi).

25 weitere Stellen haben entweder um Fristverlängerung für die Beantwortung unseres Fragebogens gebeten oder aber dargelegt, dass für ihre Antworten die übergeordnete Senatsverwaltung zuständig sei, die auch den behördlichen Datenschutzbeauftragten stellt - die aber ihrerseits nicht der Informationspflicht nachgekommen war, da es sich um eine der bereits erwähnten Senatsverwaltungen handelte.

Die Befragung betraf die Pflichten zur Bestellung eines Stellvertreters des behördlichen Datenschutzbeauftragten nach § 19 a Satz 1 BlnDSG, zur Führung von Dateibeschreibungen nach § 19 Abs. 2 BlnDSG und zur Durchführung der Vorabkontrolle nach § 5 Abs. 3 Satz 2, die nach 19 a Satz 3 Nr. 1 BlnDSG vom behördlichen Datenschutzbeauftragten durchzuführen ist. Um einen vollständigen Überblick zu erhalten, haben wir auch nach der Person des behördlichen Datenschutzbeauftragten gefragt, einer Institution, die bereits seit 1990 im BlnDSG gefordert wird. 18 Behörden, darunter auch große, haben unsere Umfrage zum Anlass genommen, ihrer gesetzlichen Pflicht zur Bestellung eines behördlichen Datenschutzbeauftragten nachzukommen.

Einige kleinere Stellen haben bedauert, dass sich aus ihrem geringen Personalbestand niemand finden lässt, der für das Amt des Datenschutzbeauftragten geeignet wäre. Die Mitarbeiter hätten nicht die erforderliche Fachkunde oder seien mit anderen Aufgaben so ausgelastet, dass die Aufgaben des Datenschutzes daneben nicht zu bewältigen seien.

Nach der Novelle des BlnDSG haben kleinere Stellen nach § 19 a Abs. 1 Satz 2 nun die Möglichkeit erhalten, ihre Datenschutzbelange durch gemeinsame Datenschutzbeauftragte oder vom Datenschutzbeauftragten einer anderen Behörde betreuen zu lassen. Dies ist zumindest dann sinnvoll, wenn Stellen ein ähnliches Aufgabenspektrum haben oder wenn der Datenschutzbeauftragte einer übergeordneten Behörde die Aufgaben mit erledigt. Von dieser Möglichkeit haben bisher sieben Stellen Gebrauch gemacht bzw. befinden sich noch im Abstimmungsprozess.

Obwohl die Verpflichtung zur Bestellung eines Stellvertreters seit bereits mehr als zwei Jahren besteht, gibt es immer noch 20 Stellen, bei denen diese Funktion nicht besetzt ist. Meist wurde jedoch die Absicht bekundet, demnächst einen Stellvertreter zu benennen. Andere Stellen waren der Auffassung, wegen ihrer geringen Größe keinen stellvertretenden Datenschutzbeauftragten benennen zu müssen. Der Gesetzgeber hatte solche Ausnahmen aber nicht vorgesehen, weil der Datenschutzbeauftragte bei Abwesenheit vertreten werden muss.

Eine weitere Frage betraf das Zeitbudget des Datenschutzbeauftragten im Verhältnis zu seinen sonstigen Aufgaben. In den überwiegenden Fällen wird der Zeitaufwand für die Durchführung der Datenschutzaufgaben nach Bedarf bemessen. Sofern Abschätzungen versucht wurden, nannten sie höchstens 5 % der Gesamtarbeitszeit. Man muss davon ausgehen, dass in all diesen Fällen eine Entlastung von den Hauptaufgaben in dieser Größenordnung nicht vorgesehen ist. Es ist zu erwarten, dass in solchen Behörden kaum die unmittelbar aus dem Gesetz folgenden formalen Pflichten (Dateibeschreibungen nach § 19 Abs. 2 BlnDSG, Vor-abkontrollen nach § 19 a Abs. 1 Satz 3 Nr. 1 BlnDSG) erfüllt werden können.

Nur acht Stellen haben einen vollzeitig tätigen Datenschutzbeauftragten für die Sicherstellung des Datenschutzes im Hause bestellt. In zehn weiteren Fällen beläuft sich die Spanne immerhin noch zwischen 50 bis 85 % der Arbeitszeit. 12 Stellen teilten mit, dass sie als Zeitbudget für den Datenschutz 5 bis 40 % vorsehen.

Die Regelungen zur Erstellung und Führung von Übersichten über die vom behördlichen oder vom Berliner Datenschutzbeauftragten zu kontrollierenden Datenverarbeitungen ist zwar mit dem neuen Gesetz vereinfacht worden, da die im Gesetz genannten Dateibeschreibungen nach § 19 Abs. 2 BlnDSG in Wirklichkeit nur für ganze Verfahren, nicht mehr für einzelne Dateien erstellt werden müssen. Jedoch gibt es nach wie vor Missverständnisse darüber, wer die Dateibeschreibungen zu erstellen hat. Obwohl ihnen die notwendigen Zeitbudgets nicht zur Verfügung gestellt werden, wird manchmal den Datenschutzbeauftragten alles zugewiesen, was mit dem Thema Datenschutz zu tun hat. Das Erstellen der Beschreibungen bzw. Verzeichnisse über Art und Umfang der Datenverarbeitung ist jedoch nicht Sache der behördlichen Datenschutzbeauftragten, denn sie können im Normalfall die technischen und organisatorischen Aspekte einer EDV-Anwendung nicht überschauen. Die Beschreibungen sind vielmehr in der Verantwortung der Leitung der Daten verarbeitenden Stelle von den örtlichen Verfahrensverantwortlichen zu erstellen und dem Datenschutzbeauftragten zur Verfügung zu stellen.

Richtigerweise werden in den meisten Fällen die Beschreibungen durch Mitarbeiter erstellt, die für die Verarbeitung der Daten verantwortlich sind. In den Antworten wurden dabei Systemverwalter, Anwendungssystembetreuer, EDV-Beauftragter, Mitarbeiter des Controllings genannt, in Einzelfällen sogar die Leiter dieser Stellen (Dienststellenleiter, Geschäftsstellenleiter, Leiter Personalverwaltung).

Ordnungs- und Sicherheitsbehörden müssen für die bei ihnen geführten Dateien Errichtungsanordnungen erstellen, die im Wesentlichen der früheren Dateiregistermeldung ent-

sprechen. Eine Stelle leitete daraus ab, keine Dateibeschreibung fertigen zu müssen. Da jedoch sowohl der Gegenstand als auch der Inhalt der Beschreibung von der Errichtungsanordnung wesentlich abweichen, trifft dies nicht zu.

Die Dateibeschreibungen nach § 19 Abs. 2 BlnDSG sind nach § 19 a Abs. 1 Satz 5 BlnDSG jeder Person zur Einsicht vorzulegen. Dies ist Aufgabe des behördlichen Datenschutzbeauftragten, der nach § 19 a Abs. 1 Satz 4 BlnDSG das Verzeichnis führt. Das wird überwiegend auch so gehandhabt. Auch andere Stellen, wie z. B. der Verfahrensverantwortliche, der dezentrale Infrastrukturbetreiber oder der Beauftragte für IuK-Technik können natürlich weitere Exemplare bereithalten.

Es gibt auch Stellen, bei denen die Dateibeschreibung in der Verwaltungsregistratur aufbewahrt oder sogar im internen IT-Netz zum Abruf bereitgestellt wird. Dies kann nur eine zusätzliche Veröffentlichungsform sein, denn der Bürger muss in jedem Fall bei einer zentralen Stelle - nämlich dem behördlichen Datenschutzbeauftragten - in die schriftlich niedergelegten Dateibeschreibungen Einsicht nehmen können.

Nach § 5 Abs. 3 Satz 2 in Verbindung mit § 19 a Abs. 1 Satz 3 Nr. 1 BlnDSG haben die behördlichen Datenschutzbeauftragten eine Vorabkontrolle durchzuführen, wenn damit die Verarbeitung personenbezogener Daten mit besonderen Risiken für Rechte und Freiheiten von Betroffenen verbunden ist, insbesondere wenn sie einem Berufs- oder besonderen Amtsgeheimnis unterliegen oder zur Verfolgung von Straftaten und Ordnungswidrigkeiten erhoben werden. Unsere Frage betraf die Stellen in den Behörden, die die erforderlichen Unterlagen (z. B. Risikoanalyse und Sicherheitskonzept) dem behördlichen Datenschutzbeauftragten dafür zur Verfügung stellen. Die Antworten benannten die IT-Stelle, die Serviceeinheit Verwaltung, den Verfahrensverantwortlichen oder die Fachabteilung. In einigen Fällen wird bei der Erstellung der Unterlagen sofort der behördliche Datenschutzbeauftragte eingeschaltet, der zumindest bei Fragen, die den Datenschutz unmittelbar berühren, beratend mitwirkt. Dagegen ist nichts einzuwenden, doch es bleibt originäre Aufgabe der Verantwortlichen einer Daten verarbeitenden Stelle, sich bei der Einführung neuer automatisierter Verarbeitungen bereits im Vorfeld Gedanken über die Sicherheitsaspekte zu machen. Die Unterlagen für die Vorabkontrolle sollten möglichst in einer Hand zusammengeführt werden, damit Dritte (z. B. behördlicher Datenschutzbeauftragter, Berliner Beauftragter für Datenschutz und Informationsfreiheit) nur einen Ansprechpartner haben.

Die Antworten (oder auch Nichtantworten) auf die Umfrage oder auch die Art der Beantwortung machten deutlich, dass es für die Durchsetzung des Datenschutzes wichtig ist, wenn

von Zeit zu Zeit an die Einhaltung der gesetzlichen Vorschriften erinnert wird, insbesondere in den nachgeordneten Bereichen der Verwaltung, die nicht immer im Rampenlicht stehen. Die Beachtung der Datenschutzgesetze wird gerade dort noch gelegentlich als Pflicht zweiter Ordnung angesehen, als eine Pflicht, um die man sich kümmert, wenn man „keine anderen Sorgen“ mehr hat.

Gesprächskreis der behördlichen Datenschutzbeauftragten der Bezirke

Auch im vergangenen Jahr fanden wieder drei Treffen der Datenschutzbeauftragten der Bezirksämter von Berlin statt, bei denen es zu angeregten Diskussionen bei besonders interessierenden Fragen kam. Einige seien an dieser Stelle herausgegriffen:

So ging es um die Akteneinsichtsrechte des behördlichen Behindertenbeauftragten im Rahmen seiner Beteiligungs- bzw. Anhörungsrechte. Übereinstimmend war man der Meinung, dass mangels einer spezialgesetzlichen Grundlage die allgemeinen datenschutzrechtlichen Regelungen gelten. Einsichtsrechte können nur gewährt werden, wenn eine Einwilligung der Betroffenen vorliegt oder aber wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Keine dieser Ausnahmeregelungen des § 6 Abs. 1 BlnDSG wurde als zutreffend angesehen.

Lediglich im Klagefall können Behindertenvertreter Einsichtsrechte für sich beanspruchen, und zwar dann, wenn auf diesem Wege bestimmte Maßnahmen der Behörde angefochten werden. Nach § 15 Landesgleichstellungsgesetz (LGG) steht dem Behindertenbeirat ein außerordentliches Klagerecht zu. Sofern eine Klage beabsichtigt ist, können personenbezogene Daten dem Beirat gegenüber offen gelegt werden.

In einem Bezirksamt ist vorgesehen, zur raschen Alarmierung der Hausmeister in Notfällen (z. B. bei Einbruch, Wasserrohrbruch, Stromausfall) außerhalb der regulären Arbeitszeiten eine Liste mit den Wohnanschriften und privaten Telefonnummern der Hausmeister zu erstellen. Dabei wurde die Frage aufgeworfen, ob und unter welchen Voraussetzungen die Datenerhebung zulässig sei. Das ASOG kommt als Spezialregelung nicht zur Anwendung, da die Hausmeister nicht als Ordnungsbehörde tätig werden. Bleibt die Regelung des § 6 Abs.1 Satz 2 BlnDSG, die stets einer restriktiven Auslegung bedarf, um den schutzwürdigen Belangen Betroffener Rechnung zu tragen. In dem diskutierten Fall war deshalb für die Erhebung der Hausmeisterdaten eine ausdrückliche Rechtsgrundlage oder aber die Einwilli-

gung der Betroffenen erforderlich, andernfalls wäre die Erhebung unzulässig. Gestützt wird dies durch den Vergleich mit den Regelungen der §§ 56 ff. LGG, wonach Auskünfte aus Personalakten nur in den gesetzlich bestimmten Fällen und ansonsten nur mit ausdrücklicher Einwilligung zulässig sind.

Wenn § 28 Abs. 1 Nr. 1 BDSG als Rechtsgrundlage für die Datenerhebung herangezogen werden soll, sie also im Rahmen der Zweckbestimmung eines Vertragsverhältnisses erfolgen soll, muss eine arbeitsrechtliche (bzw. dienst- oder tarifrechtliche) Verpflichtung der Hausmeister zur Arbeitsleistung in den genannten Notfällen erforderlich sei. Ferner muss die private Erreichbarkeit der Betroffenen unverzichtbare Voraussetzung für die Erfüllung dieser Vertragspflicht sein. Lässt sich dies im konkreten Einzelfall nicht feststellen, so kommt nur die Einwilligung der Betroffenen als Grundlage der Datenerhebung in Betracht.

In einer anderen Sitzung wurde über die Änderung des Katastrophenschutzgesetzes (KatSG) diskutiert, die nunmehr auf den Weg gebracht wurde. Die beabsichtigte Gesetzesänderung sieht eine Neufassung von § 4 Abs. 3 und Abs. 4 KatSG vor, wonach die Erhebung der Namen, Vornamen, Anschriften und privaten Telefonnummern einschließlich Mobilfunknummern von Mitarbeitern ermöglicht werden soll, soweit dies zur Vorbereitung von Katastrophenfällen erforderlich ist. Von uns wurde zu bedenken gegeben, dass eine verdeckte Erhebung von Daten – ohne Kenntnis des Betroffenen – unter Rückgriff auf das IT-Verfahren IPV nach § 4 Abs.4 Satz 2 des Gesetzentwurfs unzulässig ist.

Mit der geplanten Gesetzesänderung wird nunmehr eine besondere Rechtsgrundlage zur Datenerhebung geschaffen. Zugleich wurde auch auf ein mögliches praktisches Abgrenzungsproblem bei der Umsetzung hingewiesen. Katastrophenbehörden sind Ordnungsbehörden. Nur deren Mitarbeiter, nicht aber Mitarbeiter der Leistungs- oder der allgemeinen Verwaltung kommen für die Heranziehung in Betracht.

Erste Koordinierungsbesprechung der behördlichen Datenschutzbeauftragten der Amtsgerichte

Auf Anregung aus dem Kreis der behördlichen Datenschutzbeauftragten der Amtsgerichte haben wir zu einer konstituierenden Koordinierungsbesprechung eingeladen. Die außerordentlich rege Teilnahme machte deutlich, dass der Erfahrungsaustausch als notwendig angesehen wurde.

Einen Schwerpunkt der Diskussion bildete wieder das Thema Zeitbudget, das den Datenschutzbeauftragten für ihre Tätigkeit zur Verfügung steht. Durchgängig alle Anwesenden legten dar, dass sie die Aufgaben nur neben ihrer eigentlichen Haupttätigkeit mit unbestimmten Zeitbudget wahrnehmen. Für die Untersuchung akuter Datenschutzverstöße oder die Bearbeitung von Eingaben der Petenten wird den behördlichen Datenschutzbeauftragten in der Regel das erforderliche Zeitbudget zugestanden, weil hier negative Außenwirkung zu befürchten ist. Will der Datenschutzbeauftragte jedoch Schulungen für die Mitarbeiter oder aber auch Kontrollgänge zur Überprüfung der technisch-organisatorischen Maßnahmen nach § 5 BlnDSG durchführen, ist den Vorgesetzten dieser Zeitaufwand zu hoch und sie zeigen wenig Verständnis für diese ebenfalls wichtigen Aufgaben. Hier bedarf es offenbar noch erheblicher Überzeugungsarbeit, damit die Führungsebene - nicht nur in den Amtsgerichten - die behördlichen Datenschutzbeauftragten bei ihren gesetzlichen Aufgaben unterstützt.

