BERICHT

des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2007

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 28. März 2007*** *vorgelegten Jahresbericht 2006 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 2007 ab.*

Wiederum werden die über Berlin hinaus bedeutsamen Dokumente in einem gesonderten Band („Dokumente 2007“) veröffentlicht.

Dieser Jahresbericht ist über das Internet (http://www.datenschutz-berlin.de/) abrufbar.

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/

Druck: Brandenburgische Universitätsdruckerei
und Verlagsgesellschaft Potsdam mbH

Inhaltsverzeichnis

Einleitung

Der spätere Friedensnobelpreisträger Al Gore hat 2006 den mit einem „Oscar“ ausgezeichneten Film „An Inconvenient Truth“ (Eine unbequeme Wahrheit) gedreht, der sich mit der globalen Erwärmung beschäftigt. Genauso wichtig wie unsere physikalische Umwelt ist mittlerweile unsere informationelle Umwelt, also all das, was wir an digitalen Spuren in Telekommunikationsnetzen, insbesondere im Internet, aber auch an biometrischen Spuren z. B. bei Reisen hinterlassen. Auch hier müssen wir uns mit unbequemen Wahrheiten auseinandersetzen: Gerade im zurückliegenden Jahr sind Entscheidungen getroffen worden, die dazu führen, dass massenhaft personenbezogene Daten von staatlichen und privaten Stellen verdachtsunabhängig gespeichert werden.

Mit der ab dem 1. Januar 2008 verpflichtend vorgeschriebenen Speicherung sämtlicher Verkehrsdaten in Telekommunikationsnetzen ist ein datenschutzrechtlicher Damm gebrochen: Diese Daten bleiben für ein halbes Jahr gespeichert, auch wenn unsere Telefonrechnungen längst bezahlt sind. Dies wurde zwar unter dem Eindruck von Terroranschlägen beschlossen, mittlerweile sollen damit aber auch Beleidigungen am Telefon verfolgt werden können. Zugleich wird über jede Person, die aus Europa in die USA reisen oder dort nur zwischenlanden will, ein umfangreicher Datensatz an die US-Behörden auf Vorrat übermittelt, der dort auf Jahre hinaus gespeichert bleibt und für letztlich nicht kontrollierbare Zwecke genutzt werden kann. Nachdem die Europäische Union über mehrere Jahre hinweg dem Ansinnen der US-Regierung widerstanden und versucht hat, die Grundsätze des Datenschutzes auch im transatlantischen Reiseverkehr durchzusetzen, sollen jetzt nach dem Willen der Europäischen Kommission dieselben Grundsätze auch für Reisen in die und aus der Europäischen Union gelten. Der Richter am Bundesverfassungsgericht Udo di Fabio hat dies treffend als „präventionstechnischen Überbietungswettbewerb“ bezeichnet[1]. Eine überhandnehmende Überwachung gefährdet die freie Kommunikation und Bewegung in einer freien Gesellschaft.

So paradox es klingen mag: Die überhandnehmende Überwachung gefährdet darüber hinaus auch unsere Sicherheit. Der Vorsitzende der niederländischen Datenschutzbehörde, Jakob Kohnstamm, hat zu diesem Vorschlag der Kommission das treffende Bild verwandt, hier werde ein „Heuhaufen“ von Informationen aufgeschichtet, um darin die „Nadel“, also die entscheidende Information, aufzufinden. Dieses Bild lässt sich auf die Vorratsdatenspeicherung allgemein übertragen: Immer größere Datenbanken und Datenmengen führen nicht automatisch zu mehr

[1] Die Welt v. 12. November 2007

Sicherheit. Vielmehr ist die Wahrscheinlichkeit groß, dass die Masse der Informationen über unverdächtige Bürger gerade verhindert, dass reale Verdachtsmomente erkannt werden. Dadurch wird Sicherheit gerade nicht erhöht, sondern im Gegenteil drastisch gemindert.

Bei einer Konferenz der Datensicherheitsexperten im Herbst 2007 in London berichtete der Präsident des veranstaltenden Unternehmens RSA, Art Coviello, dass 2006 weltweit 176 Exabytes an Daten erzeugt worden seien. Das entspricht 3 Millionen Mal dem Inhalt sämtlicher Bücher. Eine derart gewaltige Menge an Informationen (die zum großen Teil personenbezogen sein dürfte) lässt sich weder verwalten noch schützen. Auf derselben Konferenz berichtete ein Vertreter von Microsoft, dass die Zahl der „Trojan Downloaders", also Schadprogramme zum Ausspähen von Daten, vom 2. Halbjahr 2006 bis zum 1. Halbjahr 2007 sprunghaft von 1 auf 5,9 Millionen angestiegen sei[2].

In Großbritannien gab es im vergangenen Jahr eine ganze Serie von dramatischen Datenverlusten, seit im November 2007 zwei CDs mit vertraulichen Daten von mehr als 25 Millionen Personen, die Kindergeld erhielten, auf dem Postweg verloren gingen. Diese Pannen haben unterschiedlichste Ursachen, die vom britischen Information Commissioner scharf kritisiert worden sind. In Deutschland sollte man sich allerdings vor der Annahme hüten, Derartiges sei bei uns ausgeschlossen. Je größer die Datenmengen werden und je bequemer sie mit verschiedensten Medien übermittelt, ausgelesen und kopiert werden können, desto wahrscheinlicher ist es, dass Daten nicht nur verloren gehen, sondern auch von Kriminellen für Zwecke des Identitätsdiebstahls genutzt werden.

Insgesamt zeigt sich, dass die permanente Maximierung der Verarbeitung personenbezogener Daten für alle möglichen Zwecke zwangsläufig zu mehr Unsicherheit führt. Je immenser die Datenmengen sind, desto schwieriger wird es, sie effektiv vor kriminellen Angriffen zu sichern. Auch wenn diese riesigen Datenhalden zunächst für legitim erscheinende Einzelzwecke angehängt werden, wächst alsbald der Druck, sie für Zwecke nutzbar zu machen, für die sie ursprünglich nicht gedacht waren. Damit steht der datenschutzrechtliche Grundsatz der Zweckbindung, der den Betroffenen Sicherheit über die Verwendung ihrer Daten geben soll, zur Disposition. Stattdessen ist es an der Zeit, gerade im Interesse größerer Datensicherheit und besseren Datenschutzes wieder zu einer größtmöglichen Datensparsamkeit zurückzukehren, wie sie das Bundesdatenschutzgesetz seit 2001 vorschreibt.

[2] Wobst, Reinhard: Große Datenmengen verhindern Sicherheit – trübe Aussichten, iX 12/2007, S. 22

Auch die Debatte über die sog. Online-Durchsuchung[3] zeigt eines ganz deutlich: Während die Verfassungsschutzbehörden des Bundes und der Länder einerseits mit Recht auf die Gefahren der Wirtschaft- und Industriespionage hinweisen, die im Zeitalter des Internets drastisch zugenommen haben, dringen vor allem das Bundesinnenministerium und das Bundeskriminalamt darauf, die sog. Online-Durchsuchung zu legalisieren. Damit würde das Vertrauen in die Nutzbarkeit des Internets auch für den Nachrichtenaustausch zwischen Bürgerinnen und Bürgern einerseits und dem Staat andererseits grundlegend erschüttert. Sämtliche Bemühungen, die die Bundesregierung mit Recht zur Erhöhung des Sicherheitsbewusstseins und der Anstrengungen für mehr Vertrauenswürdigkeit im Netz unternimmt, werden in einem zentralen Punkt konterkariert. Auch zeigt das Beispiel der Online-Durchsuchung, dass eben nicht nur verdächtige Personen von ihr betroffen sein würden; wäre dem so, dann könnte nach geltendem Strafprozess- oder Polizeirecht der jeweilige Computer sichergestellt und untersucht werden. Vielmehr werden immer auch unverdächtige Personen von einer solchen Maßnahme betroffen sein. Der Staat würde auf diese Weise Unsicherheit produzieren, statt sie zu bekämpfen.

Auf dem Umschlag dieses Jahresberichts findet sich das neue Markenzeichen (Logo) des Berliner Beauftragten für Datenschutz und Informationsfreiheit. Das Kürzel „ID“ hat eine doppelte Bedeutung: Zum einen steht es für „Informationsfreiheit“ und „Datenschutz“, wobei die Informationsfreiheit bewusst und abweichend von der offiziellen Behördenbezeichnung vorangestellt worden ist. Zum anderen steht „ID“ auch für das englische „Identity“ (Identität) und soll verdeutlichen, dass das Thema des Schutzes der eigenen Identität und Persönlichkeit vor Registrierung, Ausspähung und automatisierter Ausgrenzung in nächster Zeit stark an Bedeutung zunehmen wird. Es wird wesentlich darauf ankommen, dass Datenschutzbeauftragte sich an der Entwicklung von Instrumenten zum informationellen Selbstschutz z. B. durch ein datenschutzfreundliches Identitätsmanagement beteiligen. Insofern ist unser neues Logo auch als ein Denkanstoß zu verstehen. Dieser Jahresbericht zeigt auch bereits bestehende Möglichkeiten des Selbstschutzes[4] auf und ermutigt dazu, sie auszuschöpfen.