4.8.2 Netzwerksicherheit in einem Bezirksamt

Die Kontrollen der Netzwerksicherheit in den Bezirks- und Senatsverwaltungen wurden in diesem Jahr mit der Kontrolle eines großen Fusionsbezirks fortgesetzt. Erneut ging es darum, inwieweit die Regelungen der §§ 3 a und 5 BlnDSG und die Vorgaben der IT-Sicherheitsrichtlinie und der IT-Sicherheitsstandards des Landes Berlin eingehalten werden.

Schwerpunkt dieser Kontrolle war die Sicherheit der installierten Firewalls. In dem Bezirksamt wird eine dezentrale Firewall in den Rathausnetzen der beiden fusionierten Altbezirke betrieben, wobei das Regelwerk anlassbezogen durch einen Administrator bei Bedarf angepasst wird. Für einen wirksamen Schutz reicht allein das Vorhandensein einer Firewall nicht aus. Neben der Gewährleistung der anlassbezogenen Änderung der Firewallregeln durch die Administration, müssen auch die Protokolle der Firewall ausgewertet werden, um auf neue Gefährdungen vorbereitet zu sein. Außerdem sollte ein Notfallplan vorhanden sein, der die Vorgehensweise bei festgestellten Angriffen festlegt. Für die fehlende Auswertung der Protokolle wurde Personalmangel als Grund angegeben; ob aus dem gleichen Grunde auch ein Notfallplan fehlt, bleibt dahingestellt.

Ein weiterer Schwerpunkt war die Umsetzung der dezentralen Virenschutzkontrolle im Bezirksamt. Es bestand Einigkeit, dass ein zentraler Virenschutz am Übergangspunkt vom Internet zum Berliner Landesnetz keinen ausreichenden Schutz bietet. Zwar wird auf einem Server des Bezirksamtes ein zentraler Virenschutz betrieben. Jedoch befand sich dieser Server an einer für diese Aufgabe nicht geeigneten Stelle im Netz. Grundsätzlich sollte der

zentrale Virenschutz in einem Netzwerk so installiert sein, dass der Datenaustausch mit externen Systemen überprüft werden kann. Die IT-Sicherheitsstandards geben vor, dass alle Dateiserver im Hintergrund gegen Virenbefall überwacht werden müssen. Auch alle Endgeräte, die ausnahmsweise mit Datenträgerlaufwerken ausgestattet sind, sollten mit einer entsprechenden Virenschutzsoftware ausgestattet sein, was in diesem Bezirksamt auch zutraf.

Im Gegensatz zur Praxis in dem Bezirksamt sollte die Aktualisierung der Virendefinitionen dem Stand der Technik entsprechen. Ein Virenschutzkonzept, zu dem auch ein Notfallplan für den Fall eines Virenbefalls gehört, war nicht vorhanden.

Auch bei der Anbindung der lokalen Netze von Außenstellen an das Bezirksamtsnetz spielt die Sicherheit der Datenübertragung zur Gewährleistung der Vertraulichkeit und Integrität der Daten eine nicht zu vernachlässigende Rolle. Dies kann entweder dadurch erreicht werden, dass ein Zugriff durch Unbefugte auf die Kommunikationsleitung verhindert wird, oder dadurch, dass die Daten bei der Übertragung durch geeignete Verfahren verschlüsselt werden. Das erfolgte aus Kostengründen nicht.

In einer Abteilung des Bezirksamtes wurde ein Server betrieben, der von einer fremden Firma im Rahmen einer Fernwartung gewartet wurde. Eine vertragliche Regelung dieser Fernwartung bestand nicht. § 3 a BlnDSG, der die Wartung und Fernwartung von informationstechnischen Systemen in der Berliner Verwaltung besonders regelt, wenn in den Systemen personenbezogene Daten verarbeitet werden, wurde außer Acht gelassen.

Auf unseren Kontrollbericht erfolgte eine Stellungnahme der IT-Stelle, die sich trotz aller Bemühungen außer Stande sah, die wesentlichsten Mängel, zu den auch das Fehlen eines behördenspezifischen Sicherheitskonzepts nach den Vorgaben der IT-Sicherheitsrichtlinie gehörte, zu beseitigen. Es fehlte der notwendige Rückhalt der Behördenleitung, die Datenschutz und IT-Sicherheit nur eine untergeordnete Priorität zumessen will.

4.8.3 Der Einsatz von Firewalls

Der zunehmende Grad der Vernetzung von Rechnern und Rechnersystemen und die Erweiterung des Leistungsspektrums von Einzelplatzsystemen machen die Datensicherheit zu einem zentralen Thema. Unter dem Eindruck der beträchtlichen Schäden, die verbreitete Viren hervorriefen, wurden selbst Privatleute mit ihren PCs auf einmal „Betroffene“, die nach Sicherheitsfunktionen wie Virenscannern oder Firewallsystemen riefen.

In den letzten beiden Jahren durchgeführte Kontrollen zeigten, dass nicht jede Verwaltung den Einsatz von Firewallsystemen zum Schutz der eigenen Netze für notwendig hält, obwohl er in den IT-Sicherheitsstandards spätestens seit 2002 vorgeschrieben wurde.

Aber selbst wenn die Verwaltungen über entsprechende Systeme verfügen, so sind die Rahmenbedingungen oft unzureichend. Wir stellten dabei hauptsächlich im organisatorischen Umfeld Mängel fest. So fehlte für die Administration der Firewall oft eine Vertretung bzw. eine Vertretungsregelung. Die Auswertung der Protokolle war in vielen Fällen unzureichend, da sie nur sporadisch oder überhaupt nicht erfolgte. Die Protokollauswertung ist aber ein unverzichtbarer Bestandteil der Administration einer Firewall und wirkt sich wesentlich auf die Schutzwirkung aus.

Meistens wurde auch kein Notfallplan erstellt, der im Falle eines Angriffes die notwendigen Maßnahmen festlegt. Der Notfallplan sollte immer Teil eines allgemeinen Firewall-Betriebskonzepts sein, welches als Teil des behördlichen Sicherheitskonzepts anzusehen ist.

Eine Firewall ist eine definierte und kontrollierte Schnittstelle zwischen einem schutzbedürftigen und einem weniger vertrauenswürdigen Netz. Das wichtigste Beispiel ist die Schnittstelle zwischen lokalen Systemen (vor allem lokalen Netzen) und dem Internet. In der Berliner Verwaltung finden sich als Beispiele die Schnittstellen zwischen dem Berliner Landesnetz und dem Internet sowie zwischen den lokalen Behördennetzen und dem Berliner Landesnetz.

Im zu schützenden Netz bestehen ein einheitlicher Mindest-Schutzbedarf und ein einheitliches Mindest-Sicherheitsniveau. Soweit Teilnetze höheren Schutzbedarf aufweisen, sind mit Firewalls auch die erhöhten Sicherheitsanforderungen zu erfüllen. Eine Firewall stellt einen Schutzwall für lokale Netze gegen Angriffsversuche dar, die über einen Anschluss an öffentliche Netze erfolgen. Ähnlich einem Grenzkontrollpunkt erlaubt sie den Zugang zum geschützten System nur über eine definierte Stelle. Damit lässt sich der gesamte Datenverkehr kontrollieren, der von innen und von außen über die Schnittstelle fließt. Ohne Firewallbetrieb sind die zahlreichen Rechner einer Organisation, die unter diversen Betriebssystemen laufen, direkt aus dem öffentlichen Netz erreichbar. Eine Firewall kanalisiert dagegen die Kommunikation und erhöht damit die Chancen, einen Angriffsversuch anhand ausführlicher Protokoll-Dateien zu erkennen.

Die Firewalltechnologie befindet sich in einer stetigen Weiterentwicklung. Die einfachste Technik ist der so genannte „Paketfilter“.

Ein Paketfilter kontrolliert den eingehenden und ausgehenden Netzverkehr anhand folgender Kriterien: IP-Quelladresse, IP-Zieladresse, Protokoll (z. B. TCP, UDP, ICMP), Quellport, Zielport, ICMP-Nachrichtentyp. Er überprüft die Quell- und Zieladresse (IP-Adresse und Port) eines IP-Pakets und entscheidet, ob es passieren darf oder nicht. Dieses für den Anwender recht transparente Verfahren hat allerdings den Nachteil, dass damit nicht zwischen verschiedenen Nutzern und ihren Rechten unterschieden werden kann. Auch die Inhalte der IP-Pakete werden nicht kontrolliert. Viren oder u. U. risikobehaftete aktive Elemente in Webseiten (z. B. Javascript oder Active X) können somit nicht von einfachen WWW-Seiten unterschieden werden. Auch können fremde Dienste über zugelassene Ports „geschmuggelt“ werden (Tunneling).

Ein anderes weit verbreitetes Firewall-Konzept sind die Application Gateways, auch Proxy (Stellvertreter) genannt. Hierbei wird auf dem Firewall-Rechner für jede zulässige Anwendung ein eigenes Gateway-Programm installiert. Der Client oder auch der Nutzer muss sich dabei gegenüber dem Proxy-Programm authentifizieren. Dieser Proxy führt dann alle Aktionen im LAN stellvertretend für den Client aus. Damit lassen sich zum einen benutzerspezifische Zugangsprofile (welche Zeiten, welche Dienste, welche Rechner) erstellen, zum anderen kann man die Festlegung der zulässigen Verbindungen anwendungsbezogen vornehmen. Die daraus resultierenden separaten kleinen Regelsätze bleiben besser überschaubar als der komplexe Regelsatz eines Paketfilters. Application Gateways sind typische Vertreter der „Verboten-was-nicht-erlaubt“-Strategie und als die sicherste, aber auch aufwendigste Lösung einzuschätzen.

Server, die von außen zugänglich sein sollen, können in eine so genannte *demilitarisierte Zone* (DMZ) gestellt werden. Die Zugriffe in diese Zone von außen können somit noch besser kontrolliert werden und müssen gar nicht erst nicht in das interne Netz durchgeleitet werden.

Da beim Proxy alle Zugriffe nach außen über eine Instanz laufen, kann man den Proxy gleichzeitig als Cache (Pufferspeicher) benutzen. Der Proxy speichert alle erhaltenen WWW-Seiten zwischen, so dass er bei einem erneuten Zugriff auf eine solche Seite von einem beliebigen Anwender keine erneute Verbindung nach außen aufbauen muss.

Ein Proxy bietet aber auch die Möglichkeit, das „Surfverhalten“ der Anwender zu analysieren. Hier muss der Administrator sehr genau die bestehende Rechtslage, insbesondere die Rechte der Arbeitnehmer, berücksichtigen. Nicht in jedem Fall sind die Kontrollwünsche der Leitungsebene mit dem geltenden Recht vereinbar.

Eine Firewall setzt eine Sicherheitspolitik (Security Policy) voraus, die für das zu schützende Netz definiert wurde. In diese Definition müssen alle Anforderungen aller vernetzten Stellen einfließen. Grundsätzlich existieren zwei Arten, Regeln eines Firewall zu definieren:

Zum einen können bestimmte Kommunikationswege und -formen *verboten* werden, so dass alles andere als erlaubt angesehen werden kann. Der Vorteil dieser Lösung liegt in seiner einfachen Handhabung und der Benutzerfreundlichkeit, da neue Dienste automatisch erlaubt sind. Der Administrator sperrt nur die nach seiner Meinung „gefährlichen“ Ports. Der Nachteil dieses Ansatzes liegt in der hohen Belastung des Administrators, der das Verhalten von Anwendungen und Programmen ständig beobachten muss, um rechtzeitig Gegenmaßnahmen treffen zu können.

Dieser Sicherheitsansatz findet oft in hardwarebasierten Routern Verwendung, die handelsüblich für den Internetzugang über DSL-Technologie angeboten werden. Aus datenschutzrechtlicher Sicht ist dieser Ansatz nur für den Heimanwender sinnvoll. Für alle anderen sollte der alternative Sicherheitsansatz Verwendung finden. Dieser *erlaubt* bestimmte Kommunikationswege und -formen, so dass alle übrigen als verboten anzusehen sind. Der Vorteil liegt in dem sehr viel höheren Maß an Sicherheit, da Zugriffe auf unbekannte Ports unterbunden werden, die aus Sicherheitslücken im Betriebssystem und Anwendungsprogrammen stammen.

Der Nachteil dieser Strategie ist, dass sie von Nutzern als hinderlich angesehen werden, da der Wunsch zur Nutzung neuer Dienste nur umständlich erfüllt werden kann. Außerdem muss vor Einrichtung einer Firewall eine Kommunikationsanalyse durchgeführt werden, um die Funktionalität aller benötigten Dienste sicherzustellen. Trotz dieser Flexibilitätsnachteile ist der zweite Ansatz aus Sicherheitserwägungen zu bevorzugen.

Gleichwohl ist festzuhalten, dass keine Firewall einen absoluten Schutz gegen unbefugtes Eindringen in ein System gewährleisten kann. Sie kann lediglich einen Einbruch erschweren und damit auch unwahrscheinlicher machen. Sie kann Angriffe oder deren Versuche auf niedriger Protokollebene feststellen, meist abblocken, teilweise auch protokollieren und zurückverfolgen; gegen Angriffe auf höherer Ebene ist sie jedoch nutzlos. Eine Firewall kann

Viren oder schädliche aktive Komponenten nicht filtern, denn dazu müsste jedes einzelne Datenpaket aufwendig untersucht werden. Mittlerweile existieren zusätzliche Applikationen, die die Firewall ergänzen. Deren Einsatz erfordert jedoch ein hohes Maß an Ressourcen und schützt nur die Kommunikationswege vor entsprechenden Angriffen. Verschlüsselte Kommunikation (z. B. HTTPS) bzw. verschlüsselte Inhalte (z. B. mit GnuPP verschlüsselte E-Mails) können damit nicht geprüft werden.

Gegen Angriffe, die innerhalb des zu schützenden Netzes erfolgen, kann eine Firewall naturgemäß nicht wirken, da sie ja nur den Verkehr von und nach außen kontrolliert. Hier müssen andere Schutzsysteme, z. B. Intrusion Detection Systeme, greifen, die den internen Datenverkehr auf außergewöhnliche und damit prüfbedürftige Ereignisse überwachen.

Schutz kann eine Firewall auch nur dann bieten, wenn die gesamte Kommunikation mit externen Systemen über diese Firewall abgewickelt wird. Ein einziger zusätzlicher Kommunikationskanal (z. B. Modem) reicht aus, um das gesamte Netz zu gefährden, da so die Firewall umgangen werden kann.

Aus den beiden letzten Argumenten ist zu ersehen, dass das größte Risikopotenzial von den *Menschen* ausgeht, die mit und in dem Netz arbeiten, denn durch Unwissenheit und Leichtgläubigkeit können sie einem Angreifer viele Möglichkeiten des Eindringens öffnen. Die Entwicklung von Schutzmechanismen bleibt immer einen Schritt hinter den Möglichkeiten der Angriffmechanismen zurück, denn bevor die Entwickler einer Firewall einen Schutzmechanismus erstellen können, müssen sie wissen, gegen welche Art des Angriffs geschützt werden muss.

Um in ein Netz, bzw. in gesicherte Netzbereiche einzudringen, können von Angreifern verschiedene Methoden angewendet werden. Öffentlich diskutiert werden dabei mehr die Angriffe von außen, also von Hackern. Häufiger sind jedoch Angriffe von innen, wenn z. B. aus Frust und Enttäuschung Mitarbeiter verleitet werden, der eigenen Firma Schaden zuzufügen oder aus Gewinnsucht wichtige Daten an ein Konkurrenzunternehmen zu verkaufen.

Wir beschränken uns an dieser Stelle auf Angriffsformen von außen, da nur bei solchen Angriffen Firewalls eine wirksame Schutzmaßnahme sein können.

Beim IP-Spoofing wird mit Hilfe einer falschen IP-Nummer dem angegriffenen System eine falsche Identität vorgetäuscht. Die gegenseitige Identifikation von zwei kommunizierenden Netzen oder Systemen erfolgt bei den meisten TCP/IP-Protokollen ausschließlich über die

IP-Adresse. Im Internet sind jedoch sehr viele "Hackertools" als Freeware erhältlich, die es ermöglichen, eine falsche IP-Adresse vorzutäuschen. Gute Firewallsysteme bieten Schutzmechanismen gegen das IP-Spoofing, jedoch oft gibt es Fälle, bei denen dieser Mechanismus durch fehlerhafte Administration nicht aktiviert wurde.