[3] vgl. 2.1
[4] vgl. 2.2

1.1

1 Technische Rahmenbedingungen

1.1 Entwicklung der Informationstechnik – die Konvergenz als Motor

Konvergenz (zu spätlateinisch *convergere*, sich hinneigen) bedeutet allgemein *Annäherung* (auch: das Zusammenstreben, das Aufeinanderzugehen, Gegensatz: Divergenz) oder *Übereinstimmung* (von Meinungen, Zielen etc.). So hat der Begriff der Konvergenz in vielen Fachgebieten spezielle Bedeutungen entwickelt.[5]

„Konvergenz" war auch der dominierende Begriff auf der Cebit 2007 und benennt im Zusammenhang mit der Informationstechnik das Zusammenstreben aller möglichen Technologien, die digitale Daten verarbeiten bzw. mit digitalen Daten gesteuert werden. Auf Letzteres sei besonders hingewiesen: Es geht nicht mehr nur um das Zusammenführen von Informations- und Kommunikationstechnik (IuK), den jeweiligen Netzen und Diensten. Längst verschmilzt die Informations- und Kommunikationstechnik mit Technologiebereichen, die auf den ersten Blick niemanden auf die Idee bringen würden, dass sie etwas mit Informationstechnik zu tun haben könnten: Medizinische Diagnose- und Therapiesysteme, Kraftfahrzeuge, Flugzeuge, Lagerhallen, Supermärkte, Bekleidung. Was es lange gab, bevor die Informations- und Kommunikationstechnik ihren Siegeszug begann, sind heute vielfach IuK-Systeme in unterschiedlichen Verpackungen und zu unterschiedlichen Zwecken.

1.1.1 Die Konvergenz in der bisherigen Entwicklung der IuK-Technik

Wir haben an dieser Stelle schon häufiger über Techniken und Anwendungen gesprochen, die bereits aus der Konvergenz entstanden sind:

Erstmals berichtete der Berliner Datenschutzbeauftragte im Jahre 1984 ausführlich über den damals eingeführten Dienst „Bildschirmtext", der damals noch grob gerasterte, grafisch präsentierte Informationen aus Datenbanken über das Telefonnetz zu den Endgeräten übertrug. Zum Teil waren diese Endgeräte bereits kleine Computer, die Programme ausführen konnten, die ebenfalls über das Telefonnetz in die Rechner übertragen wurden. Wäre der technische Hintergrund nicht ein

[5] aus Wikipedia (http://de.wikipedia.org/wiki/Konvergenz), Stand: 15. Dezember 2007

völlig anderer, könnte man von einem Vorgänger des World Wide Web sprechen. Allerdings war Bildschirmtext bereits das Ergebnis einer Konvergenz zwischen Informations- und Telekommunikationstechnik. Mit ihm begann der Siegeszug der Neuen Medien. Ein nächster Schritt bestand im Folgejahr mit der Erprobung eines Fernmess- und -wirkdienstes TEMEX durch die Deutsche Bundespost. Hier wurde die Grenze der IuK-Technik bereits überschritten, denn es konnten bereits technische Geräte, die ansonsten nichts mit IuK zu tun hatten, über Kommunikationswege gesteuert werden.

1994 stand dann erstmals das Internet im Fokus unseres Jahresberichts, das mittlerweile 35 Millionen Benutzer weltweit hatte. Damit hatte die Konvergenz von Telekommunikation und Datenverarbeitung zur IuK-Technik ihren ersten Höhepunkt erreicht. Durch die Integration von Sprach- und Datenkommunikation wurden die Tore zum heutigen Internet geöffnet, denn nach und nach wurde klar, dass alles, was zu Buchstaben, Bildern, Tönen und Filmen gemacht worden war, eben auch digitalisiert werden konnte, wenn man nur die richtigen Formate dazu fand. Ein Jahr später findet erstmals der Begriff „Multimedia“ im Zusammenhang mit der Digitalisierung von Bild- und Sprachverarbeitung Verwendung.

1998 fällt uns der nächste Schritt auf: „Die Vernetzung informationstechnischer Infrastrukturen geht einher mit dem Zusammenwachsen von Informations-, Telekommunikations- und Televisionstechnik. Das Internet transportiert Daten, Sprache, Bilder, Fernsehübertragungen und Videofilme, also alles, was sich in digitalen Zeichenfolgen darstellen, übertragen und verarbeiten lässt“[6]. An gleicher Stelle beschrieben wir in einem fiktiven Szenario einen implantierten Sensor-Transponder, der über ein in die Sportkleidung integriertes Personal Area Network und ein Mobiltelefon die Notärztin oder den Notarzt alarmiert, wenn die joggende Person einen Herzinfarkt erleidet. Über solche Anwendungen wurde damals öffentlich nachgedacht. 1999 wurde deutlich, dass schon immer mehr Produkte, die man mit der Datenverarbeitung noch gar nicht in Verbindung brachte, mit „Embedded Chips“ ausgestattet waren, mit denen die Konvergenz sich über die IuK-Technik hinaus ausgebreitet hatte. Diskutiert wurde diese Technik im Zusammenhang mit dem Jahr-2000-Problem, dem man vor allem wegen dieser vielen unsichtbaren Steuerungssysteme großen Respekt entgegenbrachte – zum Glück weitgehend unbegründet, wie wir später lernten.

2001 zitierten wir einen früheren IBM-Chef, der die Vision zum Ausdruck brachte, dass bald eine Milliarde Menschen mit einer Million E-Business-Unternehmen über eine Billion vernetzter und intelligenter Geräte interagieren

[6] JB 1998, 2.1

würden. Wir skizzierten weiter ein Szenario mit Gewichtssensoren im Bett, die Diätprobleme der Schlafenden erkennen und den Kühlschrank zur Bestellung von kalorienärmerer Nahrung via UMTS beim Supermarkt veranlassen. Die Diskussion über Pervasive oder Ubiquitous Computing begann, Techniken, die die Konvergenz in Zukunft wesentlich vorantreiben werden.

2002 wurde deutlich, dass sich die heimischen PCs zum Home Entertainment Center entwickelten, bei dem die unterschiedlichsten Unterhaltungsmedien wie Fotobearbeitung und -druck, hochauflösendes Fernsehen, CD- und DVD-Player und -Brenner, Tonaufnahme und -wiedergabe auf dem PC als Zentrum der Freizeitgestaltung verschmolzen hatten. Hinzu kam der PC in seiner weiteren Funktion als universelles Kommunikationsmittel für E- Mail-Austausch und Download von allem, was digital im Netz verfügbar ist.

2003 befassten wir uns erstmals näher mit den RFID-Chips, jenen Transpondern, die automatisch die Lagerhaltung optimieren und an den elektronischen Kassen die Rechnungen addieren sollen. Im Jahr darauf wurde klar, dass auf jeden Menschen in einem entwickelten Land Dutzende von Mikroprozessoren entfielen: Im PC zu Hause, im Festnetz-Telefon, im Handy, die Chipkarten in der Tasche, die elektronisch gesteuerten Haushaltsgeräte, im Auto, im Fotoapparat und in der Unterhaltungselektronik. Ferner war klar, dass die Mikroprozessoren anfingen, miteinander zum kommunizieren, das „Internet der Dinge“ entwickelte sich, das uns vorher nur in fiktiven Szenarien begegnete und mit dem die Konvergenz weiterging, aber sicher noch nicht beendet ist.

Während wir uns 2005 erneut mit der RFID-Technologie auseinandersetzten, auch weil bei der bevorstehenden Fußballweltmeisterschaft 2006 alle Eintrittskarten mit dieser Technik ausgestattet werden sollten, befassten wir uns 2006 mit der Konvergenz zwischen Videoüberwachung, biometrischer Gesichtserkennung und RFID[7] zur Gewinnung präziser Bewegungsprofile, mit der Konvergenz von Telefonie und Internet mit „Voice over IP“[8] sowie mit der Nanotechnologie zur weiteren Miniaturisierung des „Internets der Dinge“.

1.1.2 Wirtschaftliche und technologische Bedeutung der Konvergenz

Die Konvergenz wird in der heutigen Literatur vorwiegend als das Zusammenwachsen der Telekommunikationstechnik, der Informationstechnologie, der Medien und der Unterhaltungstechnologie (Entertainment) (TIME) sowie ihrer An-

[7] vgl. 11.1
[8] vgl. 2.3

wendungen und Branchen gesehen. Die Einbeziehung anderer Technologien wird erst in Zukunft wesentliche wirtschaftliche Bedeutung gewinnen.

Eine volkswirtschaftlich geprägte Studie der Deutschen Bank Research[9] sieht in der Konvergenz der genannten Technologie- und Wirtschaftsbereiche einen wichtigen Impuls für die Wertschöpfungskette, erkennt jedoch mehr darin als das Zusammenwachsen der einschlägigen Branchen. Tatsächlich betrifft die Konvergenz unterschiedliche Ebenen, z. B. Infrastrukturen, Endgeräte und Dienste. Beispiele dafür sind für Infrastrukturen die Konvergenz von Sprach- und Datenkommunikation über die gemeinsame Netzinfrastuktur (IP-Konvergenz), für Endgeräte Smartphones, die die Funktionen von Mobiltelefon und Personal Digital Assistants (PDA) in Kombination mit Online-Diensten darstellen, für Dienste das Interaktive Fernsehen mit den Möglichkeiten zum Teleshopping und Video-on-Demand.

Die Konvergenz wird beschleunigt durch

- die vollständige Digitalisierung von Inhalten und Netzen,
- die zunehmende Verbreitung von breitbandigen Internetzugängen,
- das zunehmende Angebot der mobilen Nutzung solchen Netzzugänge,
- den Abbau von Integrationshemmnissen wie Engpässen bei Speicherkapazitäten, Energieversorgung und Displays,
- die Weiterentwicklung von Schnittstellen zwischen Maschinen wie Bluetooth, Firewire und USB und zwischen Mensch und Maschine wie die Spracherkennung,
- die Erreichbarkeit eines Dienstes über verschiedene Endgeräte.

Die künftige Entwicklung wird kurzfristig schnelle Konvergenzen im Bereich der Endgeräte aufzeigen. Hier lassen sich diverse Funktionen bisher für sich stehender Endgeräte mehr oder weniger beliebig zu neuen Endgeräten kombinieren. Mobiltelefone mit Digitalkamera sind längst Standard selbst bei Billigtelefonen. Die Ergänzung um einen MP3-Player und/oder drahtlose Datenübertragung geht den gleichen Weg.

[9] http://www.ecin.de/mobilebusinesscenter/konvergenz/

Zögerlicher und daher bei einer Betrachtung der Perspektiven und Trends eher langfristiger zu beobachten ist die weitere Konvergenz von Infrastrukturen. Dies zeigt sich am Beispiel des in den USA schon stark verbreiteten Triple Play als Konvergenz von Fernsehen, Festnetz-Telefonie und Internet (im Quadruple Play ergänzt um die Mobilkommunikation) über eine gemeinsame Infrastruktur. In Europa und speziell in Deutschland steht diese Entwicklung erst ganz am Anfang, insbesondere weil „konvergente“ Angebote aus einer Hand noch fehlen. IP-TV oder Video-on-Demand ist technisch verfügbar, kann sich aber erst durchsetzen, wenn auch die Anbieter von Inhalten mit im Boot sitzen.

Bei den Diensten verläuft die Konvergenz ebenfalls eher zögerlich, da komplexe Dienste hohe Bandbreiten benötigen, die noch nicht überall verbreitet sind. Derzeit dominieren noch die Klingeltöne auf dem Feld des Abrufs mobiler Inhalte. Das erwartete Wachstum bei mobilen Informationsdiensten und Musik-Downloads startet auf niedrigem Niveau. Hoffnung auf eine Killerapplikation für UMTS-Handys macht die Konvergenz zweier Technologien, die bisher eher komplementär zu sein schienen: Mobiltelefon und Fernsehen.

Neben den Konvergenzen in den TIME-Branchen sind weitere Konvergenzen zu erwarten und werden – zumindest experimentell – genutzt.

Das intelligente Haus bietet seinen Bewohnerinnen und Bewohnern fast jeden erdenklichen Luxus und Bequemlichkeit, weil es die Funktionen der häuslichen Systeme steuert und optimiert. Die Gebäude-Telematik kann z. B.:

- die Heizungs- und Warmwasserversorgung ökonomisch genauer optimieren,

- Gerätestörungen autonom erkennen und Abhilfe über Telekommunikationssysteme anfordern (automatischer Anruf über Fest- oder Mobilnetz, automatische E-Mail),

- Fernsteuerung von Kühlschränken und Herden, die ebenfalls zur Rückmeldung fähig sind.

Die Zukunft der Gebäude-Telematik wird jedoch nicht nur mit (wirtschaftlichem) Optimismus betrachtet. Abgesehen von Energiesparmaßnahmen wird die Kosten-Nutzen-Relation angesichts aufwändiger Umbauten nicht gesehen, die Massentauglichkeit wird angezweifelt.

1.1

Für die Verkehrs-Telematik, die Ausdruck der Konvergenz von IuK-Technologie, Automobil- und Verkehrsinfrastruktur-Technologie ist, wird vermutet, dass sich der Kostenanteil der Elektronikbauteile eines durchschnittlichen Kraftfahrzeugs gegenüber derzeit 20 % binnen zehn Jahren verdoppeln wird. Dabei handelt es sich z. B. um

- Steuerungen klassischer Bauteile wie Motoren, Bremsen, Fahrwerke, Fahrzeugbeleuchtung, Heizsysteme für Innenraum, Scheiben und Spiegel, Sicherheitstechnik wie Sicherheitsgurte, Airbags usw.,

- die Kommunikation des Kfz mit seiner Umwelt: Abstandswarnungen, Prüfung der Lichtverhältnisse, Auswerten von eingehenden Stau- und Gefahreninformationen,

- die Kommunikation mit anderen Fahrzeugen.

Die Studie der Deutschen Bank geht beim Aufzeigen weiterer Technologiefelder, die der Konvergenz mit der IuK-Technik unterliegen, nicht weiter, wohl weil sie keinen Massenmarkt adressieren. Weitere Bereiche sind z. B.:

- die Telematik in anderen Verkehrsmitteln wie Flugzeugen, Schiffen, Eisenbahnen, in denen sie ähnliche Aufgaben wahrnehmen kann wie bei den Kraftfahrzeugen;

- die Medizintelematik zur Steuerung medizinischer Diagnosesysteme wie Ultraschallgeräte, Computer-Tomografen (CT), Magnetspinresonanz-Tomografen (MRT), Elektroenzephalografie (EEG), Positronen-Emissions-Tomografie (PET) sowie zur Steuerung therapeutischer Systeme in der Nuklearmedizin, der Chirurgie (minimalinvasive Chirurgie, Tele-Chirurgie mit Robotik usw.) und der Hirnforschung; gerade im Bereich der Hirnforschung kündigen z. B. Neuroimplantate eine neue Form der Konvergenz zwischen Menschen und Maschine an;

- die Handelstelematik zur Realisierung virtueller Warenhäuser, RFID- oder mobilfunkbasierter Bezahlsysteme, Homebanking und Homeshopping.

1.1.3 Rechtlicher Rahmen für die Konvergenz

Die gerade aus der Konvergenz folgende dynamische Entwicklung von Infrastrukturen, Endgeräten und Diensten macht es den Gesetzgebern schwer, den nötigen Regulierungsrahmen den aktuellen Entwicklungen anzupassen.

Bereits 1997 wird die Konvergenz der Branchen Telekommunikation, Medien und Informationstechnologie in Hinblick auf ihre ordnungspolitischen Auswirkungen in einem Grünbuch der Europäischen Kommission thematisiert[10]. Damals wurde bereits die Befürchtung ausgesprochen, dass die Entwicklung neuer Dienste von diversen Schranken, so auch rechtlicher Art, behindert werden könnte.

An dieser Befürchtung hat sich offensichtlich zehn Jahre später wenig geändert. In Fachkreisen wird beklagt, dass die rechtlichen Entwicklungen zur Medien- und Telekommunikationsregulierung eher divergieren, während die technologischen Entwicklungen konvergieren[11].

Der Datenschutz spielt in den Veröffentlichungen zur Konvergenz im IuK- und Medienbereich bisher eine untergeordnete Rolle. Allerdings beobachten wir seit langem eine hohe Frequenz rechtlicher Anpassungen im Bereich der „Telemedien“[12]. Dies zeigt, dass der Gesetzgeber versucht, sich der Dynamik, manchmal aber auch der Hektik der technischen Entwicklung anzupassen.