Eine einfache Angriffsmethode besteht im Versand von Datenpaketen mit einem unbekannten IP-Paketheader an einen der Netzserver des zu attackierenden Netzes. Der Server interpretiert diesen Header falsch, und wird so zu unvorhergesehenen Reaktionen verleitet. Infolge dieser Reaktionen ist es dem Angreifer dann möglich, in das System einzudringen.

Es ist möglich, einem IP-Paket die Route, die es nehmen soll, um ans Ziel zu gelangen, vorzugeben. Ebenso ist es möglich, die Route vorzugeben, die das Antwortpaket zu nehmen hat. Während der Übertragung besteht jedoch die Möglichkeit, die Wegvorgaben zu manipulieren, sodass nicht der vorgeschriebene, sichere Weg (z. B. über die Firewall) genommen wird, sondern ein oder mehrere unkontrollierte Wege.

Diese und noch weitere Angriffsformen, die hier nicht näher behandelt werden sollen, zeigen, dass es selbst bei bestem Firewallschutz ein absolut sicheres Netz nicht gibt und niemals geben wird. Eine ausgereifte Sicherheitspolitik verlangt, dass ein Sicherheitsmanagement dafür sorgt, dass die getroffenen Maßnahmen - und dazu gehören auch die Sicherheitseinstellungen der Firewalls – regelmäßig überprüft und verbessert werden. Auch die Kommunikationsanalyse, mit der erfasst wird, welche Anwendungen welche Kommunikationswege benutzen, bedarf der häufigen Wiederholung, da sich die Anforderungen schnell ändern können. Das Regelwerk, welches die Funktion der Firewall steuert, muss dann angepasst werden; auch muss neu festgelegt werden, was wie, wo und wann protokolliert wird.

4.8.4 Postdienstleistungen und Datenschutz

> *Beim Landesverwaltungsamt fällt sehr viel Briefpost an. Aus Kostengründen lässt es die Post nicht mehr durch die Deutsche Post AG, sondern durch einen anderen privaten Anbieter ausliefern. Seitdem erreichen uns regelmäßig Beschwerden über Unzulänglichkeiten.*

Das Landesverwaltungsamt hat uns im Sommer 2002 dazu mitgeteilt, dass in einer Pilotanwendung festgestellt werden soll, ob dieser private Anbieter neben der notwendigen Fachkunde auch die für derartige Dienstleistungen erforderliche Zuverlässigkeit besitzt. Bei Qualitätsprüfungen wurden Beschwerden über die Briefzustellung bekannt, die allerdings nach Gesprächen mit

dem Aufsichtsrat bzw. dem Vorstand ausgeräumt werden konnten. Jedoch wurden in einigen Postzustellbezirken erhebliche Probleme bekannt, die zu Entlassungen der jeweils zuständigen Zusteller führten. In einem Fall musste sogar Strafanzeige gegen einen Zusteller gestellt werden, weil dieser den Verbleib der nicht zugestellten Postsendungen nicht offenbart hatte.

So wurde uns wiederholt vorgetragen, dass Lohnsteuerkarten oder Bescheide der Beihilfestelle mit Arztrechnungen verloren gegangen seien. Nicht selten konnte der Vorgang dann nicht nachvollzogen oder nicht mehr geklärt werden.

In einem Fall hat ein Hausbewohner bei der Entsorgung seines Hausmülls etwa 100 Briefe in der Mülltonne gefunden. Der private Anbieter hat dazu erklärt, dass die Briefsendungen einem Kooperationspartner übergeben wurden. Dieser war allerdings nicht anwesend, so dass keine persönliche Übergabe erfolgen konnte; die Sendungen wurden vor der Haustür abgelegt und waren somit unbeaufsichtigt. Offensichtlich haben Unbekannte die Post dann in die Mülltonne geworfen.

Der Datenschutz für private Postunternehmen wird durch das Postgesetz und die Verordnung über den Datenschutz für Unternehmen, die Postdienstleistungen erbringen, geregelt. Danach ist der Bundesbeauftragte für den Datenschutz Aufsichtsbehörde. Eine öffentliche Stelle des Landes, die sich einer solchen Dienstleistung bedient, hat jedoch für eine ordnungsgemäße Auftragserfüllung zu sorgen. Im vorliegenden Fall hat das Landesverwaltungsamt mit der Kündigung des Vertragsverhältnisses gedroht.

4.9 Informationsfreiheit

4.9.1 Jahr der Informationsfreiheit

Um die Informationsfreiheit als wichtiges Instrument der Teilhabe an politischen Entscheidungen mehr in den Mittelpunkt der öffentlichen Wahrnehmung zu rücken, hatte die Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands (AGID), der die bisher bestehenden Informationsfreiheitsbeauftragten angehören, 2003 zum Jahr der Informationsfreiheit ausgerufen. Vier größere Veranstaltungen der Informationsbeauftragten von Nordrhein-Westfalen, Berlin, Brandenburg und Schleswig-Holstein, die sich unterschiedlichen Schwerpunkten widmeten, standen im Mittelpunkt.

Den Anfang machte die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen mit einem Sommersymposium „Informationsfreiheit“ am 23. Juli 2003 im

Plenarsaal der Bezirksregierung Düsseldorf. Die Veranstaltung schlug einen Bogen von den historischen Wurzeln der Informationsfreiheit über ihre verfassungsrechtlichen Grundlagen bis hin zur Verwaltungspraxis. Ein Erfahrungsbericht unserer Dienststelle, der anhand von Beispielen die Reichweite und Grenzen der Informationsfreiheit illustrierte, wurde ergänzt durch einen Vortrag über die weltweite Verbreitung der Informationsfreiheit. Einen Aspekt des erklärten Ziels von Informationsfreiheitsgesetzen, die Kontrolle staatlichen Handelns zu ermöglichen, beleuchtete ein Vorstandsmitglied von Transparency International in seinem das Symposium beschließenden Vortrag, der auf die Möglichkeiten und Potenziale der Informationsfreiheit im Dienste der Korruptionsbekämpfung einging.

In langjähriger Tradition veranstaltete unsere Dienststelle im Rahmen der Internationalen Funkausstellung wieder ein Symposium, das sich in diesem Jahr in die Reihe der Veranstaltungen zum Jahr der Informationsfreiheit einfügte. Es stand unter der Überschrift „Informationsfreiheit und Datenschutz im Internet“. Neben der von Prof. Dr. Friedrich Schoch, Universität Freiburg, behandelten grundsätzlichen Fragestellung, wie die Zielvorstellungen von Datenschutz und Informationsfreiheit insbesondere im Zeitalter der elektronischen Informationsvermittlung miteinander harmonisiert werden können, berichteten internationale Referenten über ihre Erfahrungen bei der Umsetzung und Nutzung von Informationsfreiheitsgesetzen.

Marc Rotenberg, Direktor der renommierten amerikanischen Bürgerrechtsorganisation „Electronic Privacy Information Center“ erläuterte anhand praktischer Beispiele die Möglichkeiten und Grenzen des amerikanischen *Freedom of Information Act (FOIA)* im Hinblick auf die Durchsetzung und Thematisierung von Bürger- und Freiheitsrechten. Für die Arbeit seiner Organisation stellt dieser eine der wichtigsten Grundlagen dar, um Informationen von staatlichen Stellen zu erhalten. Unverzichtbar sind diese beispielsweise für Gerichtsverfahren, mit denen Einschränkungen von Bürgerrechten angegriffen werden. Die weitreichende Informationstätigkeit von EPIC in den Bereichen von Datenschutz und Informationsfreiheit wäre überdies ohne die Zugangsrechte nach dem FOIA auf der einen Seite und das Internet auf der anderen nicht denkbar. Über den Einfluss, den die Terroranschläge des 11. September 2001 auf die Einschränkungen in der Informationszugangspolitik der US-Regierung hatte, referierte Gina Stevens, Anwältin und Mitarbeiterin des Congressional Research Service der Library of Congress, der Nationalbibliothek der USA, in Washington D.C.

Die Datenschutzbeauftragten der Republik Irland und Argentiniens, Joe Meade und Prof. Dr. Juan Antonio Travieso gingen auf das Verhältnis von Informationsfreiheit und Datenschutz in ihren Ländern ein und berichteten über deren gesetzliche Entwicklung. Privatdozent Dr. Her-

bert Burkert beleuchtete einen besonderen Aspekt der Informationsfreiheit, der auch im Rahmen der europäischen Gesetzgebung eine immer größere Rolle spielt, die Kommerzialisierung öffentlicher Informationen.

In seinem Beitrag, der sich mit dem Gesetzgebungsverfahren für ein Informationsfreiheitsgesetz des Bundes befasste, äußerte Jörg Tauss, Mitglied der SPD-Fraktion im Deutschen Bundestag, die Hoffnung, dass noch im Jahr 2003 ein neuer Referentenentwurf in die parlamentarische Beratung eingebracht wird.

Am 10. und 11. November 2003 veranstaltete der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg ein internationales Symposium „Informationsfreiheit und Datenschutz – Transparenz und E-Government in Mittel- und Osteuropa“ in Potsdam. Auch diese Veranstaltung war Teil einer im zweijährigen Rhythmus stattfindenden Tagungsreihe. Als östlichstem Bundesland kam es Brandenburg zu, hier den Bogen nach Ost- und Mitteleuropa zu schlagen. Referenten aus Estland, Slowenien, der Ukraine, der Türkei sowie aus der Schweiz stellten die dort entwickelten rechtlichen Grundlagen und elektronischen Behördendienste vor und referierten über Hindernisse und Probleme bei deren Umsetzung. Deutlich machten diese Vorträge, dass E-Government ein wichtiges Instrument für einen umfassenden Informationszugang der Bürgerinnen und Bürger darstellt, es sich gleichzeitig jedoch auch datenschutzrechtlichen Herausforderungen stellen muss, um von ihnen akzeptiert zu werden.

Als Informationsbeauftragter des nördlichsten Bundeslandes richtete das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein mit seinem Symposium, das gemeinsam mit dem Präsidenten des schleswig-holsteinischen Landtages veranstaltet wurde, seinen Blick nach Skandinavien. Unter dem Titel „Informationsfreiheit – Vom Norden lernen“ kamen Vertreter Schwedens, Dänemarks und Finnlands zu Wort, um über ihre Erfahrungen, die zumindest in Schweden schon über Jahrhunderte bestehen, zu berichten. Dass diese Erfahrungen auch für andere Erdteile wertvoll sind, machte der Vortrag eines thailändischen Universitätsprofessors deutlich, der über das thailändische Informationsfreiheitsgesetz referierte – unter der Überschrift: „Vom Norden gelernt“.

Gründung der Internationalen Konferenz der Informationsbeauftragten (ICIC)

Ein besonderer Höhepunkt des Jahres der Informationsfreiheit war das erstmals stattfindende internationale Treffen von Informationsbeauftragten am 7. April 2003 in Berlin, zu dem wir

gemeinsam mit dem brandenburgischen Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht eingeladen hatten. Im Mittelpunkt der Beratungen stand ein erster Erfahrungsaustausch über die Einführung und Anwendung von Informationsfreiheitsgesetzen in den jeweiligen Ländern. Die Teilnehmer erhielten einen Überblick über die Organisation der verschiedenen Dienststellen und die rechtlichen Grundlagen ihrer Arbeit. Die Vorträge illustrierten auch die verschiedenartigen Ansatzpunkte der jeweiligen Gesetze, die den historischen und politischen Umständen ihrer Verabschiedung wie auch der Rechtstradition in den teilnehmenden Ländern geschuldet sind.

Die Informationsbeauftragten vereinbarten eine regelmäßige Kooperation. Als Grundlage hierfür verabschiedeten sie eine Deklaration der Zusammenarbeit, die in der Berliner Sitzung durch Vertreter von 14 Institutionen aus 11 Ländern unterzeichnet wurde. Diese ständige Internationale Konferenz der Informationsbeauftragten soll auch Kollegen in anderen Ländern offen stehen und nach der bisherigen Planung zumindest einmal jährlich zu einem Arbeitstreffen zusammenkommen. Im Frühjahr 2004 wird sich die Konferenz mit Standards für Ausnahmetatbestände der Informationsfreiheit und Fragen der Einbeziehung Privater in den Anwendungsbereich von IFG befassen. Gastgeber wird die Human Rights Commission der Republik Südafrika sein.

4.9.2 Stillstand in der Bundes- und Landesgesetzgebung

Zum dritten Mal in Folge beginnt unser Berichtsteil zur Informationsfreiheit mit der Feststellung, dass das lang erwartete Informationsfreiheitsgesetz des Bundes auch im letzten Jahr nicht Wirklichkeit geworden ist. Trotz einzelner Initiativen innerhalb der Koalitionsfraktionen und hoffnungsvoller Ankündigungen von Mitgliedern des Bundestages, dass noch im Jahr 2003 Bewegung in den Gesetzgebungsprozess kommen würde, lag bis zum Ende des Jahres ein Referentenentwurf nicht vor. Daher fällt es schwer, wie in den vergangenen Jahren eine Prognose abzugeben oder gar Hoffnung zu äußern, wann und ob der Bundesgesetzgeber sich zur Verabschiedung eines Informationsfreiheitsgesetzes durchringen wird. Leider schlägt sich dieser Stillstand auf Bundesebene auch auf die in wenigen Bundesländern noch anhängigen Gesetzgebungsverfahren nieder. Es muss festgestellt werden, dass auch dort die Informationsfreiheit auf der Prioritätenliste der politischen Entscheidungsträger weit abgeschlagen ist.

4.9.3 Weitere Erfahrungen

Auch das Berliner Informationsfreiheitsgesetz hat Mängel vor allem gesetzestechnischer Art. Diese müssen, ebenso wie ähnliche Mängel des neuen Berliner Datenschutzgesetzes, demnächst beseitigt werden. Das Abgeordnetenhaus hat dies zum Anlass genommen, einen früheren Vorschlag von uns aufzugreifen und die Senatsverwaltung für Inneres zu bitten zu überprüfen, ob beide Gesetze nicht in einem Informationsgesetzbuch zusammengeführt werden könnten[137].

Trotz einer skeptischen, allerdings mehr von Arbeitsscheu als von inhaltlich überzeugenden Argumenten getragenen Einstellung der Innenverwaltung[138] soll dieses Projekt im laufenden Jahr in Angriff genommen werden.

Preisgestaltung: Betriebs- oder Geschäftsgeheimnis?

> *Ein Student der Humboldt-Universität Berlin hatte zunächst aus datenschutzrechtlichen Erwägungen Anstoß an der Praxis der Video- und Tonüberwachung von Vorlesungssälen genommen. Danach interessierte ihn aber auch die Rechtmäßigkeit der Vergabe des Installationsauftrages für die Anlage und er bat um Einsicht in die entsprechenden Unterlagen. Die Universität stellte ihm umfangreiche Materialien zur Verfügung, schwärzte jedoch mit dem Hinweis auf Betriebs- und Geschäftsgeheimnisse des Auftragnehmers sämtliche Angaben zur Preisgestaltung. Hiergegen wandte sich der Petent und bat um Unterstützung bei der Durchsetzung seines Akteneinsichtsanspruchs.*

Das IFG verzichtet wie auch andere Bestimmungen zum Schutz von Betriebs- und Geschäftsgeheimnissen[139] auf deren begriffliche Definition. Gleichwohl hat sich in der Literatur und Rechtsprechung eine einheitliche Auffassung entwickelt, welche Kriterien erfüllt sein müssen, um vom Vorliegen eines solchen Geheimnisses ausgehen zu können. Danach ist ein Betriebs- und Geschäftsgeheimnis jede Tatsache,

- die im Zusammenhang mit einem wirtschaftlichen Geschäftsbetrieb steht,
- die nicht offenkundig, d. h. nur einem begrenzten Personenkreis bekannt ist,

---

[137] Abghs.-Drs. 15/1056
[138] Abghs.-Drs. 15/1693 und 15/2123
[139] § 17 Gesetz gegen den unlauteren Wettbewerb (UWG), § 30 Abgabenordnung, § 30 VwVfG, § 8 Umweltinformationsgesetz (UIG)

- die nach dem (ausdrücklichen oder konkludenten) Willen des Unternehmers geheim gehalten werden soll und
- an deren Geheimhaltung ein berechtigtes wirtschaftliches Interesse besteht.

Insbesondere das letzte Tatbestandsmerkmal ist für die Feststellung, ob ein Betriebs- und Geschäftsgeheimnis vorliegt, ausschlaggebend. Soweit die Offenbarung von Informationen, die zwar nicht offenkundig sind, einen wirtschaftlichen Nachteil oder Schaden nicht nach sich ziehen würde, liegt ein Betriebs- oder Geschäftsgeheimnis nicht vor.

Im konkreten Fall, der Herausgabe der Angebotsunterlagen der Installationsfirma, bedeutete dies, dass zwar die Beträge zu den einzelnen Positionen des Angebots nicht offenbart werden durften, da Konkurrenten daraus Rückschlüsse auf die Geschäftsführung des Anbietenden hätten ziehen können. Die Gesamtsumme des Angebots musste dem Petenten jedoch mitgeteilt werden. Die Humboldt-Universität hat sich unserer Auffassung angeschlossen und dem Petenten die Unterlagen dementsprechend zur Verfügung gestellt.

Behördliche Genehmigung und Betriebs- und Geschäftsgeheimnisse

> *Öffentlich geförderte Pflegeheime, die ihre investiven Aufwendungen wie z. B. Renovierungskosten auf die Bewohner umlegen wollen, bedürfen hierfür einer Genehmigung durch die zuständige Sozialbehörde. Ein Petent hatte bei der Senatsverwaltung für Gesundheit, Soziales und Verbraucherschutz Einblick in die Unterlagen zur Genehmigung der gesonderten Erhebung von Entgelt für solche Aufwendungen gegenüber einer privaten Pflegeheim GmbH beantragt. Dem wurde nach unserer Einschaltung beschränkt stattgegeben, die Offenbarung der einzelnen Beträge der betriebsnotwendigen Aufwendungen (bauliche Erhaltung, Mietzins für die Räumlichkeiten) mit dem Hinweis, dass es sich hierbei um Betriebs- und Geschäftsgeheimnisse im Sinne von § 7 IFG handele, aber abgelehnt.*

Entgegen der Auffassung der Senatsverwaltung kamen wir zu dem Schluss, dass die Beträge keine Wettbewerbsrelevanz haben, da aus ihnen auf die Geschäftsführung der GmbH nicht geschlossen werden kann. Die Offenlegung der Aufwendungen bot keinen Einblick in Bilanzen und Planungen der Einrichtungen, da wesentliche Bereiche der Geschäftsführung wie Personalkosten oder Ausgaben für den täglichen und Geschäftsbedarf hiervon nicht betroffen waren. Auch handelte es sich nicht um Kalkulationen des Leistungsträgers, sondern vielmehr um tatsächlich angefallene und somit ihrem Grunde nach nachvollziehbare Auf-

wendungen, deren Summe betriebswirtschaftliche Hintergründe nicht offen legt. Da diese Kosten auf die Bewohner umgelegt werden sollen, haben sie auch keine Aussagekraft hinsichtlich etwaiger Gewinne des Unternehmens.

Die in Rede stehenden Angaben waren überdies Grundlage einer staatlichen Entscheidung, deren Nutznießer der Leistungsträger selbst ist, da die Zustimmung der Sozialverwaltung ihn unmittelbar berechtigt, die Aufwendungen auf die Bewohner umzulegen. Die Zustimmung belastete überdies auch – zumindest mittelbar – die Heimbewohner. Schon aus diesem Grunde konnte ein berechtigtes Interesse an der Geheimhaltung der Kosten dieser Aufwendungen nicht vorliegen.

Ein weiterer Aspekt unterstützt diese Rechtsauffassung: Auch in herkömmlichen Mietverhältnissen ist der Vermieter verpflichtet, seine Aufwendungen, die für die Betriebskosten oder für Umlagen von Modernisierungen von Belang sind, offen zu legen. Gerade bei den der Genehmigung zugrunde liegenden Aufwendungen sind die Parallelen zum Mietrecht augenscheinlich.

IFG im Strafvollzug

> *Die Redaktion der Gefangenenzeitschrift „Der Lichtblick“ und die Gesamtinsassenvertretung der Justizvollzugsanstalt (JVA) Tegel hatten bereits vor geraumer Zeit Einsicht in die Vertragsunterlagen der JVA mit dem Betreiber der JVA-Telefonanlage beantragt, die den Gefangenen auch für Telefonate nach außen zur Verfügung steht. Die JVA lehnte unter beträchtlichem Zeitverzug die Anträge zunächst mit dem Argument ab, bei den Antragstellern handele es sich weder um eine natürliche noch um eine juristische Person, das IFG könne daher im Hinblick auf § 3 Abs. 1 nicht als Anspruchsgrundlage herangezogen werden. Überdies stelle der Vertrag insgesamt ein Betriebs- und Geschäftsgeheimnis des Telefonanbieters dar. Schließlich gelte für die Akteneinsicht im Strafvollzug allein § 185 StVollzG.*

Nach § 3 Abs. 1 IFG hat jeder Mensch einen Einsichts- oder Auskunftsanspruch. Ausdrücklich festgehalten ist, dass dieses Recht auch von juristischen Personen geltend gemacht werden kann. Der Rückschluss der JVA, dass damit nicht-rechtsfähige Personenvereinigungen vom IFG keinen Gebrauch machen können, geht fehl. Das IFG will ausweislich seiner Begründung erstmals einen umfassenden Anspruch auf Akteneinsicht in allen Verwaltungsbereichen schaffen. Dieser umfassende Informationsanspruch kann nicht dadurch verengt

werden, dass auf die Organisationsform der Antragsteller abgestellt wird. Die ausdrückliche Nennung juristischer Personen soll vielmehr den Kreis der Anspruchsberechtigten erweitern und nicht einengen. Wir wiesen die JVA überdies darauf hin, dass der Antrag ohne weiteres auch von einer natürlichen Person hätte gestellt werden können, was im Nachgang zur Ablehnung durch einen einzelnen Gefangenen tatsächlich auch geschehen ist.

Auch ein pauschaler Verweis auf das Vorliegen von Betriebs- und Geschäftsgeheimnissen im Vertrag der JVA mit dem Telekommunikationsanbieter ist unzulässig. Betriebs- und Geschäftgeheimnisse müssen im Einzelnen als solche spezifiziert sein, ein Verweis darauf, dass der Vertrag solche enthält, ist nicht ausreichend. Überdies sieht § 12 IFG eine beschränkte Akteneinsicht vor, wenn im Einzelnen Ausschlusstatbestände der Akteneinsicht bestehen.

§ 185 StVollzG hat keinerlei Auswirkung auf die Anwendbarkeit des IFG, da diese Bestimmung ein allgemeines Akteneinsichtsrecht nicht regelt. Sie ist vielmehr Bestandteil der Regelungen zum Datenschutz in Justizvollzugsanstalten und sichert das informationelle Selbstbestimmungsrecht der Gefangenen hinsichtlich ihrer Personalakten. Ein weiter gehender Regelungsgehalt ist ihr nicht zu entnehmen. Insbesondere stellt § 185 StVollzG kein abschließendes Akteneinsichtsrecht hinsichtlich der von der Justizvollzugsanstalt geführten Akten dar.

Verstoßen wurde darüber hinaus gegen § 15 Abs. 2 und 3 IFG, wonach der Antragsteller über den Inhalt der vorenthaltenen Akte zu informieren ist und auch begründet werden muss, weshalb keine beschränkte Akteneinsicht oder Aktenauskunft nach § 12 IFG erteilt werden kann. Eine formelhafte Wiederholung des Gesetzestextes ist ebenso unzureichend.

Eine vollständige Ablehnung des Akteneinsichtsantrages war schon deshalb unzulässig, weil die Bescheide erst Monate nach Antragstellung ergangen sind, nach § 15 Abs. 5 IFG die Ablehnung des Akteneinsichtsantrages aber innerhalb von zwei Wochen zu erfolgen hat. Nach Ablauf dieser Frist können nur noch schutzwürdige Interessen Dritter (personenbezogene Daten, Betriebs- und Geschäftsgeheimnisse) als Ablehnungsgründe herangezogen werden.

Trotz der von uns mehrfach gegebenen Hinweise zur rechtmäßigen Auslegung des IFG hält die JVA Tegel an ihrer Ablehnung der Akteneinsichtsanträge fest – im Übrigen auch in den Fällen, bei denen einzelne Gefangene einen solchen Antrag gestellt hatten. Wir haben dies beanstandet.

Informationsfreiheit im Dienste des Verbraucherschutzes

Alle vier deutschen Informationsbeauftragten sind derzeit mit einer Eingabe der Bundesverbraucherzentrale befasst. Sie hatte bei den Landeseichbehörden der Länder mit IFG um Auskunft zu konkreten Beanstandungsfällen bei einer systematischen Unterfüllung von Verpackungen gebeten, da aus der veröffentlichten Füllmengenkontrollstatistik nicht erkennbar ist, welche Unternehmen regelmäßig die auf der Verpackung aufgedruckte Menge unterschreiten.

Die Berliner Landeseichbehörde hatte zunächst darauf verwiesen, dass es sich bei diesen Angaben um Betriebs- und Geschäftsgeheimnisse der Unternehmen handeln würde, deren Bekanntwerden zu einer Kaufzurückhaltung führen würde. Unbestritten ist, dass Letzteres der Fall sein könnte. Zur Auslegung der Betriebs- und Geschäftsgeheimnisse kann diese Argumentation jedoch nicht dienen. Es ist zunächst jedem Verbraucher überlassen, selbst nachzuprüfen, ob die Füllmenge den Angaben auf der Verpackung entspricht – mithin kann von einer Geheimheit nicht gesprochen werden. Überdies kann von einem berechtigten Geheimhaltungsinteresse nicht gesprochen werden, wenn ein Unternehmen systematisch weniger in seine Tüten packt, als auf der Verpackung angegeben. Das IFG stellt daher auch in § 7 Satz 2 klar, dass der Schutz von Betriebs- und Geschäftsgeheimnissen dann endet, wenn tatsächliche Anhaltspunkte für das Vorliegen einer strafbaren Handlung gegeben sind. Bei einer systematischen Unterfüllung wird man davon ausgehen können, dass ein Unternehmen Betrug am Verbraucher begeht.

Die Zurückhaltung der Landeseichbehörden kann möglicherweise darauf zurückzuführen sein, dass sie Schadensersatzforderungen fürchten, wie sie im Fall Birkel auf das Land Baden-Württemberg zugekommen waren, das wegen einer unberechtigten Warnung zu einem erheblichen Schadensersatz verurteilt wurde. Ob die Weigerung der Akteneinsicht vor diesem Hintergrund aber auch im Hinblick auf die gesetzlichen Vorgaben des IFG Bestand haben wird, wird der Ausgang eines anhängigen Gerichtsverfahrens zeigen.

Landeseigene Privatunternehmen

Zwei Eingaben befassten sich mit Akteneinsichtsanträgen gegenüber landeseigenen Unternehmen, die als GmbH tätig sind. Beide Male wurde der Antrag mit der Begründung abgelehnt, dass die Unternehmen, obwohl sie im alleinigen Eigentum des Lan-

des stehen und im weitesten Sinne öffentliche Aufgaben wahrnehmen, dem Anwendungsbereich des IFG nicht unterfallen.

Zu unserem Bedauern mussten wir beiden Petenten mitteilen, dass die Ablehnung ihres Einsichtsbegehrens zu Recht erfolgt ist. Private unterfallen dem IFG nur, wenn sie mit der Ausübung hoheitlicher Befugnisse betraut sind. Wenngleich die Unternehmen im Bereich der Daseinsvorsorge tätig sind, erfüllen sie doch keine hoheitlichen Aufgaben und sind somit auch nicht Adressaten des IFG.

Angesichts der zunehmenden Verlagerung öffentlicher Aufgaben in die Zuständigkeit privatrechtlicher Unternehmen, die zumindest mehrheitlich im Besitz des Staates sind, ist dieses Ergebnis unbefriedigend. Auch und gerade in diesen Bereichen werden öffentliche Mittel verwendet, ohne dass diese Unternehmen der gleichen Transparenz wie die Verwaltung unterliegen. Daher ist es dringend geboten, dass das IFG hier eine Klarstellung erfährt. Die Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands (AGID) hat dies gemeinsam in einer Entschließung vom Dezember 2003[140] gefordert.

Ähnlich gelagert sind die derzeit laufenden parlamentarischen Bemühungen zu einer Änderung des Petitionsgesetzes. Auf Initiative des Petitionsausschusses des Abgeordnetenhauses sollen künftig die rechtlich eigenständigen Unternehmen des Landes Berlin gegenüber dem Petitionsausschuss auskunftspflichtig sein, da diese Unternehmen eben nicht mit anderen Privatunternehmen vergleichbar sind und die Öffentlichkeit ein Anrecht darauf hat zu erfahren, wie das Land auch wirtschaftlich agiert.

Informationsfreiheit jenseits des IFG

Ein Bürger hatte bei seinem zuständigen Sozialamt darum gebeten, bestimmte Verwaltungsrichtlinien zum BSHG einsehen zu können. Zunächst war er an die nächstgelegene Stadtbibliothek verwiesen worden; nachdem er dort aber nicht fündig geworden war, erneuerte er sein Begehren und verwies nunmehr ausdrücklich auf den Anspruch aus dem IFG. Als das Sozialamt darauf nicht reagierte, trat er an uns mit der Bitte heran, ihn zu unterstützen.

[140] „Ausweitung der Informationsfreiheit statt Flucht ins Privatrecht“, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2003“, S. 111

In seiner Stellungnahme gegenüber unserer Dienststelle machte das Sozialamt geltend, dass das Informationsfreiheitsgesetz sich auf den Bereich Soziales nicht beziehe. Dort griffen allein die Bestimmungen des SGB X. Im Übrigen könne der Petent die Ausführungsvorschriften zum BSHG selbstverständlich in den öffentlichen Bibliotheken einsehen.

Das SGB X regelt das Sozialverwaltungsverfahren und den Sozialdatenschutz. Darin enthalten sind auch Bestimmungen, die die Akteneinsicht der Beteiligten in einem konkreten Verfahren feststellen. Vorschriften zu allgemeinen Informationsansprüchen, die sich auf Unterlagen beziehen, welche den Sozialbehörden zur Aufgabenerfüllung dienen – so der Text von § 3 Abs. 1 und 2 IFG –, enthält das SGB X nicht. Also sind zumindest bezüglich dieser Unterlagen die Bestimmungen des IFG auch im Bereich Soziales anzuwenden.

Darüber hinaus ist die Existenz eines Verwaltungsverfahrensgesetzes keine Besonderheit für die Sozialverwaltung. Auch die anderen Verwaltungen sind an ein (allgemeines) Verwaltungsverfahrensgesetz gebunden. Würde dieses immer dem IFG vorgehen, liefe es vollkommen leer, da dessen Adressaten als öffentliche Stellen durchweg Bestimmungen von Verwaltungsverfahrensgesetzen unterliegen.

Im vorliegenden Fall bedurfte es jedoch nicht einmal eines Rückgriffs auf das IFG. Bereits § 22 Abs. 1 der Gemeinsamen Geschäftsordnung für die Berliner Verwaltung, Allgemeiner Teil (GGO I) schreibt vor, dass die Einsicht in die einschlägigen Rechtsvorschriften und in die im Amtsblatt für Berlin veröffentlichten Verwaltungsvorschriften den Bürgern zu ermöglichen ist. Schon hieraus ergab sich somit die Pflicht des Sozialamtes, dem Petenten Einsicht in die begehrten Unterlagen zu ermöglichen.

5. Telekommunikation und Medien

5.1 Telekommunikation und Teledienste

Missbrauch von 0190er-/0900er-Rufnummern

Im August 2003 ist das Telekommunikationsgesetz (TKG) durch das Gesetz zur Bekämpfung des Missbrauchs von 0190er-/0900er-Mehrwertdiensterufnummern[141] geändert worden. Die neu eingefügten §§ 43a bis c TKG sehen unter anderem eine Preisangabepflicht der Anbieter von 0190er-/0900er-Mehrwertdiensten, eine Preisobergrenze, eine Registrierungs-

[141] BGBl. I, S. 1590

pflicht für Anwählprogramme (so genannte Dialer) sowie einen Auskunftsanspruch der Verbraucher gegenüber der Regulierungsbehörde für Telekommunikation und Post (www.regtp.de) vor. Die Telekommunikations-Datenschutzverordnung (TDSV) wurde in diesem Zusammenhang dahingehend geändert, dass künftig abweichend von § 7 Abs. 3 Satz 3 TDSV die 0190er oder 0900er-Mehrwertdiensterufnummern ungekürzt gespeichert werden dürfen. Eine Wahlmöglichkeit, die die Datenschutzbeauftragten gefordert hatten, besteht nicht.