Aus der Sicht des technischen Datenschutzes, insbesondere der IT-Sicherheit, weisen einzelne Beobachtungen auf die Tendenz hin, dass mit der Konvergenz von Infrastrukturen, Geräten und Diensten auch die Konvergenz der IT-Sicherheitsprobleme, die mit den konvergierenden Komponenten verbunden sind, einhergeht. So zeigt das Beispiel von Voice over IP (VoIP), dass diese Konvergenz von Telefonie und Internet die Sicherheitsprobleme des schwächsten Gliedes vererbt. Das bedeutet in diesem Falle, dass VoIP Telefonie mit den Risiken des Internet ist[13].

---

[10] http://ec.europa.eu/avpolicy/docs/library/legal/com/greenpaper_97_623_de.pdf

[11] Artikuliert wurde dies zum Beispiel auf einem Diskussionsforum bei den Medientagen 2007 in München, vgl. http://www.heise.de/newsticker/meldung/98628/from/rss09.

[12] vgl. 12 mit der Darstellung der neuesten Anpassungen

[13] vgl. 2.3

1.2 Datenverarbeitung in der Berliner Verwaltung

1.2.1 IT-Politik für die Berliner Verwaltung

Die IT-Politik des Landes wird nach wie vor von der Arbeit an den prioritären IT-Projekten bestimmt, über die wir im Vorjahr ausführlich berichtet haben[14]. Das Projekt ProStandard zur Verabredung von Standards und Normen für den IT-Einsatz in der Berliner Verwaltung erbrachte – wie im Vorjahr berichtet – zunächst Standardisierungsgrundsätze, die bei der Erarbeitung der IT-Standards 2007 im Jahre 2006 herangezogen wurden. Erfreulicherweise hat diese Regelung ihre Praxistauglichkeit dadurch bewiesen, dass die neuen IT-Standards 2008 pünktlich als Entwurf vorlagen.

Zu den übrigen Projekten, die nicht schon im Vorjahr abgeschlossen worden waren, liegen keine neuen verbindlichen Ergebnisse vor.

1.2.2 IT-Sicherheit in Berlin

Die wichtigste Entscheidung zur Weiterentwicklung der IT-Sicherheit bei den öffentlichen Stellen des Landes war die Aktualisierung der Verwaltungsvorschrift, die die öffentlichen Stellen zur Gewährleistung der IT-Sicherheit anhält. Die IT-Sicherheitsrichtlinie aus dem Jahre 1999[15] wird jetzt ersetzt durch die IT-Sicherheitsgrundsätze[16].

Folgendes hat sich verändert:

- Das *Ziel* der Regelung wird explizit vorangestellt. Danach soll „für die eingesetzten IT-Systeme und IT-Anwendungen einschließlich der baulichen und gebäudebezogenen Komponenten ein Sicherheitsniveau“ erreicht werden, „das den sicheren Einsatz der Informationstechnik in der Berliner Verwaltung gewährleistet“.

- Analog zur Verschiebung der Prioritäten beim Verfahren der Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik

[14] JB 2006, 1.2

[15] Richtlinie zur Gewährleistung der notwendigen Sicherheit beim IT-Einsatz in der Berliner Verwaltung (IT-Sicherheitsrichtlinie) v. 5. Januar 1999, DBl. 1, 5

[16] Grundsätze zur Gewährleistung der notwendigen Sicherheit beim IT-Einsatz in der Berliner Verwaltung (IT-Sicherheitsgrundsätze) v. 11. Dezember 2007

(BSI) wird erstmals ein *IT-Sicherheitsmanagement* verlangt. Es ist ein Sicherheitsprozess einzuleiten, der ein Sicherheitsmanagement organisatorisch festlegt und die Verantwortlichkeiten klar bestimmt, der zu einer IT-Sicherheitsleitlinie führt, mit der die Behördenleitungen das für ihr Haus anzustrebende Sicherheitsniveau differenziert festlegen, in dem behördliche und verfahrensspezifische IT-Sicherheitskonzepte erarbeitet und umgesetzt werden und in dem insbesondere dafür gesorgt wird, dass die IT-Sicherheit fortlaufend auf Aktualisierungsbedarf überprüft wird.

- Es wird ausdrücklich darauf hingewiesen, dass die Entscheidung, ob Risiken als tragbar oder untragbar eingeschätzt werden, auf Grundlage einer *Schutzbedarfsanalyse* oder einer *Risikoanalyse* getroffen werden muss.

- Bei der Beschreibung der Verantwortlichkeiten werden erstmals die Aufgaben einer oder eines *IT-Sicherheitsbeauftragten* beschrieben.

- Es wird für alle Sicherheitsdomänen ausdrücklich mindestens der Grundschutz durch Anwendung der IT-Grundschutzkataloge des BSI[17] verlangt. Ergänzende Sicherheitsmaßnahmen bei höherem Schutzbedarf sind durch eine ergänzende Risikoanalyse zu ermitteln. Als Methode dafür wird beispielhaft auf die Risikoanalyse nach dem IT-Sicherheitshandbuch des BSI[18] oder auf den neuen BSI-Standard 100-3 verwiesen[19].

- Es wird erstmals auf das inzwischen entwickelte Modellsicherheitskonzept verwiesen, das die IT-Grundschutzkataloge vereinfacht und vereinheitlicht, indem es eine speziell auf die Rahmenbedingungen der Berliner Verwaltung abgestellte Adaption der IT-Grundschutzkataloge anbietet.

Wir begrüßen es ausdrücklich, dass in den neuen IT-Sicherheitsgrundsätzen noch deutlicher als in der IT-Sicherheitsrichtlinie von 1999, in der die damals aktuellen Handbücher des BSI pauschal als anzuwendende Methoden erwähnt wurden, die wesentlichen methodischen Vorgaben der IT-Grundschutzkataloge explizit genannt werden. Dies dürfte hoffentlich dazu führen, dass die teilweise abenteuer-

[17] http://www.bsi.de/gshb/index.htm

[18] Das aus dem Jahre 1992 stammende IT-Sicherheitshandbuch ist zwar sehr veraltet, kann aber dennoch nach wie vor für die Risikoanalyse verwendet werden. Es hat sich gezeigt, dass in manchen Fällen genauere Ergebnisse erzielt werden können als mit dem neuen BSI-Standard 100-3. Das IT-Sicherheitshandbuch kann heruntergeladen werden unter http://www.bsi.de/literat/kriterie.htm.

[19] http://www.bsi.de/literat/bsi_standard/standard_1003.pdf

lichen Kombinationen unterschiedlicher methodischer Ansätze uns nicht mehr vorgelegt werden.

Außerdem begrüßen wir es sehr, dass die Einrichtung eines IT-Sicherheitsmanagements ausdrücklich verlangt wird. Wir haben in der Zwischenzeit begonnen, im Rahmen der Kontrollen bei großen Daten verarbeitenden Behörden das IT-Sicherheitsmanagement in die Fragenkataloge einzubeziehen, da wir insbesondere bei ihnen so etwas erwarten. Die IT-Sicherheitsgrundsätze werden uns helfen, die in diesem Bereich häufig noch anzutreffende Ratlosigkeit zu beseitigen.

Die IT-Sicherheitsgrundsätze werden durch IT-Sicherheitsstandards ergänzt, die 2006 Teil der IT-Standards geworden sind. Die aktuellen IT-Sicherheitsstandards haben wir bereits im letzten Jahresbericht kommentiert[20]. Inzwischen liegt der Entwurf der IT-Standards 2008 vor, der jedoch beim Thema IT-Sicherheit keine wesentlichen Änderungen gegenüber 2007 enthält.

1.2.3 Aktuelle IT-Projekte des Landes

ZW-Expert für die Bearbeitung von KfZ-Angelegenheiten in den Ordnungsämtern

Das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) führt für die Zulassung von Kraftfahrzeugen mit dem neuen Verfahren *ZW-Expert* eine Weblösung ein, die es den Bürgerämtern der Bezirke ermöglicht, ihnen zugewiesene Aufgaben aus dem Aufgabenspektrum der Zulassungsbehörde Berlin (ZB) zu erledigen. Dabei handelt es sich um Namens- und Adressenänderungen, die vorübergehende Stilllegung von Fahrzeugen und die endgültige Abmeldung von Fahrzeugen.

Bisher wurden diese Aufgaben handschriftlich – durch Änderungen in den Fahrzeugpapieren sowie Ausfüllung von Formularen – erledigt. Diese Belege wurden dann von der ZB manuell erfasst. Nunmehr sollen mithilfe dieser Weblösung die Veränderungen im Fahrzeugbestand in den Bürgerämtern erfasst und sofort in das örtliche Fahrzeugregister übernommen werden.