Novellierung des Telekommunikationsgesetzes (TKG)

Die Bundesregierung hat inzwischen den Entwurf für ein neues Telekommunikationsgesetz (TKG-E) vorgelegt. Der Bundesrat hat seine Stellungnahme abgegeben[142]. Der Gesetzentwurf dient in erster Linie der (verspäteten) Umsetzung des EU-Richtlinienpakets für elektronische Kommunikationsdienste aus dem Jahr 2002 in nationales Recht mit dem Ziel einer technologieneutralen Regulierung aller Kommunikationsmittel und der Fortentwicklung eines funktionsfähigen Wettbewerbs in möglichst weiten Bereichen.

Die geplanten Neuregelungen sind allerdings seit langem heftig umstritten. Zu kritisieren sind neben den Wettbewerbsregeln und den für die Unternehmen kostspieligen Überwachungsauflagen des Gesetzes vor allem auch Teile der neuen Datenschutzbestimmungen in den §§ 89 ff. TKG-E (Teil 7 Abschnitt 2).

Um den gesamten Telekommunikationsdatenschutz zu straffen und um Redundanzen zu vermeiden, werden nach dem Vorschlag der Bundesregierung die Vorschriften der Telekommunikations-Datenschutzverordnung (TDSV) auf Gesetzesebene in das TKG übernommen. Dabei werden die Reglungen, die ursprünglich in § 89 TKG enthalten waren, eingearbeitet. Weitere Änderungen dienen der Umsetzung der europäischen Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vom 12. Juli 2002[143]. So dürfen etwa entsprechend den Vorgaben aus Art. 9 der Richtlinie Standortdaten bei „Location Based Services“ nach § 96 TKG-E künftig nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer seine Einwilligung gegeben hat. Von einer Zusammenführung

[142] vgl. Gesetzentwurf der Bundesregierung, BT-Drs. 15/2316, und die Stellungnahme des Bundesrats, BR-Drs. 755/03 (Beschluss)
[143] JB 2002, 5.1

der Datenschutzbestimmungen für Telekommunikations- und Teledienste wurde vor dem Hintergrund der Ende Oktober 2003 abgelaufenen Umsetzungsfrist abgesehen.

Die Datenschutzbeauftragten haben im Zuge des Novellierungsverfahrens mehrfach auf die Gefahren einer gravierenden Verschlechterung des Datenschutzniveaus im Telekommunikationssektor hingewiesen, sollte der vorliegende Entwurf des neuen TKG Gesetz werden. Dabei wurden zwei Problemkreise besonders hervorgehoben:

Speicherung von Verkehrsdaten

§ 95 TKG-E regelt den Umfang der zulässigen Verwendung von Verkehrsdaten (ersetzt den bisherigen Begriff der Verbindungsdaten) für Zwecke der Entgeltermittlung und -abrechnung und übernimmt im Wesentlichen die Regelungen des § 7 der geltenden TDSV. Entsprechend der Änderung in § 95 Abs. 3 TKG-E besteht nunmehr allerdings die Möglichkeit für die Diensteanbieter, grundsätzlich alle Verkehrsdaten (also auch alle Zielrufnummern) innerhalb der vorgegebenen sechsmonatigen Frist ungekürzt zu speichern. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daran deutliche Kritik geübt und darauf hingewiesen, dass damit ohne Not und ohne überzeugende Begründung eine in der Praxis bewährte Regelung aufgegeben werde, die bisher die Speicherung von verkürzten Zielrufnummern vorsieht, wenn die Kundinnen und Kunden sich nicht für die vollständige Speicherung oder vollständige Löschung entscheiden[144]. Es steht zu befürchten, dass Millionen von Verkehrsdatensätzen selbst dann noch unverkürzt gespeichert bleiben und dem Zugriff anderer Stellen ausgesetzt sind, wenn die Diensteanbieter sie für Abrechnungszwecke nicht mehr benötigen. Zwar wird den Kunden auch im neuen Entwurf das Recht zugestanden, die Speicherung gekürzter Zielrufnummern oder ihre vollständige Löschung nach Rechnungsversand zu verlangen. Die Beibehaltung des bisherigen Datenschutzstandards sollte aber nicht von der Initiative der Betroffenen abhängig gemacht werden.

Über den Vorschlag der Bundesregierung hinausgehend, fordert der Bundesrat in seiner Stellungnahme zum TKG-Entwurf sogar eine gesetzliche Pflicht zur Vorratsdatenspeicherung von Verkehrsdaten für sechs Monate. Den Diensteanbietern solle dabei nicht die Erhebung zusätzlicher Daten, sondern allein eine befristete Sicherung der zu Zwecken des Dienstes gewonnenen Informationen in Ansehung der Bedürfnisse einer effektiven Strafver-

[144] Entschließung vom 21. November 2003 „Gravierende Verschlechterungen des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes“, vgl. Anlagenband, a. a. O., S. 44

folgung und wirksamen Gefahrenabwehr aufgegeben werden[145]. Aus Sicht der Datenschutzbeauftragen des Bundes und der Länder bestehen gegen eine solche Regelung erhebliche verfassungsrechtliche Bedenken[146]. Sie widerspräche datenschutzrechtlichen Prinzipien wie dem der Zweckbindung und werfe Fragen der Verhältnismäßigkeit auf.

Die Vorschläge des Bundesrates zur zwangsweisen Vorratsdatenspeicherung stehen im internationalen und europäischen Kontext nicht allein da, sondern spiegeln eine allgemeine Tendenz wieder, Telekommunikations-Diensteanbieter zu verpflichten, Verkehrsdaten längerfristig vorzuhalten, um Strafverfolgungs- und Sicherheitsbehörden den möglichen Zugang zu erlauben. Wir haben darüber bereits im letzten Jahresbericht ausführlich informiert[147]. Die Konferenz der Europäischen Datenschutzbeauftragten hatte im Jahr 2002 in einer Erklärung gravierende Zweifel hinsichtlich der Legitimität und Legalität von weitreichenden Maßnahmen zur Vorratsdatenspeicherung angemeldet und unter Bezugnahme auf die Rechtsprechung des Europäischen Menschenrechtsgerichtshofs betont, dass eine solche Vorratsdatenspeicherung ein unzulässiger Eingriff in die Grundrechte des Einzelnen nach Art. 8 der Europäischen Menschenrechtskonvention sei[148]. Diese Auffassung wird jetzt durch ein Memorandum von Privacy International vom Oktober 2003 gestützt[149].

Die Art. 29-Datenschutzgruppe hat in einer Stellungnahme[150] empfohlen, Maßnahmen zur harmonisierten Auslegung des begrenzten Zeitraums zu ergreifen, in dem Telekommunikations-Diensteanbieter Verkehrsdaten nach den Vorgaben der europäischen Datenschutzrichtlinien zum Zwecke der Gebührenabrechung und Zusammenschaltung speichern dürfen. Hier gebe es in den Mitgliedstaaten erhebliche Unterschiede bei der Auslegung.

Zwangsidentifizierung beim Erwerb von Prepaid-Produkten

In § 109 Abs. 1 Satz 1 des TKG-Entwurfs wird festgelegt, welche Kundendaten (Name, Anschrift, Geburtsdatum) von den Diensteanbietern zu erheben und für ein mögliches Auskunftsersuchen der Sicherheitsbehörden bereitzuhalten sind, und zwar unabhängig von der

[145] vgl. BR-Drs. 755/03 (Beschluss), S. 33 f.
[146] vgl. oben
[147] JB 2002, 5.1
[148] Erklärung der Konferenz der Europäischen Datenschutzbeauftragten zur zwangsweisen systematischen Speicherung von Verkehrsdaten der Telekommunikation vom 11. September 2002, vgl. Anlagenband “Dokumente zu Datenschutz und Informationsfreiheit 2002”, S. 63
[149] Memorandum of Laws concerning the Legality of Data Retention with Regard to the Rights guaranteed by the European Convention on Human Rights
[150] Stellungnahme zur Speicherung von Verkehrsdaten zu Zwecken der Gebührenabrechnung, WP 69 vom 29. Januar 2003

Erforderlichkeit der Datenerhebung zum Zwecke der Begründung, Änderung oder Ausgestaltung eines Vertragsverhältnisses. Diese Anforderungen gelten folglich auch für Kundenverhältnisse, bei denen die vom Kunden in Anspruch zu nehmende Telekommunikationsdienstleistung im Voraus bezahlt wird, also etwa bei Prepaid-Produkten. Mit dieser Neuregelung soll die längjährige Praxis der Diensteanbieter, auch ihre Prepaid-Kunden zu identifizieren und nach Überprüfung in eine Kundendatei einzustellen, gesetzlich ausdrücklich festgeschrieben werden. Bisher hatten sich die Diensteanbieter bei ihrem Vorgehen auf Leitlinien der Regulierungsbehörde für Telekommunikation und Post gestützt, die in dem aktuell geltenden § 90 TKG eine ausreichende Ermächtigungsgrundlage für eine derartige Verpflichtung zur Datenerhebung sah[151].

Im Oktober 2003 hat das Bundesverwaltungsgericht dieser Auffassung allerdings den Boden entzogen und entschieden, dass die Anbieter von Prepaid-Karten nicht verpflichtet sind, personenbezogene Daten ihrer Kunden zu erheben[152]. Da der Kunde bei dem Erwerb einer Prepaid-Karte in Vorleistung trete, sei für den Diensteanbieter – anders als bei Standardverträgen – die Erhebung und Speicherung personenbezogener Daten des Kunden für die Begründung und Abwicklung des Vertragsverhältnisses nicht erforderlich. Eine Pflicht des Mobilfunkunternehmens, personenbezogene Kundendaten zu erheben, stelle einen staatlichen Eingriff in das verfassungsrechtlich gewährleistete Recht des Kunden auf informationelle Selbstbestimmung dar. Dies setze notwendig eine ausreichende, dem Gebot der Normenklarheit genügende gesetzliche Grundlage voraus, die § 90 TKG gerade nicht enthalte. Die darin vorgesehe Verpflichtung zur Führung von Kundendateien, auf die Polizei- und Strafverfolgungsbehörden zugreifen können, betreffe nur denjenigen Datenbestand, der zuvor von den Unternehmen nach Maßgabe einer anderen Bestimmung des TKG im eigenen Geschäftsinteresse freiwillig erhoben worden ist.

Durch das Urteil des Bundesverwaltungsgerichts sehen sich die Datenschutzbeauftragten des Bundes und der Länder in ihrer Auffassung bestätigt und wenden sich in ihrer Entschließung[153] zugleich gegen die mit der TKG-Novelle geplante Einführung einer derartigen Identifikationspflicht. Diese würde zu einer verdachtslosen Datenspeicherung auf Vorrat führen. Es wird erneut darauf hingewiesen, dass auch die geplante Gesetzesänderung nicht verhindern wird, dass Straftäterinnen und Straftäter bewusst und gezielt in kurzen Zeitabständen neue Prepaid-Karten erwerben, Strohleute zum Erwerb einsetzen, die Karten häufig - teilweise nach jedem Telefonat - wechseln oder die Karten untereinander austauschen und diese Da-

[151] JB 2002, 5.1
[152] Urteil vom 22. Oktober 2003, Az.: 6 C 23.02
[153] vgl. oben

ten deshalb keinen nennenswerten Informationsgewinn für die Sicherheitsbehörden bringen[154].

AG „Telekommunikation, Tele- und Mediendienste“ des „Düsseldorfer Kreises“

Ein zentraler Punkt der Beratungen der Arbeitsgruppe war zum wiederholten Mal die Frage der Zulässigkeit der Speicherung von IP-Adressen von P2P-Nutzern durch Access-Provider. Das Regierungspräsidium Darmstadt als zuständige Aufsichtsbehörde für den privaten Bereich hatte in einer kontrovers diskutierten Entscheidung am 14. Januar 2003 die Speicherung der dynamisch vergebenen IP-Adresse durch einen Internet-Zugangsprovider nebst Datum, Uhrzeit und Länge einer Internetsitzung über das Ende der Verbindung hinaus auch bei der Nutzung eines zeit- und volumenabhängigen Pauschaltarifs (Flatrate) nach § 6 Abs. 4 TDDSG und nach § 1 Abs. 2 TDDSG, § 9 BDSG für zulässig erklärt. Die Speicherung der IP-Adresse sei zum einen als Abrechnungsdatum erforderlich, damit der Access-Provider im Zweifelsfall die kostenpflichtige Erbringung der Leistung korrekt und durchsetzbar nachweisen kann. Zum anderen sei die Speicherung auch als geeignete Maßnahme zur Gewährleistung der Datensicherheit im Sinne von § 9 BDSG (nebst Anlage) gerechtfertigt.

Einigkeit bestand unter den Teilnehmern der Arbeitsgruppe insoweit, als die Entscheidung des Regierungspräsidiums Darmstadt als Einzelfallentscheidung eingestuft wurde. Ob und inwieweit gleichartige Voraussetzungen auch bei anderen Anbietern vorliegen, müsse jeweils gesondert geprüft werden.

Die Arbeitsgruppe befasste sich ferner mit der Veröffentlichung personenbezogener Daten von Domain-Inhabern durch Registrare in den „generic top level domains“ (gTLD: .com, .net, .org), die ihren Sitz in Deutschland haben. Kernproblem aus Sicht des Datenschutzes ist, dass die Vorschriften des „Registrar Accreditation Agreement“ (RAA), das von den deutschen Registraren mit der jeweiligen Registry bzw. mit ICANN geschlossen wird, in einzelnen Punkten dem geltenden nationalen Datenschutzschutzrecht widersprechen. Dies betrifft etwa die Veröffentlichung der Telefonnummer des Domain-Inhabers und Fragen der Zweckbestimmung und Zweckbindung. Auf diese Thematik weist auch die Art. 29-Datenschutzgruppe in ihrer Stellungnahme zur Anwendung der Datenschutzgrundsätze auf

[154] so bereits eine Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Mai 2002, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2002“, S. 25

die Whois-Verzeichnisse hin[155]. ICANN plant eine weitere, vertiefte Befassung mit Datenschutzaspekten der Verarbeitung personenbezogener Daten in Whois-Datenbanken.

AK Medien der Konferenz der Datenschutzbeauftragten

Beim Arbeitskreis Medien war ein zentrales Thema die neue Medienordnung, insbesondere die Neuordnung des Datenschutzes bei Tele- und Mediendiensten. Seit Anfang 2003 liegen erste Strukturüberlegungen für ein Gesetz über den Datenschutz bei der Nutzung elektronischer Medien (Elektronische-Medien-Datenschutzgesetz – EMDSG) des Bundesministeriums für Wirtschaft und Arbeit (BMWA) vor. Mit dem EMDSG sollen zunächst die gesetzlichen Datenschutzanforderungen für die Verwendung von Nutzerdaten in allen elektronischen Medien (Tele- und Mediendienste) in einem Bundesgesetz auf der Grundlage der geltenden spezifischen Datenschutzbestimmungen in Bund und Ländern vereinheitlicht werden. Zugleich soll im Hinblick auf die Datenschutzrichtlinie für elektronische Kommunikation klargestellt werden, dass Kommunikationsdienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, nicht unter das EMDSG fallen. Weitere Ziele sind die Schaffung klarer Strukturen für die Datenschutzaufsicht und die Schaffung einer wirksamen freiwilligen Selbstkontrolle der Wirtschaft im Bereich des Datenschutzes in den elektronischen Medien.

Die Teilnehmer des Arbeitskreises waren sich einig, das die materiell-rechtlichen Regelungen des Entwurfs weitgehend akzeptiert werden können. Positiv ist aus Sicht des Arbeitskreises insbesondere die vorgesehene Zusammenfassung der datenschutzrechtlichen Bestimmungen aus dem Teledienstedatenschutzgesetz (TDDSG) und dem Mediendienste-Staatsvertrag (MDStV). Auf erhebliche Kritik stieß bei den Teilnehmern des Arbeitskreises jedoch die im ursprünglichen EMDSG-Entwurf vorgesehene Aufsichtsstruktur für den Datenschutz. Es bestanden erhebliche Bedenken vor allem gegen die freiwillige Selbstkontrolle durch die Internetwirtschaft, die die staatliche Kontrolle teilweise ersetzen soll. Unklar blieb auch das Verhältnis zwischen den Aufsichtsbehörden bzw. Landesdatenschutzbeauftragen einerseits und dem Bundesbeauftragten andererseits. Im Mai 2003 hat das BMWA Änderungsvorschläge für den EMDSG-Entwurf unterbreitet, aus denen sich ergibt, dass nunmehr von der Neuordnung der Aufsichtsstruktur Abstand genommen wird. Seitdem hat es keinen sichtbaren Fortgang der Angelegenheit mehr gegeben.

[155] WP 76, Stellungnahme 2/2003 vom 13. Juni 2003

Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation

Die Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation/International Working Group on Data Protection in Telecommunications (IWGDPT) feierte 2003 ihr 20-jähriges Bestehen und kann auf eine erfolgreiche Arbeit seit 1983 zurückblicken. Im zurückliegenden Jahr wurden wieder Arbeitspapiere zu weltweit aktuellen Datenschutzfragen aus dem Telekommunikationssektor verabschiedet:

Ein Arbeitspapier setzt sich mit den potenziellen Datenschutzrisiken im Zusammenhang mit der geplanten Einführung des so genannten ENUM-Service auseinander[156]. Mit dem ENUM-Protokoll werden unter Nutzung des Domain Name Systems (DNS) die verschiedensten Kommunikationsdienste über nur eine Rufnummer identifiziert und angesprochen (z. B. Abbildung von Telefonnummern auf URLs). Die öffentlich zugänglichen Dokumente über den ENUM-Dienst haben zu kritischen Äußerungen durch Regierungsstellen, Bürgerrechtsgruppen und Datenschutzaktivisten aus verschiedenen Ländern geführt. Es wird unter anderem auf die Möglichkeiten der Verletzung der Privatsphäre durch den Missbrauch zu Werbezwecken sowie darauf hingewiesen, dass ENUM in Zukunft zu einem weltweit eindeutigen Wiedererkennungszeichen für eine Person, einem „globally unique identifier“, werden könnte. Die Internationale Arbeitsgruppe fordert die ITU und die IETF sowie die beteiligten Industrievertreter und die zuständigen nationalen Regulierungsgremien auf, dem Datenschutz eine hohe Priorität bei der weiteren Entwicklung des ENUM-Dienstes einzuräumen. Es sei von großer Bedeutung, dass die personenbezogenen Daten von Nutzern der ENUM-Nummern nur mit der informierten Einwilligung zum öffentlichen Abruf bereitgestellt werden. Auch wird betont, dass die Privatsphäre von Nutzern besser geschützt werden könne, wenn eine Option zur Nutzung pseudonymer Daten als ENUM-„Domainnamen“ vorgesehen würde.

Die DENIC führt seit Herbst 2002 einen Testbetrieb durch, in dem ein Betriebsmodell für ENUM in Deutschland entwickelt werden soll. Dieses Vorhaben wird von den Datenschutzbeauftragten begleitet.

Ein weiteres Arbeitspapier hat die Internationale Arbeitsgruppe zum Thema Intrusion Detection Systems (IDS) erarbeitet[157]. Unter Intrusion Detection ist der Prozess des Erkennens unberechtigter Nutzung von Systemen und Netzen unter Nutzung spezieller Software und/oder Hardware zu verstehen. Da IDS viele Verkehrs- oder Ereignisdaten sammeln und aufzeichnen, die auch personenbezogene Daten enthalten können, liegen die Datenschutz-

[156] Arbeitspapier der 34. Sitzung am 2./3. September 2003, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2003“, S. 101

bedenken auf der Hand. Die Arbeitsgruppe hält es daher für notwendig, die Aufmerksamkeit aller Verantwortlichen für die Entwicklung von IDS auf die Einhaltung zentraler Datenschutzprinzipien hinzuweisen: Intrusion Detection muss dem Zweck der Datensicherheit oder des Systemschutzes dienen, die Speicherung der Daten (Netzwerk-Pakete, Audit-Logs) muss dem Schutzzweck angemessen sein, eine Datenschutz-Policy, die die Anforderungen an den Schutz personenbezogener Daten abdeckt, die in IDS gespeichert werden, sollte entwickelt und angewandt werden. Derzeit gibt es zu IDS bereits erste Standardisierungsbemühungen von Seiten der ISO[158].

Darüber hinaus wurde in der Herbstsitzung der Arbeitsgruppe in Berlin eine Resolution zu Radio-Frequency Identification (RFID) zur Diskussion gestellt und zur Entscheidung an die Internationale Konferenz der Datenschutzbeauftragten überwiesen[159]. Bei RFID handelt es sich um einen winzigen Funkchip, der zunehmend von Herstellern und Warenhäusern zur Kennzeichnung und Preisauszeichnung von Warenbeständen eingesetzt wird. Zukünftig soll er den Barcode im Einzelhandel ablösen. Der Anwendungsbereich umfasst aber auch die Markierung von Firmeninventar, das auf diese Weise (auch gekoppelt mit Videoüberwachung) gegen Diebstahl durch die Beschäftigten gesichert werden soll. Die Europäische Zentralbank hat zudem angekündigt, dass auch Euro-Banknoten mit dem neuen Mikrochip ausgestattet werden sollen. Die Internationale Arbeitsgruppe und die Internationale Konferenz weisen auf die damit verbundenen neuen Herausforderungen für den Datenschutz hin und fordern die Beachtung der grundlegenden Prinzipien bei der Entwicklung und dem Einsatz der neuen Technologie. So sollten vornehmlich datensparsame Alternativen, d. h. solche ohne zwingende Verarbeitung personenbezogener Daten eingesetzt werden, wenn mit ihnen das gleiche Ziel erreichbar ist. Sind die Erhebung und Speicherung personenbezogener Daten unumgänglich, sollte dies in einer für den Betroffenen transparenten Weise geschehen. Schließlich sollten die personenbezogenen Daten nur zu dem Zweck verwendet werden, zu dem sie erhoben wurden, und bei Zweckerreichung umgehend gelöscht werden[160].

Weitere Tagesordnungspunkte auf den Sitzungen der Arbeitsgruppe im Jahr 2003 waren unter anderem die Möglichkeiten und Verfahren zur Bekämpfung von Online-Kriminalität (Cyber-Fraud), Datenschutzprobleme im Zusammenhang mit Wireless LAN/WIFI, die Verarbeitung personenbezogener Daten in Whois-Datenbanken, der Umgang mit SPAM (uner-

---

[157] a. a. O., S. 104

[158] Richtlinien für die Herstellung, den Betrieb und die Verwaltung von Intrusion-Detection-Systemen (IDS), ISO/IEC WD 18043

[159] Entschließung der Internationalen Konferenz der Datenschutzbeauftragten vom 20. November 2003, vgl. Anlagenband, a. a. O., S. 98

wünschter Werbung), Datenschutz und Multimedia-Messages (MMS) und die Vorratsspeicherung von Telekommunikations-Verkehrsdaten zum Zwecke der Kriminalitäts- und Terrorismusbekämpfung.

Neuordnung des Jugendschutzes im Internet

Mit der Ausweitung der Online-Kommunikation wächst die Gefahr, dass Minderjährige mit für sie schädlichen Inhalten konfrontiert werden. Vor diesem Hintergrund haben sich Bund und Länder auf eine Neuordnung des Jugendmedienschutzes im Internet geeinigt. Zentrales Element der Reform ist ein von den Ländern abgeschlossener Staatsvertrag zum Jugendmedienschutz (JMStV)[161], der zusammen mit dem novellierten Jugendschutzgesetz des Bundes am 1. April 2003 in Kraft getreten ist. Ziel der Neuordnung ist die Schaffung eines kohärenten Ordnungsrahmens für alle Onlinedienste, dessen Einhaltung durch eine einheitliche, von den Ländern zu errichtende Aufsichtsinstanz, die Kommission für Jugendmedienschutz (KJM), überwacht werden soll. Vorgesehen sind auch der Einsatz von Selbstkontrollmechanismen als Steuerungsinstrument sowie deren Verzahnung mit der hoheitlichen Medienaufsicht.

5.2 Datenschutz und Medien

Fusion von ORB und SFB zum RBB

Am 1. Mai 2003 wurde die im Jahr zuvor durch den Staatsvertrag über die Errichtung einer gemeinsamen Rundfunkanstalt der Länder Berlin und Brandenburg beschlossene Fusion von Ostdeutschem Rundfunk Brandenburg und Sender Freies Berlin zum Rundfunk Berlin - Brandenburg vollzogen. Damit gilt nun für die gesamte Rundfunkanstalt – auch soweit sie im Land Brandenburg tätig ist – das Berliner Datenschutzgesetz (BlnDSG), zusätzlich die besonderen Regelungen zum Datenschutz nach dem Staatsvertrag. Letztere regeln auch die Zuständigkeit für die Kontrolle des Datenschutzes innerhalb des RBB.

Verarbeitet der RBB personenbezogene Daten zu eigenen journalistisch-redaktionellen oder literarischen Zwecken, ist für die Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften die Datenschutzbeauftragte des RBB zuständig. Diese eigenverantwortliche Kontrollzustän-

---

[160] vgl. 2.1

digkeit folgt der verfassungsrechtlich garantierten Rundfunk- und Pressefreiheit in Deutschland.

In allen anderen Bereichen (z. B. Hörerservice, Personalverwaltung, Fragen der Rundfunkgebühren) kontrollieren die Einhaltung des Datenschutzes die Landesbeauftragten von Berlin und Brandenburg. § 38 Abs. 8 des Staatsvertrages hat hierzu eine Kooperation der beiden Dienststellen vorgesehen. Danach erfolgt die Kontrolle durch den Berliner Beauftragten für Datenschutz und Informationsfreiheit im Benehmen mit dem Landesbeauftragten für den Datenschutz und das Recht auf Akteneinsicht Brandenburg. Diese gesetzlich normierte Kooperationspflicht fügt sich ein in die ohnehin bestehenden engen Verbindungen unserer beiden Dienststellen.

Die datenschutzrechtlichen Bestimmungen des Staatsvertrages waren in Abstimmung mit uns und unseren Brandenburger Kollegen erstellt worden. Sie beschränken sich nicht allein auf die Vorgaben des Bundesdatenschutzes, sondern regeln auch dezidiert die Auskunfts- und Berichtigungsrechte der Betroffenen wie auch ein Anrufungsrecht der Datenschutzbeauftragten und sichern somit ein hohes Niveau des Datenschutzes auch im journalistisch-redaktionellen Bereich. In ersten Gesprächen mit der Intendantin und der Datenschutzbeauftragten der gemeinsamen Rundfunkanstalt haben wir uns davon überzeugen können, dass der Datenschutz auch künftig einen hohen Stellenwert im öffentlichen Rundfunk der beiden Bundesländer haben soll.

Neuordnung der Rundfunkfinanzierung

Der steigende Finanzbedarf der öffentlichen Rundfunkanstalten führte zu einer intensiven Diskussion über eine Neuordnung der Rundfunkfinanzierung. Ein Vorschlag der Rundfunkanstalten sah hierzu vor, die Rundfunkgebührenpflicht nicht mehr an einzelne Personen (Haushaltsvorstand) zu knüpfen, sondern an den jeweiligen Haushalt selbst. Dies hätte zunächst den positiven Aspekt, dass unklare Befreiungstatbestände entfallen könnten. Gleichwohl wären alle Mitglieder eines Haushalts Gesamt-Gebührenschuldner und somit in den Datenbeständen der GEZ zu erfassen, was einen enormen Zuwachs an Daten mit sich gebracht hätte. Des Weiteren sollte zum Abgleich der GEZ-Datenbestände neben der bereits bestehenden regelmäßigen Übermittlung aller Zu- und Wegzüge aus den Meldedaten nun auch ein Zugriff auf weitere öffentliche Dateien wie die Register von berufsständischen

[161] Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien vom 20. November 2002

Kammern, die Schuldnerverzeichnisse und das Gewerbezentralregister erfolgen. Zum In-Kraft-Treten der Neuregelung sollten alle Meldebehörden verpflichtet werden, der GEZ ihre Daten vollständig zu übermitteln. Zudem sollte die Erhebung von personenbezogenen Daten bei Dritten, beispielsweise durch Ankauf von privaten Adresshändlern, ausdrücklich erlaubt werden. Vorgeschlagen wurde schließlich, dass die datenschutzrechtliche Aufsicht durch Landesbeauftragte für den Datenschutz bei den Rundfunkanstalten generell und nicht nur im journalistisch-redaktionellen Bereich ausgeschlossen wird.

Diese Vorschläge hätten zum Teil gravierende Verschlechterungen des Datenschutzes mit sich gebracht[162]. Durch die Übermittlung aller Daten der Meldebehörden der Bundesrepublik Deutschland wäre bei der GEZ ein bundesweites zentrales Register aller über 16-jährigen Personen mit zusätzlichen Informationen über ihre sozialen Verhältnisse (wie Partnerschaften, gesetzliche Vertretungen, Haushaltszugehörigkeit und Empfang von Sozialleistungen) entstanden, ohne dass dies für den Einzug der Rundfunkgebühren erforderlich wäre. Durch den Zugriff auf die vielfältigen Register wäre der GEZ die Datenerhebung in einem Umfang gestattet worden, wie sie für keine andere Stelle in Deutschland besteht. Dies wäre ohne Zweifel unverhältnismäßig gewesen.

Auch besteht kein Anlass zur Befürchtung, dass durch die Kontrolle der Einhaltung des Datenschutzes durch Landesbeauftragte in die Rundfunk- und Pressefreiheit der Rundfunkanstalten eingegriffen würde, da von dieser Kontrollbefugnis der journalistisch-redaktionelle Bereich ausdrücklich ausgenommen ist. In allen anderen Bereichen unterscheiden sich die Rundfunkanstalten in ihrer Tätigkeit im Grundsatz nicht von öffentlichen oder auch privaten Stellen.

Nicht zuletzt auch wegen der Bedenken der Datenschutzbeauftragten des Bundes und der Länder sind die Planungen für eine Neuordnung der Rundfunkfinanzierung zunächst zurückgestellt worden. Der Siebte Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge sieht daher auch keine Änderungen von Regelung zum Einzug der Rundfunkgebühren vor, verlängert vielmehr die Befristung der Gebührenfreiheit für Rechner, die Rundfunkprogramme ausschließlich über Angebote aus dem Internet wiedergeben können, vom 31. Dezember 2004 auf den 31. Dezember 2006. Da auch eine Änderung dieser Ausnahmeregelung zum Konzept der Rundfunkanstalten gehörte, kann davon ausgegangen werden, dass die bisherigen Pläne so nicht umgesetzt werden.

Fernseher abmelden: Die GEZ fragt gerne nach

> *Ein Bürger hatte sich entschlossen, künftig auf seinen Fernseher zu verzichten. Als moderner Mensch lud er aus dem Internet ein Formular der GEZ, das zur Abmeldung des Fernsehgerätes verwendet werden sollte, herunter und sandte es ausgefüllt an die GEZ. Daraufhin erhielt er von dort ein Schreiben, dass er doch bitte weitere Angaben zum Grund seiner Abmeldung machen möge. Unter anderem wurde danach gefragt, was mit dem Fernsehgerät geschehen sei. Für den Fall, dass das Fernsehgerät an einen anderen abgegeben wurde, möge man diese Person doch bitte unter Angabe ihrer Adresse benennen. Das mitgesandte Antwortformular vermerkte zwar, dass diese Angaben freiwillig sein, gleichwohl teilte die GEZ vor- und fürsorglich mit, dass sie die Abmeldung bis zur Rückantwort des Betroffenen noch zurückstellen werde.*

Die Aufforderung der GEZ, Namen und Anschrift derjenigen Person mitzuteilen, an die ein Empfangsgerät abgegeben wurde, ist unzulässig. Weder der Rundfunkgebührenstaatsvertrag noch das BlnDSG lassen eine solche Erhebung durch die GEZ im Auftrag des RBB zu. Nach § 10 Abs. 4 BlnDSG ist eine Datenerhebung bei Dritten nur zulässig, wenn eine Rechtsvorschrift dies vorsieht. Nach einer solchen sucht man aber vergeblich. Die unzulässige Datenerhebung wird auch dadurch nicht rechtmäßig, dass auf dem Antwortformular vermerkt ist, eine solche Angabe sei freiwillig, da es allein auf die gesetzliche Erhebungsbefugnis der GEZ ankommt. Eine *freiwillige* Preisgabe von Daten Dritter ist im datenschutzrechtlichen Sinne ohnehin nicht möglich. Von Freiwilligkeit kann nämlich nur dann die Rede sein, wenn der Betroffene selbst ohne Zwang *seine* Daten offenbart.