[20] JB 2006, 1.2

Weiterhin soll ein Zugriff auf die Daten der Zulassungsbehörde plattformunabhängig für die Aufgabenerledigung der Polizei, der Ordnungsämter und der Bußgeldstelle realisiert werden.

In einem weiteren Schritt soll die Grundlage für die mobile Zulassung gelegt werden, was das Angebot für die Bürgerinnen und Bürger des Landes Berlin attraktiver macht.

Das Pflichtenheft, das von einem externen Unternehmen erarbeitet wurde, beschreibt die Geschäftsprozesse, das Systemkonzept, die Organisation der Benutzerverwaltung, die zu erhebenden Daten sowie die Sicherheitsanforderungen, insbesondere für den internen und externen Zugriff.

Die Risikoanalyse und das darauf aufbauende Sicherheitskonzept liegen noch nicht vor.

IT-Verfahren zum Gesamtplan nach § 58 SGB XII

Für die Eingliederungshilfe für Menschen mit bestehender und drohender Behinderung im Einzelfall wird nach § 58 Sozialgesetzbuch – Zwölftes Buch (SGB XII) als zentrales Koordinierungs- und Kontrollinstrument des Sozialhilfeträgers ein sog. Gesamtplan angelegt. In ihm werden alle wesentlichen Informationen zusammengefasst, die für eine ganzheitliche und individuelle Planung, Umsetzung und Anpassung des Verfahrens der Eingliederungshilfe notwendig sind. Unterschieden werden Gesamtpläne für Menschen mit geistiger Behinderung und Menschen mit seelischer Behinderung.

Vorgesehen ist, das für diese Gesamtpläne zu nutzende IT-Verfahren in das künftige Sozialhilfe-Verfahren OpenPROSOZ einzubinden, welches aber für den Einsatz noch nicht reif ist. Übergangsweise wurde eine Lösung auf der Grundlage des Tabellenkalkulationsprogramms EXCEL von Microsoft entwickelt, die Gegenstand unserer Unterrichtung wurde.

Nicht nur aus rechtlicher[21], sondern auch aus technisch-organisatorischer Sicht war jedoch festzustellen, dass das Verfahren mit sehr sensitiven Daten arbeitet, die insbesondere gegen die Grundbedrohung der Vertraulichkeit hohen Schutzbedarf aufweisen. Wenn gleichwohl wegen des Übergangscharakters dieses Verfahrens

[21] JB 2006, 5.1.2

auf das nach § 5 Abs. 3 Berliner Datenschutzgesetz (BlnDSG) gebotene Sicherheitskonzept auf der Grundlage einer Risikoanalyse verzichtet wird, dann darf dies nicht bedeuten, dass bei dem technisch immerhin überschaubaren Verfahren auf elementare, aber wirksame technische und organisatorische Maßnahmen des Datenschutzes verzichtet wird.

Dazu gaben wir die Empfehlungen,

- die Passwortverwaltung bei der Datenpflege, die nur optional verlangt wurde, verbindlich zu machen;

- wegen der hohen Sensitivität der Daten den lesenden Zugriff Dritter, d. h. auch durch Benutzerinnen und Benutzer mit privilegierten Zugriffsberechtigungen wie z. B. Systemverwalter, zu unterbinden, ggf. mit einer Verschlüsselung der Daten bei ihrer Speicherung oder durch den Betrieb des Verfahrens auf einem separaten lokalen Netz, das nur lokal im Einflussbereich der zuständigen Stelle im Sozialamt administriert wird;

- darauf zu achten, dass für die Rathausnetze in den Bezirken hinreichende Sicherheitskonzepte für die bezirkliche Infrastruktur (z. B. die Möglichkeit zur Speicherverschlüsselung) bestehen und umgesetzt werden, anderenfalls bestünde die Notwendigkeit, sich auf ein isoliertes lokales Netz zurückzuziehen.

Wegen der Nutzung von EXCEL als Grundlage des Verfahrens ist eine differenzierte Benutzerführung durch das System nicht möglich. Deshalb stützt sich das Verfahren auf eine Vielzahl von Handlungsanweisungen, wie sie in einem Manual beschrieben werden. Auch Plausiblitätskontrollen sind nur beschränkt möglich. Die ordnungsgemäße Verarbeitung der Daten ist also mehr als üblich von der persönlichen Sorgfalt der bearbeitenden Person bei der Beachtung der vielen Regeln abhängig. Dies führt zu Risiken hinsichtlich der Integrität und Verfügbarkeit der Daten und des Verfahrens. Da bezüglich dieser sog. Grundbedrohungen kein hoher Schutzbedarf gegeben ist, weil nach wie vor die Papierakte führend sein wird, sahen wir hier zunächst von weitergehenden Empfehlungen ab.

Die Senatsverwaltung hat unsere Empfehlungen im Wesentlichen umgesetzt, hat jedoch wegen des hohen Aufwandes und angesichts der vorgesehenen Betriebsdauer bis zum 30. Juni 2008 auf die Speicherverschlüsselung verzichtet. Wir haben diese Gründe angesichts der Befristung akzeptiert.

Erneuerung der IT-Verfahren der Berliner Steuerverwaltung - EOSS

Die Steuerverwaltungen des Bundes und der Länder bemühen sich seit längerem darum, bundeseinheitliche IT-Verfahren für die Steuerverwaltung zu entwickeln. Seit 1993 wurde versucht, mit dem Projekt FISCUS in überregionaler Zusammenarbeit dieses Ziel zu erreichen. Seinerzeit ging die Berliner Steuerverwaltung von einem Softwareentwicklungsprojekt bis dahin unbekannten Ausmaßes aus. Veranschlagt wurden eine Entwicklungszeit von 10 Jahren und ein Entwicklungsaufwand von 1000 Mannjahren. Im Jahre 2000 schied das Land Bayern aus dem bis dahin erfolglosen Projekt aus, mit dem die Steuerverwaltung hinsichtlich der Informationstechnik „revolutioniert“ werden sollte. Das Land Bayern ging einen Sonderweg und entwickelte eine „Evolutionär orientierte Steuersoftware“ (EOSS), die dann von den neuen Bundesländern und dem Saarland übernommen wurde. 2004 schlossen sich Bremen, Hamburg und Schleswig-Holstein ebenfalls dem Verbund an. 2005 trat auch Berlin bei, wobei die Inbetriebnahme der neuen Software für den 1. Januar 2008 vorgesehen wurde. Die Senatsverwaltung für Finanzen hatte vergessen, uns darüber zu unterrichten, und holte dies erst im August 2007 nach, sodass eine nähere datenschutzrechtliche Begleitung, die bei der Übernahme einer fertigen Software ohnehin nur beschränkt erfolgen könnte, nicht mehr möglich war.

EOSS ist ein – wohl grundlegender – Zwischenschritt auf dem Weg zu einer bundeseinheitlichen Lösung, die unter der Bezeichnung KONSENS (Koordinierte neue Softwareentwicklung der Steuerverwaltung) erfolgt. Grundsätzlich ist die Vereinheitlichung der steuerlichen Automationsverfahren zu begrüßen, da dies zur Transparenz der Verfahren beiträgt.

Allerdings konnten die gesetzlichen Rahmenbedingungen für die technisch-organisatorischen Maßnahmen nach § 5 BlnDSG für das neue IT-Verfahren der Berliner Steuerverwaltung nicht rechtzeitig erfüllt werden. Eine Vorabkontrolle konnte nicht rechtzeitig erfolgen, weil dazu Vorgaben der bayerischen Entwickler fehlten. Ein Sicherheitskonzept wird erstellt, lag uns jedoch zum Beginn des Einsatzes noch nicht vor. Wir haben im Vorfeld darauf hingewiesen, dass das Sicherheitskonzept für ein IT-Verfahren, mit dem alle Berliner Steuerdaten, die überdies durch ein hochrangiges Amtsgeheimnis, nämlich das Steuergeheimnis, geschützt werden, einem hohen Schutzbedarf unterliegt. Dies wurde zunächst nicht so gesehen, denn den Unterlagen war zu entnehmen, dass man bezüglich aller Sicherheitsziele nur von der niedrigstmöglichen Schutzkategorie ausgehen wolle.

Diese unzutreffende Einschätzung des Schutzbedarfs soll korrigiert werden. Zudem wurde die Einrichtung eines IT-Sicherheitsmanagements für die Senats-

verwaltung für Finanzen angekündigt. Dies sowie das Ergebnis der Vorabkontrolle und das Sicherheitskonzept bleiben abzuwarten.