Der Zweck heiligt die Mittel nicht

> *Immer wieder treten Petenten an uns heran, die sich darüber beschweren oder zumindest überrascht sind, dass sie von der Gebühreneinzugszentrale (GEZ) schriftlich aufgefordert werden mitzuteilen, ob sie Rundfunkgeräte zum Empfang bereithalten, und gegebenenfalls diese anzumelden.*

Im Auftrag der Landesrundfunkanstalten führt die GEZ seit Jahren so genannte „Direkt-Mailing-Aktionen“ durch, mit denen sie nicht angemeldete Personen oder solche, die nur als

---

[162] vgl. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 30. April 2003 zur Neuordnung der Rundfunkfinanzierung, vgl. Anlagenband, a. a.

Hörfunkteilnehmer gemeldet sind, anschreibt und auffordert, gegebenenfalls ihrer Rundfunkgebührenpflicht nachzukommen. Grundlage dieser Aktionen ist ein Abgleich des Datenbestandes der Rundfunkteilnehmer bei der GEZ mit anderen Adressbeständen.

Soweit hierfür die Daten der Meldebehörden über Ab- und Anmeldungen Verwendung finden, ist dagegen grundsätzlich nichts einzuwenden. Die Datenübermittlung an die GEZ geschieht auf einer gesetzlichen Grundlage und nicht zuletzt eben zu diesem Zweck. In einer Reihe von Fällen konnten wir daher den Petenten mitteilen, dass die GEZ ihre Daten auf rechtmäßige Weise erhoben hat.

Bei einigen Eingaben bestätigte sich jedoch der Verdacht der Petenten, dass ihre Anschrift von privaten Adresshändlern durch Kauf, Miete oder Leasing durch die GEZ erworben wurde. Der RBB, als Auftraggeber der GEZ, vertritt die Auffassung, dass er nach §§ 28, 29 BDSG hierzu befugt sei, da er die Anschriften für „werblich-informierende Zwecke“ nutze. Hilfsweise verweist er auf § 6 Abs. 1 BlnDSG, wonach die Verarbeitung personenbezogener Daten zulässig ist, wenn wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Im Übrigen sei der Ankauf von Adressen aus wirtschaftlicher Sicht unverzichtbar, da durch solche Mailing-Aktionen nicht wenige neue Rundfunkteilnehmer gewonnen würden.

Trotz dieser wirtschaftlichen Argumente haben wir gegenüber dem RBB wiederholt darauf aufmerksam machen müssen, dass diese Rechtsauffassung nicht zutrifft und daher der Ankauf von Adressbeständen bei privaten Adresshändlern wegen einer fehlenden Rechtsgrundlage unzulässig ist. Zum einen kann sich der RBB als öffentliche Stelle nicht auf §§ 28, 29 BDSG berufen, da es sich hierbei um Regelungen für die Datenverarbeitung nichtöffentlicher Stellen bzw. öffentlich-rechtlicher Wettbewerbsunternehmen handelt. Zum anderen sind Datenbestände, die von Adresshändlern angeboten werden, gerade nicht offenkundig, da sie nicht jedermann zugänglich sind, sondern vielmehr aufgrund eines Vertrages und einer entsprechenden Gegenleistung übermittelt werden. Überdies kann nicht davon ausgegangen werden, dass ihre Verwendung durch die GEZ schutzwürdige Belange der Betroffenen nicht beeinträchtigt. Die Rasterung der Rundfunkteilnehmerdaten mit den erworbenen Daten führt vielmehr dazu, dass die dabei festgestellten Nicht-Rundfunkteilnehmer bzw. Rundfunkteilnehmer, die nur ein Rundfunkgerät, jedoch kein Fernsehgerät bereithalten, dem Verdacht einer Ordnungswidrigkeit ausgesetzt werden.

---

6. Aus der Dienststelle

6.1 Entwicklung

Angesichts der Haushaltslage des Landes ist es selbstverständlich, dass die Ausstattung der Dienststelle nicht an den aufgabengerechten Bedarf angepasst werden konnte. Dies führt dazu, dass wir uns nach wie vor im Wesentlichen auf die Bearbeitung der von außen an uns herangetragenen Aufgaben beschränken müssen und nur in äußerst beschränktem Umfang eigentlich erforderliche Prüfungen von Amts wegen bei Unternehmen und Behörden des Landes durchführen können.

Mit dem Umzug der Dienststelle in das Bürogebäude An der Urania 4 - 10, 10787 Berlin (Tel. 030/1 38 89-0) haben sich die räumlichen Bedingungen dagegen verbessert. Einerseits sind wir nunmehr für Bürgerinnen und Bürger, die häufig persönlich unsere Beratung suchen, noch leichter erreichbar, andererseits waren wir in der Lage, gerade hierfür ein BürgerOffice mit einem angemessenen Empfangsbereich einzurichten, das künftig als zentrale Anlaufstelle für alle Besucher dienen wird. Im gleichen Gebäude sind auch der Rechnungshof und die Landeszentrale für politische Bildungsarbeit untergebracht, mit denen uns - jeweils unterschiedliche - Interessen verbinden. Wir werden uns bemühen, die dadurch möglichen Synergieeffekte zu nutzen.

6.2 BürgerOffice

Um den Kontakt zum Bürger und die damit verbundenen Aufgaben zu bündeln, haben wir bereits im Jahr 2002 mit der schrittweisen Einführung eines BürgerOffice begonnen. Diese Aufbauphase konnte im Berichtszeitraum abgeschlossen werden. Die Arbeitsabläufe, Zuständigkeiten und Verfahren zur Bearbeitung von Bürgereingaben wurden in einer internen Geschäftsanweisung festgelegt. Danach werden alle schriftlichen Eingaben an den Berliner Beauftragten für Datenschutz und Informationsfreiheit im BürgerOffice zentral erfasst und von der dortigen Geschäftsstelle verwaltet. Die inhaltliche Bearbeitung der Anfragen erfolgt in einfachen Fällen allein durch das BürgerOffice und in komplexeren Angelegenheiten unter Beteiligung der Referenten in den einzelnen Arbeitsgebieten.

Im Berichtszeitraum erhielten wir insgesamt ca. 1000 schriftliche Anfragen und Beschwerden von Bürgerinnen und Bürgern, die sich auf sehr unterschiedliche Weise mit der Beeinträchtigung ihres Rechts auf informationelle Selbstbestimmung konfrontiert sahen. Die Anzahl der

telefonischen Beratungsersuchen wird nicht erfasst, dürfte jedoch um ein Vielfaches höher sein.

Die inhaltliche Bandbreite der Anliegen ist groß. Sie reicht von der Bitte um Übersendung von Informationsmaterial, allgemein gefasste Anfragen zum Thema Datenschutz, Beschwerden über datenschutzrechtliche Verstöße in konkreten Einzelfällen bis zur Behandlung von abstrakten Grundsatzproblemen. Auch der subjektive Betroffenheitsgrad der Beschwerdeführer differiert erheblich. Während sich einige Petenten durch Verstöße gegen datenschutzrechtliche Bestimmungen lediglich belästigt fühlen, geht es für andere um existenzielle Bedrohungen.

Auffällig ist, dass das Verhältnis der schriftlichen Eingaben gegen Datenverarbeiter im privaten und im öffentlichen Bereich nahezu ausgewogen ist. Während die schriftlichen Eingaben in der Vergangenheit zumeist auf dem traditionellen Postweg erfolgten, nutzen die Beschwerdeführer zunehmend auch E-Mails, um ihre Anliegen vorzutragen. Dabei ist zu beobachten, dass der Anteil von Bagatell- und Standardanfragen bei den E-Mail-Eingaben erheblich höher ist als bei den Eingaben, die auf dem Postweg eingehen.

Die Verteilung der Vorgänge auf die Arbeitsgebiete entspricht derjenigen des Vorjahres: Die meisten Fälle betrafen die Arbeitsgebiete Wirtschaft sowie Gesundheit und Soziales, gefolgt von Telekommunikation und Medien (u. a. Fragen des Datenschutzes beim Internet) und Wissenschaft und Forschung. Weiterhin zurückgegangen sind Eingaben im Bereich der Inneren Sicherheit.

6.3 Zusammenarbeit mit dem Parlament

Die Zusammenarbeit mit dem Abgeordnetenhaus konzentrierte sich auf die Beratungen im Unterausschuss „Datenschutz und Informationsfreiheit“ des Ausschusses für Inneres, Sicherheit und Ordnung. In insgesamt elf Sitzungen wurde im Wesentlichen der Jahresbericht 2001 erörtert. In sechs Beschlüssen zu kontroversen Themen wurde der Senat zur Verbesserung des Datenschutzes aufgefordert. Sie wurden in der Sitzung des Abgeordnetenhauses am 29. Januar 2004 angenommen[163]. In den Reden der Vorsitzenden des Unterausschusses Marion Seelig (PDS) und des Berliner Beauftragten für Datenschutz und Informationsfreiheit wurde erneut die konstruktive Zusammenarbeit in diesem Gremium betont[164].

[163] vgl. Anhang 1
[164] vgl. Anhang 2

Neu eingeführt wurde im Unterausschuss eine aktuelle Viertelstunde, in der ungeachtet formeller Beratungspunkte eine Aussprache über die jeweils öffentlich erörterten Datenschutzprobleme stattfand.

6.4 Kooperation 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).

Im Berichtsjahr hatten wir den Vorsitz in der Arbeitsgemeinschaft der Obersten Aufsichtsbehörden für den Datenschutz („Düsseldorfer Kreis“), von der in zwei Sitzungen am 8./9. Mai sowie am 27./28. November eine Vielzahl von Problemen aus dem Bereich der Privatwirtschaft erörtert wurde. Deutlich wurde, in welchem Umfang die Vorgaben aus der Europäischen Union zunehmend auch die Praxis des Datenschutzes in Deutschland beeinflussen[165]. Den Vorsitz im laufenden Jahr übernahm die Oberste Aufsichtsbehörde in Bayern.

Im Rahmen des „Düsseldorfer Kreises“ leiten wir ferner die Arbeitsgruppen für „Internationalen Datenverkehr“ sowie für „Telekommunikation, Tele- und Mediendienste“. Über die Ergebnisse wurde oben berichtet[166].

Im ersten Halbjahr 2003 betreuten wir auch die Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands, der die Informationsfreiheitsbeauftragten der Bundesländer Berlin, Brandenburg, Nordrhein-Westfalen und Schleswig-Holstein angehören. In der Sitzung am 26. Mai wurde ein Beschluss gefasst, in dem „Gleiche Transparenz in Verwaltung und Archiven“ gefordert wurde[167].

Das zentrale Gremium für die Zusammenarbeit in Deutschland ist die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die unter dem Vorsitz des Sächsischen Datenschutzbeauftragten Dr. Thomas Giesen am 27./28. März in Dresden und am 25./26.September in Leipzig tagte. Die Vielzahl von Beschlüssen[168] zeigt erneut die Bandbrei-

---

[165] vgl. 4.7.1
[166] vgl. 4.7.2 und 5.
[167] Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2003“, S. 110
[168] a. a. O., S. 11 ff.

te dieser Zusammenarbeit. Den Vorsitz im laufenden Jahr hat der Landesbeauftragte des Saarlandes Karl Albert.

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

Auf europäischer Ebene ist der Berliner Beauftragte für Datenschutz und Informationsfreiheit deutscher Ländervertreter in der Art. 29-Datenschutzgruppe, der alle europäischen Datenschutzinstitutionen angehören und die die Europäische Kommission in Datenschutzfragen berät.

Unter unserem Vorsitz tagte erneut zweimal die Internationale Arbeitsgruppe Datenschutz in der Telekommunikation im Rahmen der Internationalen Konferenz der Datenschutzbeauftragten, und zwar am 17./18. März auf Einladung des Datenschutzbeauftragten des Kantons Zürich, Dr. Bruno Baeriswyl, sowie am 2./3. September in Berlin[169]. Damit verbunden war wie alle zwei Jahre ein Symposium bei der Internationalen Funkausstellung, diesmal zu „Datenschutz und Informationsfreiheit im Internet“, eine Veranstaltung, die unseren Beitrag zum „Jahr der Informationsfreiheit“ bildete[170].

Schließlich wurde am 7. April auf Einladung des brandenburgischen Beauftragten und uns in Zusammenarbeit mit der Europäischen Akademie für Informationsfreiheit und Datenschutz die Internationale Konferenz der Informationsbeauftragten (ICIC) gegründet, an der 14 Institutionen aus 11 Ländern teilnahmen und die größtes Interesse fand[171].

6.5 Europäische Akademie für Informationsfreiheit und Datenschutz

Nach ihrer Gründung 2002, der Eröffnungsveranstaltung und einer Sitzung des Complaint Handling Workshop der Europäischen Datenschutzkonferenz[172] wurde der Aufbau intensiv fortgesetzt. Auf die Gründung der ICIC[173] folgte im Mai ein Workshop zum Identity Management, im August ein Workshop für Rechtsanwälte zu Datenschutzgarantien durch verbindliche Unternehmensregelungen sowie im November die 5. Sitzung der Mittel- und Osteuropäischen Datenschutzbeauftragten**,** in deren Mittelpunkt der Datenschutz bei der Offenlegung

[169] vgl. 5.2
[170] vgl. 4.9.1
[171] vgl. 4.9.1
[172] JB 2002, 6.5
[173] vgl. 6.4

der Akten der Geheimdienste ehemaliger sozialistischer Länder stand. Hier hat der frühere Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR, Dr. Joachim Gauck, als Gastredner von seinen wertvollen Erfahrungen berichtet. Die Konstituierung eines internationalen Beirats, in dem kompetente Datenschutzexperten aus Politik, Verwaltung, Praxis und Wissenschaft versammelt sind, ist in Vorbereitung.

Zwei größere, miteinander verbundene Kooperationsprojekte der Europäischen Akademie für Informationsfreiheit und Datenschutz mit der Bertelsmann Stiftung wurden im vergangenen Jahr von uns unterstützt. Zum einen handelte es sich um eine internationale Vergleichsstudie, die einen möglichst vielschichtigen Überblick über Regelungen zur Informationsfreiheit bieten soll. Als Exempel dienten sechs Staaten, deren jeweilige Ausgestaltung der Informationsfreiheit näher beleuchtet wurde. Hierzu gehörten die USA, deren Freedom of Information Act das bekannteste Beispiel eines Informationsfreiheitsgesetzes darstellt, Kanada, insbesondere im Hinblick auf die Verbindung der Aufgaben des Datenschutz- und Informationsbeauftragten, Ungarn als Vertreter der osteuropäischen Transformationsstaaten und Schweden als das Land, das über die längste Tradition der Informationsfreiheit verfügt. Mit Thailand und Südafrika wurden auch zwei Schwellenländer untersucht, wobei das thailändische Modell insbesondere deshalb von Interesse war, weil Datenschutz hier als Ausnahmeregelung eines Informationsgesetzes gestaltet ist, und Südafrika, da im dortigen IFG auch Regelungen zum Zugang zu Informationen bei Privaten enthalten sind. Ziel dieser Untersuchung ist es insbesondere, politischen Entscheidungsträgern eine umfangreiche Informationsgrundlage zu liefern, anhand derer die Erarbeitung und Verabschiedung eines Bundesinformationsfreiheitsgesetzes vorangetrieben werden kann.

Diesem Ziel diente auch eine Fachkonferenz mit internationalen Experten zum Thema „Informationsfreiheit und der transparente Staat“ am 8. April 2003 in der Repräsentanz der Deutschen Gesellschaft für Technische Zusammenarbeit in Berlin. Zu den über 100 Teilnehmern gehörten die Mitglieder der tags zuvor gegründeten Internationalen Konferenz der Informationsbeauftragten. Neben Stellungnahmen aus Politik, Wirtschaft, Journalismus und Verwaltung zur Notwendigkeit oder Verzichtbarkeit eines Bundesinformationsfreiheitsgesetzes bot diese Konferenz Gelegenheit, an Erfahrungen mit existierenden Informationsfreiheitsgesetzen zu partizipieren. ?
?