Online-Bewerbungen und -Einstellungen für Berliner Lehrkräfte (BEO) und für Vertretungslehrkräfte (BEO V)

Der Hauptpersonalrat der Berliner Landesverwaltung bat uns um Unterstützung beim Mitbestimmungsverfahren für die Projekte „Bewerbungen und Einstellungen Online – BEO“ und „Bewerbungen und Einstellungen Online für Vertretungseinstellungen – BEO V“ der Senatsverwaltung für Bildung, Wissenschaft und Forschung, die eine Bewerbung über das Internet auf entsprechende Stellen bei den Schulen ermöglichen. Die Senatsverwaltung selbst hatte nicht für erforderlich gehalten, uns zu unterrichten, wie es das Gesetz vorschreibt. Sie erhielt unsere Stellungnahme gegenüber dem Hauptpersonalrat zur Kenntnisnahme.

Bewerberinnen und Bewerber für Festanstellungen in den Schuldienst haben ausdrücklich die Option, anstelle von Online-Bewerbungen auch den normalen Weg einer schriftlichen Bewerbung zu gehen. Bei Bewerbungen für Vertretungseinstellungen wird diese Option nicht eingeräumt. Wer keine Online-Bewerbung abgeben will oder kann, z. B. weil kein Internet-Zugang vorhanden ist – muss sich in schriftlicher Form direkt an die Schulen wenden.

Unsere in zwei Fällen geäußerten Zweifel an der Rechtmäßigkeit bestimmter anzugebender Daten wurden ausgeräumt.

Das zunächst fehlende verfahrensspezifische Sicherheitskonzept und die Risikoanalyse nach § 5 Abs. 3 Satz 1 BlnDSG wurden nachgereicht. Es basiert auf einem behördlichen Sicherheitskonzept, das von einer Fachfirma nach der Grundschutzmethodik erstellt und nach Angaben der Senatsverwaltung vom Rechnungshof von Berlin geprüft wurde, der feststellte, dass die Anforderungen des Grundschutzes im Wesentlichen erfüllt werden.

Zunächst sollten Bewerberinnen und Bewerber, die nicht über einen Browser verfügen, der SSL-verschlüsselte Verbindungen beherrscht, die Option erhalten, ungeschützt zu übertragen, allerdings mit eindringlich formulierten Warnungen. Auf unseren Einwand hin wurde diese Option aufgegeben, zumal es unwahrscheinlich sein dürfte, dass solche Browser noch verbreiteten Einsatz finden.

Wird das Passwort vergessen, so kann sich eine Bewerberin oder ein Bewerber ein neues Passwort per E-Mail zusenden lassen, indem auf der Anmeldeseite ein entsprechender Link angeklickt wird. Es ist der Nutzername oder die E-Mail-Adresse einzutragen, daraufhin wird geprüft, ob es die Person gibt. Wenn dies bestätigt wird, wird ein neues Passwort erzeugt, verschlüsselt in der Datenbank abgespeichert und – unverschlüsselt – per E-Mail zurückgeschickt. Das hierin bestehende Sicherheitsrisiko soll gemindert werden, indem darauf hingewiesen wird, das übersandte Passwort sofort zu ändern.

Nachdem die Senatsverwaltung alle geltend gemachten Einwände bereitwillig abgearbeitet hatte, erhielten wir Monate später erneut Post vom Hauptpersonalrat, die einige Verfahrenserweiterungen betraf, von denen eine datenschutzrechtlich kritisch erschien. Es war der Senatsverwaltung aufgefallen, dass viele Bewerberinnen und Bewerber vergaßen, ihre den Schulen zur Auswahlentscheidung bereitgestellten Bewerbungsdaten zu ändern, wenn sie z. B. nach Annahme einer Stelle zur weiteren Vermittlung nicht mehr zur Verfügung standen. Daher sollten die Schulen, die eine Bewerberin oder einen Bewerber übernommen hatten, die Daten selbst ändern dürfen. Wir haben den Hauptpersonalrat und die Senatsverwaltung darauf hingewiesen, dass diese Änderung der von den Betroffenen eingegebenen Personaldaten nur mit der expliziten Einwilligung der Betroffenen zulässig ist.

AUGUSTA – Ausnahmegenehmigungen für die Umweltzone

Seit dem 1. Januar 2008 darf die Berliner Umweltzone innerhalb des S-Bahnrings nur noch von Fahrzeugen befahren werden, die entweder über eine grüne, rote oder gelbe Plakette verfügen oder für die eine Ausnahmegenehmigung ausgestellt wurde. Um die erwartete hohe Zahl von Anträgen für eine solche Ausnahmegenehmigung bewältigen zu können, wurde das IT-Verfahren AUGUSTA entwickelt und in den Einsatz gebracht. Zuständig für die Ausnahmegenehmigungen sind die acht Bezirke, die Gebiete innerhalb der Umweltzone enthalten. Wer eine Ausnahmegenehmigung beantragen will, kann sich an ein beliebiges dieser Bezirksämter wenden. Um zu verhindern, dass eine Antrag stellende Person nach einem erfolglosen Antrag ihr Glück in einem anderen Bezirksamt versucht, sollte ein überbezirklicher Datenabgleich erfolgen, der ansonsten als Mittel gegen Sozialleistungsmissbrauch eingesetzt wird.

Ein solches Verfahren ist als automatisiertes Abrufverfahren zu bewerten, weil es die Übermittlung personenbezogener Daten „durch Abruf“ der zuständigen Dienstkraft ermöglicht. Der Umstand, dass es hier nur um die Informationen „Kfz-

Kennzeichen“ und „Bezirk“ ging, ändert daran nichts. Denn auch diese Informationen sind der Antrag stellenden Person zuzuordnen und stellen damit personenbezogene Daten dar.

Ein derartiges automatisiertes Abgleichverfahren erlaubt das Allgemeine Sicherheits- und Ordnungsgesetz für Ordnungsbehörden nicht: § 46 Abs. 1 Allgemeines Sicherheits- und Ordnungsgesetz (ASOG) lässt automatisierte Abrufverfahren nur für die Polizei, nicht aber für Ordnungsbehörden zu. Ein Rückgriff auf das allgemeine Berliner Datenschutzgesetz verbietet sich angesichts dieser bereichsspezifischen Regelung, würde aber auch nicht helfen, weil § 15 Abs. 1 BlnDSG vorsieht, dass ein automatisiertes Verfahren zum Abruf personenbezogener Daten durch Dritte nur eingerichtet werden darf, wenn ein Gesetz dies ausdrücklich zulässt. Nach Abs. 2 wären die Bedingungen des Abrufs überdies durch Rechtsverordnung zu regeln, die hier ebenfalls fehlt.

Aufgrund unserer Einwände wurde auf den automatisierten Datenabgleich verzichtet. Anders als im Sozialhilferecht ist das Problem des Missbrauchs von Genehmigungsanträgen begrenzt, wenn die Bezirke einheitliche Genehmigungsstandards einhalten.

Das verfahrensspezifische Sicherheitskonzept für AUGUSTA folgt einer methodischen Mixtur aus IT-Grundschutz und der eingeschränkten Anwendung des IT-Sicherheitshandbuchs von 1992. Dabei wird unterstellt, dass die bezirklichen IT-Infrastrukturen den Anforderungen des Grundschutzes gerecht werden.

In der Regel wird man allerdings nicht davon ausgehen können, dass behördenspezifische Sicherheitskonzepte umgesetzt wurden, die alle erforderlichen Grundschutzmaßnahmen berücksichtigen. Soweit dies nicht der Fall ist, muss ein verfahrensspezifisches Sicherheitskonzept für AUGUSTA die Versäumnisse kompensieren, um die erforderliche IT-Sicherheit zu gewährleisten. Dies bedeutet nicht, dass im Rahmen des Projekts AUGUSTA das vollständige behördenspezifische Sicherheitskonzept erarbeitet werden muss, jedoch ist alles, was zur Sicherheit des Verfahrens erforderlich ist, im verfahrensspezifischen Sicherheitskonzept zu berücksichtigen.

2 Schwerpunkte

2.1 Online-Durchsuchung

Bereits im vorangegangenen Jahr mussten wir über die besorgniserregende Entwicklung berichten, dass der Bundesgesetzgeber die Sicherheitsbehörden ohne werthaltige Evaluation und ohne hinreichende begleitende rechtsstaatliche Kontrollen mit immer mehr Befugnissen ausstattet[22]. Dieser Trend hat sich leider fortgesetzt. Dabei sind besonders zwei Gesetzesinitiativen zu erwähnen, weil sie auf nachhaltige datenschutz- und verfassungsrechtliche Bedenken stoßen. Neben der bereits in Kraft getretenen Pflicht zur Vorratsspeicherung von Telekommunikationsdaten[23] ist die sog. Online-Durchsuchung zu nennen.