Berlin, 30. März 2004

Prof. Dr. Hansjürgen Garstka
Berliner Beauftragter für Datenschutz und Informationsfreiheit

((Anhang 1))

Ergebnisse der Beratungen des Unterausschusses „Datenschutz und Informationsfreiheit“

Beschlussempfehlung

des Ausschusses für Inneres, Sicherheit und Ordnung vom 8. Dezember 2003

zur Vorlage – zur Kenntnisnahme –

Stellungnahme des Senats zum Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2001

Drs 15/591

Das Abgeordnetenhaus wolle beschließen:

Die Vorlage – zur Kenntnisnahme – Drs 15/591 – wird unter der Maßgabe folgender Beschlüsse zur Kenntnis genommen:

zu Bekämpfung des Rechts- und Linksextremismus
(4.1.2, Drs S. 65 ff)

Der Senat wird aufgefordert, dafür zu sorgen, dass Platzverweise und Personalienfeststellungen weiterhin nicht allein der Anlass für die Speicherung unverdächtiger Personen in bundesweiten Dateien über links orientierte und rechts orientierte Gewalttäter sowie politisch motivierte Ausländerkriminalität sein sollen.

zu Polizeiberichte an alle
(4.1.2, Drs S. 70 ff))

Der Senat wird aufgefordert, dafür zu sorgen, dass die Versendung personenbezogener Polizeiberichte an andere als die Strafverfolgungsbehörden auf das erforderliche Maß beschränkt wird.

zu Sicherheit im Landesnetz
(3.6, Drs S. 55 ff))

Der Senat wird aufgefordert, dafür zu sorgen, dass bei der Übertragung personenbezogener Daten über das Berliner Landesnetz oder über andere Übertragungswege zwischen unterschiedlichen Standorten der Verwaltung zur Gewährleistung ihrer Vertraulichkeit und Integrität (§ 5 Abs. 2 Nr. 1 und 2 Berliner Datenschutzgesetz) geeignete Verschlüsselungstechniken (z. B. die vom Landesbetrieb für Informationstechnik angebotenen Verschlüsselungssysteme) eingesetzt werden.

zu Petienten im Leistungssystem
(4.4.2, Drs S. 99 ff))

Der Senat wird aufgefordert, dafür zu sorgen, dass die seiner Aufsicht unterliegenden Krankenkassen unverzüglich die Konsequenzen aus der Entscheidung des Bundessozialgerichts vom 23. Juli 2002 (Az.: B 3 KR 64/01R) ziehen und medizinische Unterlagen von den Krankenhäusern nur noch dem medizinischen Dienst der Krankenkassen übermittelt werden.

zu Wechselnde Verantwortung für Patientenunterlagen
(4.4.2, Drs S. 103 ff)

Der Senat wird aufgefordert, zu Beginn des Jahres 2004 eine Gesetzesregelung zur datenschutzgerechten Verwaltung von herrenlosen Patientenunterlagen herbeizuführen, sei es landesrechtlich oder ggf. per Bundesratsinitiative bundesrechtlich.

zu Kontrolle eines Krankenhauses der Vivantes GmbH
(4.4.2, Drs S. 107 ff))

Nach Feststellung besonders erheblicher Mängel bei der Sicherheit der informationstechnischen Infrastrukturen und Systeme, mit denen personenbezogene Daten der Patienten verarbeitet werden, sowie bei Schutz der patientenbezogenen Bild- und Textunterlagen gegen Zerstörung, Manipulation und unbefugten Datenzugriff in einem Klinikum des Krankenhaus-

unternehmens Vivantes Netzwerk für Gesundheit GmbH wird der Senat aufgefordert, dafür zu sorgen, dass bis Mitte 2004 ein konzernweit geltendes Sicherheitskonzept für den Umgang mit patientenbezogenen Daten entwickelt und umgesetzt wird.

Berlin, den 8. Dezember 2003

Der Vorsitzende des Ausschusses für Inneres, Sicherheit und Ordnung

Peter Trapp

((Anhang 2))

Reden im Abgeordnetenhaus am 29. Januar 2004 zur Beschlussempfehlung über den Jahresbericht 2001 des Berliner Beauftragten für Datenschutz und Informationsfreiheit

Rede des Berliner Beauftragten für Datenschutz und Informationsfreiheit, Prof. Dr. Hansjürgen Garstka:

„Herr Präsident, sehr geehrte Damen und Herren,

seit einigen Jahren nimmt dieses Haus den Abschluss der Beratung unserer Jahresberichte im Unterausschuss Datenschutz und Informationsfreiheit des Innenausschusses zum Anlass, einen Blick auf die Situation des Datenschutzes im Land Berlin zu werfen. Die dort erarbeiteten Beschlussvorlagen geben dabei natürlich nur ein sehr bruchstückhaftes Bild: Sie bündeln einige wenige Probleme, bei denen Grund besteht, den Senat zu Maßnahmen zur Verbesserung des Datenschutzes aufzufordern. So speziell sie allerdings erscheinen mögen, deuten allerdings auch die Beschlüsse zum Jahresbericht 2001 auf grundlegende Probleme bei der Durchsetzung der informationellen Selbstbestimmung hin:

- die Tendenz, die Speicherung personenbezogener Daten in polizeilichen Informationssystemen auch dann vorzunehmen, wenn kein konkreter Tatverdacht vorliegt,
- gelegentliche Leichtfertigkeit bei der Nutzung von Verteilern mit Adressaten personenbezogener Dokumente,
- die mangelhafte Bereitschaft, bei der Einführung informationstechnischer Verfahren auch hinreichende Mittel für die Datensicherheit aufzubringen,
- die Neigung von Krankenkassen, unter Umgehung gesetzlich vorgeschriebener Übermittlungswege unmittelbar Zugriff auf Patientendaten zu nehmen,
- überhaupt bei allen Beteiligten im Gesundheitssystem Nachlässigkeiten bei der Sicherung patientenbezogener Unterlagen und Datenbestände.

Ich hoffe, dass durch die Beschlussfassung deutliche Anstöße zur Verbesserung des Datenschutzes in unserem Land gegeben werden.

Der vorliegende Jahresbericht deckt im Wesentlichen einen Zeitraum ab, der noch nicht von den Ereignissen des 11. September 2001 überschattet war. Aber bereits bald nach diesem

monströsen Terroranschlag zeigte sich, wie schnell weltweit die Bereitschaft vorhanden war, angesichts derartiger Bedrohungen die informationelle Selbstbestimmung als zweitrangig, ja gar als hinderlich zu betrachten. So mussten wir im Bericht selbst den Bundesinnenminister mit der völlig überzogenen Äußerung zitieren, der Datenschutz sei zu überprüfen und ‚dort zu lockern, wo Datenschutz zu Terroristenschutz werde'.

Die anfängliche Aufregung hat sich in den vergangenen beiden Jahren jedenfalls in unserem Land gelegt und ist wieder einem sachlicheren Umgang mit dem Datenschutz auch im Sicherheitsbereich gewichen. Der Berliner Gesetzgeber hat etwa bei der Anpassung des Landesverfassungsschutzgesetzes an das deutlich hinter den Vorstößen anderer Staaten zurückbleibende Terrorismusbekämpfungsgesetz des Bundes Augenmaß walten lassen. Das Hauptinteresse wendete sich vielmehr der datenschutzgerechten Gestaltung neuer informationstechnischer Verfahren zu, die zur Meisterung der schwierigen haushalts- und strukturpolitischen Probleme einerseits, zur Fortentwicklung der Kommunikationsbeziehungen der Behörden untereinander und dieser mit ihren Klienten andererseits für erforderlich gehalten werden. Auch diese Themen haben unseren Unterausschuss in den vergangenen Monaten bereits beschäftigt. Künftige Jahresberichte werden sich dem sicherlich verstärkt widmen müssen.

An Sie möchte ich wiederum die Bitte richten, bei allen Gesetzen und anderen Vorlagen, die das Haus durchlaufen, der informationellen Selbstbestimmung den ihr gebührenden Rang einzuräumen. In den nächsten Monaten werden nicht einfache Aufgaben auf uns zukommen. So ist die Novellierung des Melderechts, auch durch Beschlüsse dieses Hauses mehrfach angemahnt, in Gang gekommen. Datenschutzgesetz und Informationsfreiheitsgesetz müssen überarbeitet und - trotz der dem Abgeordnetenhaus gegenüber geäußerten Skepsis der Innenverwaltung - in einem einheitlichen Informationsgesetzbuch des Landes zusammengefasst werden. eGovernment wird seinen legislativen datenschutzrechtlichen Rahmen finden müssen. Neue technische Entwicklungen, etwa die in den letzten Wochen heiß diskutierte Videoüberwachung verbunden mit automatischer Nummernschildkontrolle, fordern das Eingreifen des Gesetzgebers, wenn sie denn genutzt werden sollen.

Die Mitglieder des Unterausschusses Datenschutz und Informationsfreiheit aller Fraktionen haben bei der Beratung des Jahresberichts 2001, aber auch aller anderen anstehenden Themen in der Sache sehr konstruktiv und im persönlichen Umgang bei allen Differenzen, die selbstverständlich auch beim Datenschutz bestehen, sehr wohlmeinend zusammengearbeitet. Hierfür möchte ich mich, auch im Namen meiner Mitarbeiterinnen und Mitarbeiter, sehr herzlich bedanken."

Rede der Vorsitzenden des „Unterausschusses Datenschutz und Informationsfreiheit“, Frau Marion Seelig (PDS):

„Frau Präsidentin! Meine Damen und Herren! Sehr geehrter Herr Dr. Garstka!

In der Eigenschaft als Vorsitzende des Unterausschusses Datenschutz möchte ich die Gelegenheit unserer Beschlussempfehlung nutzen, um mich bei den Mitgliedern unseres kleinen Ausschusses zu bedanken, bei Ihnen Herr Dr.Garstka – da kann ich mich der Präsidentin nur anschließen – und ebenso bei Ihrem Haus für die fachkundige Begleitung. Aber auch bei Herrn Baer, unserem Ausschussassistenten, bedanke ich mich, denn wir agieren ab und zu etwas unorthodox. Ich halte es wie die Vorsitzende des so viel größeren und gewichtigeren Hauptausschusses, weil wir eines gemeinsam haben: Wir sind mit allen Bereichen der Berliner Verwaltung befasst, und das ist nicht immer eine Freude. Es muss aber deutlich festgehalten werden, dass der Stellenwert des Datenschutzes in den letzten Jahren zugenommen hat, dass er ernster genommen wird und die meisten Verwaltungen es sich inzwischen schon überlegen, dass es ihnen nützt, den Beauftragten für Datenschutz und Informationsfreiheit sehr frühzeitig in ihre Überlegungen einzubeziehen. Deshalb ist unsere Beschlussempfehlung auch übersichtlich ausgefallen, weil es sehr häufig gelungen ist, im Rahmen der Debatten und der Verhandlungen Beanstandungen in Sachen Datenschutz gemeinsam mit den Verwaltungen aus der Welt zu schaffen. Dazu trägt auch bei, dass die Auseinandersetzung mit den Sachfragen in diesem Ausschuss kurioserweise deutlich vor parteipolitischen und sonstigen Differenzen steht. Kurios nenne ich es deshalb, weil Datenschutz und auch Informationsfreiheit keine technokratischen, sondern hoch politische Themen sind. Umso mehr freue ich mich, dass wir es alle mit großer Ernsthaftigkeit und Kritikfähigkeit gegenüber Verstößen behandeln. Ich kann es mir nur so erklären, dass die Befassung mit einem Thema, das leider immer weniger Bürgerinnen und Bürger zu bewegen scheint, die Augen für die zunehmenden Gefahren der Informationsgesellschaft schärft. Wenn wir im Berliner öffentlichen Dienst nicht mit gutem Beispiel vorangehen, werden wir uns der Zumutungen aus der privaten Wirtschaft immer weniger erwehren können. Ich denke an die zunehmende Privatisierung des öffentlichen Raums, die wir an jedem kommerziellen Gebäude feststellen können, wo Kameras nicht nur den Eingang und das Gebäude erfassen. Ich denke auch an weitere Zumutungen, die in Vorbereitung sind, wie beispielsweise elektronische Chips in der Schuh- und Textilbranche, die an den Erzeugnissen belassen und nicht im Kaufhaus entfernt werden. Man kann sich vorstellen, in welchem Maße Informationen über Kundinnen und Kunden gesammelt werden. Ich denke auch an immer mehr Rabattkarten für den ‚gläsernen Kunden’ und an die gefährlichen Schlupflöcher im Internet.

Im Unterausschuss ‚Datenschutz und Informationsfreiheit' werden –und davon spricht unsere Beschlussempfehlung– auch die heiklen Sicherheitsbelange nicht ausgespart. Wenn wir über Dinge so konkret reden wie in unserem Ausschuss, habe ich bei keiner Partei den Eindruck, dass die Grund- und Freiheitsrechte keinen Stellenwert hätten.

Für die Zukunft wünsche ich mir weiterhin diese gute Zusammenarbeit, auch viele Konsensbeschlüsse um des Datenschutzes und der Informationsfreiheit willen sowie auch in der Zukunft einen engagierten und streitbaren Beauftragten für Datenschutz und Informationsfreiheit. Allzu viele Sorgen mache ich mir um die Erfüllung dieser Wünsche nicht. – Danke schön!“

Auszug aus dem Geschäftsverteilungsplan

Stand: 1. Januar 2004

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, E-Government
Dipl.-Germanistin Laima Nicolaus	Redaktion von Veröffentlichungen, Bibliothek, Rechtsprechungssammlung, Sekretariat
	Allgemeine Verwaltung
Doris Werth	Haushaltsplanung und -bewirtschaftung, Personal, Büroorganisation, Beauftragte für den Haushalt
Carola Peplau	Rechnungsstelle, Sekretariat
	Bereich Recht
Dagmar Hartge	Bereichsleiterin (kommissarisch) AG: Verfassungsorgane, Finanzen, Nachrichtendienste, Grundsatzangelegenheiten des Datenschutzrechts sowie des Strafverfolgungs-, Sicherheits- und Ordnungsrechts
Kerstin Göhler	Sekretariat, Archiv

	Bürgeroffice
Volker Brozio	Leitung; Öffentlichkeitsarbeit; AG: Stadtentwicklung, Justiz
Detlef Schmidt	AG: Inneres, Staatsanwaltschaft, Bezirksämter
Sabine Krissel	Geschäftsstelle, Sekretariat
Sandra Ließmann	Sekretariat
	Recht I
Dr. Ulrich von Petersdorff	AG: Gesundheit und Soziales, Kultur
Dipl.-Volkswirt **Dr. Rainer Metschke**	AG: Wissenschaft, Forschung und Statistik; Schule
	Recht II
Daniel Holzapfel	AG: Wirtschaft, Zivilrecht (insbes. Vereinsrecht)
Birgit Saager	AG: Personaldaten, Wirtschaft
	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
Nicole Berger	Sekretariat, Informationsverteilung Führung des Registers nach §§ 4 d, 4 e BDSG, Organisation der Beteiligung an Kontrollen im privaten Bereich
	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, LIT)
Jürgen Horn	Status und Beratung der behördlichen und betrieblichen Datenschutzbeauftragten, Koordination der Kontrollen im privaten Bereich, Organisation des Datenschutzes, Meldepflicht AG: Verfassungsorgane, Senatskanzlei, Bauen und Wohnen, Umweltschutz, Justiz, Betriebe, Bildung

	Behördlicher Datenschutzbeauftragter
Dipl.-Informatiker Ralf Hauser	Microsoft-Betriebssysteme, Office-Produkte (auch Nicht-MS), Lokale Netze incl. Wireless LAN, Mobile Computer AG: Gesundheit, Kultur, Schule, Verkehr
	Informatik II
Roman Maczkowsky / Dipl.-Dokumentar Axel Tönjes	Berliner Landesnetz, Telekommunikationssysteme AG: Inneres (Senatsverwaltung, Polizei, Feuerwehr, Verfassungsschutz) Systemkoordinatoren
Carsten Schmidt	UNIX, LINUX, SAP R/3, Firewallsysteme, Wartung und Fernwartung AG: Soziales, Inneres (Landesverwaltungsamt, Standesämter), Arbeit, Jugend und Sport Systemverwaltung Kommunikationsnetz
André Drescher	Systemverwaltung Büro-Netz, Anwendungsprogrammierung, Benutzerbetreuung Büro-Netz, Webmaster

Berliner Beauftragter für
Datenschutz und Informationsfreiheit (BlnBDI)
An der Urania 4 - 10, 10787 Berlin
Telefon: (0 30) + 1 38 89-0,
Telefax: (03 0) 2 15 50 50
E-Mail: mailbox@datenschutz-berlin.de,
Internet:http://www.datenschutz-berlin.de

Agenda:
AG = Arbeitsgebiet