Auch wenn die konkret geplanten technischen Details noch nicht bekannt sind, soll die Online-Durchsuchung den Sicherheitsbehörden ermöglichen, Spionageprogramme zur Erforschung der Kommunikation und von Daten auf internetfähigen Rechnern verdächtiger Personen einzusetzen. Die Grundprinzipien der technischen Vorgehensweise bei der Online-Durchsuchung sind jedoch Gegenstand diverser Anhörungen und Tagungen gewesen, sodass sich die Datenschutzbeauftragten inzwischen ein sachliches Bild von den geplanten Maßnahmen machen konnten[24].

Bevor die eigentliche Online-Durchsuchung erfolgen kann, muss eine technische Vorabklärung durchgeführt werden, bei der unter Einsatz von technischen Überwachungsmaßnahmen und offenen oder verdeckten Ermittlungsmethoden Erkenntnisse über das Zielsystem gewonnen werden müssen. Solche Erkenntnisse betreffen Details über die technische Umgebung (Betriebssystem, Art des Internetzugangs, Browser, vorhandene Software), aber auch das Verhalten der Zielperson beim Umgang mit dem Internet. Schließlich soll bereits abgeklärt werden, auf welche Weise die sog. Remote Forensic Software (RFS) in das Zielsystem eingebracht werden kann. Welche Optionen gesehen werden, darüber äußert sich das Bundesministerium des Innern nur vage. Sicher ist nur, dass es die einzige Methode zum Einbringen der RFS nicht gibt, vielmehr muss im Laufe der Vorbereitungen erst entschieden werden, welchen Weg man geht. Es wird jedoch offenbar

[22] JB 2006, Einleitung, 3.2, 8.1, 10.1.2

[23] vgl. 12.1

[24] Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat am 27. August 2007 an einer Expertenanhörung der Bundesministerien des Innern und der Justiz teilgenommen; vgl. außerdem https://www.datenschutzzentrum.de/sommerakademie/2007/sak2007-hansen-krause-online-durchsuchung.pdf, http://www.datenschutz.mvnet.de/dschutz/informat/internet/onlinedurchsuchung.pdf.

nicht daran gedacht, Hersteller zum Einbau von Hintertüren in Betriebs- und Anwendungssystemen zu veranlassen. Die E-Mail-Kommunikation wird im Einzelfall als probates Mittel angenommen. Diskutiert wurde die Infizierung von Zielsystemen durch Anlagen von amtlichen oder amtlich erscheinenden E-Mails. Zu bedenken ist jedoch, dass die Bürgerinnen und Bürger den Bemühungen der Behörden zur Hinwendung zu einem verstärkten E-Government dann mit großem Misstrauen begegnen würden, was den Erfolg dieser Anstrengungen in Frage stellt.

In der Literatur wird über das Ausnutzen von Sicherheitslücken durch sog. Exploits, Zero-Day-Exploits und Less-Than-Zero-Day-Exploits diskutiert[25].

Exploit:	Programm oder Skript zur Ausnutzung bekannter Sicherheitslücken von Programmen.
Zero-Day-Exploit:	Programm oder Skript zur Ausnutzung von Sicherheitslücken von Programmen zwischen dem allgemeinen Bekanntwerden und dem Schließen von Sicherheitslücken.
Less-Than-Zero-Day-Exploit:	Programm oder Skript zur Ausnutzung von Sicherheitslücken vor dem allgemeinen Bekanntwerden der Sicherheitslücken.

Zero-Day-Exploits bieten hohe Erfolgschancen für Angriffe, da Abwehrmaßnahmen in der Regel noch nicht zur Verfügung stehen. Bei Less-Than-Zero-Day-Exploits ist es praktisch ausgeschlossen, dass man sich gegen einen Angriff schützen kann.

Um Zero-Day-Exploits und vor allem Less-Than-Zero-Day-Exploits ist ein weltweiter – bisher in aller Regel illegaler – Markt entstanden, auf dem hohe Preise bezahlt werden. Es ist nicht ausgeschlossen, dass die deutschen Sicherheitsbehörden sich an diesem Markt beteiligen, um Zielrechner infiltrieren zu können.

Darüber hinaus werden der Infektion von Downloads während des Download-Vorgangs („on the fly“) hohe Erfolgschancen eingeräumt.

Bei der Online-Durchsuchung werden neben der Überwachung von Internet-Telefonie („Quellen-TKÜ“) zwei Zielstellungen unterschieden: Die Online-Durch-

[25] Pohl, Hartmut: Zur Technik der heimlichen Online-Durchsuchung, Datenschutz und Datensicherung (DuD) 31 (2007) 9, 684 ff.

sicht, die die Analyse der auf einem Zielsystem gespeicherten Dateien nach verschiedenen Kriterien betrifft und Auskunft zum in der Vergangenheit liegenden Handeln der Zielperson geben soll, und die Online-Überwachung, die darüber hinaus beobachten soll, was aktuell am System geschieht, und die insbesondere Klartexte vor einer Verschlüsselung und nach einer Entschlüsselung sowie Authentisierungsdaten wie Passwörter und Schlüssel zum Ziel hat. Beide Zielstellungen unterscheiden sich in der technischen Vorgehensweise kaum, jedoch ist die Online-Durchsicht eher von kurzer Dauer, während die Online-Überwachung auf längere Dauer angelegt ist. Wenn die Maßnahmen zum Ziel geführt haben oder aus rechtlichen Gründen beendet werden müssen, muss sich das RFS auf dem Zielsystem auf ein Kommando hin selbst deinstallieren, ohne dass Spuren hinterlassen werden oder das Zielsystem beeinträchtigt wird. Es müssen auch Maßnahmen ergriffen werden, um dafür zu sorgen, dass RFS-Kopien, die z. B. bei der Datensicherung anfallen, bei einer Aufspielung der Datensicherung nicht erneut aktiv werden.

Weitere offene Fragen der Online-Durchsuchung betreffen die Sicherheitsrisiken für die Zielrechner, die Sicherung der Beweiskraft der Durchsuchung, die Wirkung von Gegenmaßnahmen gegen die Durchsuchung, die Reichweite der Eingriffe und den Schutz des Kernbereichs der privaten Lebensgestaltung. Insbesondere ist die Online-Durchsuchung datenschutzrechtlich hochproblematisch, weil sie eine heimliche längerfristige Ausforschung der betroffenen Person ermöglicht.

Insoweit ist der Begriff „Online-Durchsuchung“ missverständlich und beschönigend. Bei einer Durchsuchung nimmt eine Ermittlungsbehörde in aller Regel eine offene, für die Betroffenen erkennbare Ermittlungshandlung vor. Die Strafprozessordnung (StPO) schreibt für die Durchsuchung von Räumen sogar ausdrücklich vor, dass die von ihr betroffene Person „der Durchsuchung beiwohnen“, sie also mit eigenen Augen verfolgen können soll[26]. Aus diesem Grund hat der Bundesgerichtshof die Online-Durchsuchung nach geltendem Recht für unzulässig erklärt[27]. Zugleich beschränkt sich die Durchsuchung auf den zeitlichen Rahmen, in dem die Ermittlungshandlung vorgenommen wird.

Demgegenüber kann eine Online-Durchsuchung nur dann eine sinnvolle Ergänzung der vorhandenen Ermittlungsmethoden darstellen, wenn sie ohne Wissen der Betroffenen – also *heimlich* – vorgenommen wird. Ansonsten wäre sie überflüssig, weil man die mit ihr verbundenen Ziele zum Beispiel auch mit einer Durchsuchung und Beschlagnahme des Rechners erreichen könnte. Aus den Ver-

[26] § 106 StPO

[27] Beschluss v. 31. Januar 2007, NJW 2007, 930

lautbarungen des Bundesinnenministeriums ergibt sich weiterhin, dass die Online-Durchsuchung eine *langfristige* Überwachung bzw. *langfristige* Infiltrationsversuche voraussetzt, zumindest so langfristig, bis die Zielperson einen Fehler macht, der die Infiltration des Zielrechners ermöglicht. Dabei betrifft die gesamte Maßnahme auch Personen, die weder einer Straftat verdächtig sind noch von denen eine konkrete polizeiliche Gefahr ausgeht – von Mitnutzerinnen und -nutzern des Zielrechners ganz zu schweigen. In ihrer Eingriffsintensität entspricht die Online-Durchsuchung also einer heimlichen, rund um die Uhr stattfindenden Durchsuchung.

Der Einsatz von Spionagesoftware ist damit stets ein massiver Eingriff in die Privatsphäre der jeweils betroffenen Internetnutzerinnen und -nutzer. Das Bundesverfassungsgericht hat deshalb in einer jüngst getroffenen Grundsatzentscheidung[28] festgestellt, dass das allgemeine Persönlichkeitsrecht auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst. Gleichzeitig hat es darauf hingewiesen, dass bereits der einmalige und punktuelle Zugriff auf Speichermedien ein „beträchtliches Potential für die Ausforschung der Persönlichkeit des Betroffenen“ aufweist[29]. Das Gewicht der Grundrechtsbeeinträchtigung wiegt noch schwerer, wenn „die heimliche technische Infiltration die längerfristige Überwachung der Nutzung des Systems und die laufende Erfassung der entsprechenden Daten ermöglicht.“[30] Technisch können die Ermittlungsbehörden mit ihr den Gesamtdatenbestand des betroffenen internetfähigen Rechners erfassen und die Kommunikation, die von ihm ausgeht, laufend überwachen. Da heute Computer auch die Funktionen von Tagebüchern und Briefen erfüllen, ermöglicht die Online-Durchsuchung nahezu zwingend den staatlichen Zugriff auf intime Informationen der Betroffenen. Sind solche intimen Informationen dem „Kernbereich privater Lebensgestaltung“ zuzurechnen, hat der Gesetzgeber nach der Feststellung des Bundesverfassungsgerichts im Rahmen eines zweistufigen Schutzkonzepts diesen Kernbereichsschutz zu gewährleisten[31]. Die einzige bislang in Kraft getretene Befugnisnorm, die der Verfassungsschutzbehörde des Landes Nordrhein-Westfalen eine Online-Durchsuchung gestattet, ist diesen Anforderungen nicht gerecht geworden und wurde unter anderem deshalb vom Bundesverfassungsgericht für nichtig erklärt.

Die Auswirkungen der Entscheidung sind im Einzelnen noch nicht absehbar. Durch das Urteil klargestellt ist jedoch, dass auch Verfassungsschutzgesetze den

[28] Urteil v. 27. Februar 2008 – 1 BvR 370/07 und 1 BvR 595/07

[29] a.a.O., Rn. 230

[30] a.a.O., Rn. 234

[31] A.a.O. Rn. 280 ff.

Schutz des Kernbereichs privater Lebensgestaltung zu gewährleisten haben. Umso bedauerlicher ist es, dass der Senat bislang unsere Empfehlung nicht aufgegriffen hat, den Kernbereichsschutz auf den Verfassungsschutz zu erstrecken[32].

Unabhängig von der Entscheidung des Bundesverfassungsgerichts wäre die Einführung der Online-Durchsuchung aus datenschutzrechtlicher Sicht auch deshalb besonders problematisch, weil sie das Vertrauen unserer Gesellschaft in die Sicherheit unserer IT-Strukturen nachhaltig erschüttern würde. Sie würde überdies immense wirtschaftliche Schäden anrichten, sofern sie zu Zwecken der Wirtschaftsspionage gegen Unternehmen eingesetzt wird. In Anhörungen und in einer Presseerklärung haben wir darauf hingewiesen, dass auch das Bundesministerium des Innern (zu Recht) Schutzmaßnahmen gegen den Einsatz von Spionageprogrammen durch Wirtschaftskriminelle fördert. Es wäre widersinnig, wenn deutsche Sicherheitsbehörden die Befugnis erhalten würden, genau dieselben Schadprogramme einzusetzen, vor denen das Bundesministerium des Innern warnt.

Bei der Entscheidung über die Einführung neuartiger Ermittlungsinstrumente sollte der Gesetzgeber sein Augenmerk nicht allein darauf legen, ob die geschaffenen Befugnisnormen noch verfassungsrechtlichen Anforderungen genügen. Selbst wenn die Online-Durchsuchung unter bestimmten Voraussetzungen verfassungskonform ausgestaltet werden kann, sollte sie gleichwohl nicht legalisiert werden: Der Schaden für die Vertrauenswürdigkeit der Informationstechnik wäre ungleich größer als der erhoffte Sicherheitsgewinn.

2.2 Surfen im Internet – aus gutem Grund anonym und unbeobachtbar

Seit 2001 enthalten das Bundesdatenschutzgesetz und das Berliner Datenschutzgesetz für Anbieter informationstechnischer Verfahren die Verpflichtung, eine anonyme oder pseudonyme Nutzung ihrer Dienste zu ermöglichen. Diese Verpflichtung zur „Datensparsamkeit“ umfasst mehrere Aspekte. Einerseits ist bei der gezielten Erhebung von Daten zu beachten, in welchem Umfang und zu welchem Zweck sie erhoben, und andererseits, über welchen Zeitraum sie gespeichert werden müssen. Es ist zu untersuchen, ob der Zweck des informationstechnischen Verfahrens auch erfüllt werden kann, wenn diese Daten nicht oder nur pseudony-

[32] vgl. JB 2006, 3.1.1, JB 2005, 1.2

misiert gespeichert werden. Im Jahresbericht 2005 wurden diese Fragen in einem Schwerpunkt behandelt[33].

Das Gebot der Datensparsamkeit geht zurück auf das Informations- und Kommunikationsdienstegesetz von 1997, in dem der Bundesgesetzgeber erstmals das Recht festgeschrieben hat, Multimedia-Dienste und insbesondere das Internet grundsätzlich spurlos, also anonym und unbeobachtbar nutzen zu können. Dahinter steht die Überlegung, dass niemand, der das Internet als Informationsquelle nutzt, dabei auf Schritt und Tritt (bei jedem Mausklick) überwacht werden soll. In einer freiheitlichen Informationsgesellschaft ist dies ein Gebot der Informations- und Meinungsfreiheit. Diese seit 1997 geltenden Grundsätze des Multimedia-Rechts sind heute – im Wesentlichen unverändert – im Telemediengesetz[34] festgelegt.

Das Telemediengesetz konkretisiert die Verpflichtung zur Datensparsamkeit für Daten, die beim Surfen quasi nebenbei anfallen und entweder vom Anbieter selbst oder von Dritten beobachtet und gespeichert werden könnten. Bei internetgestützten Verfahren sind diese nebenbei anfallenden Daten insbesondere

1. die Absenderadressen (Internet Protokoll (IP)-Adresse) der das Verfahren nutzenden Personen,

2. die Kommunikationsinhalte, wie beispielsweise die abgerufenen Webseiten und die in die Formulare eingegebenen Daten, und

3. die Kommunikationszeitpunkte.

Die Kommunikationsinhalte können relativ leicht durch Verwendung von Verschlüsselungsmechanismen geschützt werden. In aktuellen Webbrowsern ist leicht zu erkennen, ob die aktuelle Verbindung (mittels SSL bzw. HTTPS) verschlüsselt, d. h. vor dem Mitlesen durch Dritte geschützt ist: Die Adresszeile einer verschlüsselt übertragenen Webseite ist meist farblich hervorgehoben und zusätzlich wird ein geschlossenes Vorhängeschloss oder ein Schlüssel angezeigt. Zudem kann man sich das digitale Zertifikat des Kommunikationspartners (der Webseite) anzeigen lassen, in welchem die Identität der Eigentümerin oder des Eigentümers der Webseite, mit der gerade verschlüsselt und nichtmanipulierbar kommuniziert wird, von einer „Zertifizierungsstelle“ bestätigt wird. Die Aufgabe einer Zertifizierungsstelle wie beispielsweise TC Trustcenter oder VeriSign ist die Überprüfung der Identität von Personen oder Firmen und die Ausstellung von digitalen Zertifikaten, die ne-

[33] JB 2005, 3.4
[34] vgl. 12.2

ben einem kryptografischen Signierschlüssel die Zusicherung beinhalten, dass eine bestimmte Internetadresse (URL – Uniform Resource Locator) zu einer Person oder Firma gehört.

Der Einsatz von Verschlüsselung schützt aber nicht vollständig vor Überwachung durch Dritte. So können Beobachtende mit ausreichenden Fähigkeiten durchaus erfahren, zu welchem Zeitpunkt eine Kommunikation zwischen welchen Internetadressen (IP-Adressen) stattgefunden hat. Selbst wenn die Kommunikationsinhalte wegen einer verwendeten Verschlüsselung nicht ermittelt werden können, ist die Tatsache, dass ein bestimmtes Internetangebot genutzt wurde, oft schon eine sehr private Information. Beispielsweise wäre die Kenntnis von einem Besuch des Webangebots der Anonymen Alkoholiker oder der AIDS-Beratungsstelle sicher aufschlussreich, auch wenn nicht ermittelt werden kann, welche Webseiten des Webangebots konkret aufgerufen wurden. Normalerweise kann diese Information an jeder Zwischenstation, z. B. bei dem Dienstleister, der den Internetzugang anbietet (dem ISP – Internet Service Provider), oder von der Systemadministration in der Firma ermittelt werden, da alle Nachrichten im Internet als „Datenpakete“ verschickt werden, die auch die Absender- und die Zieladresse enthalten, und die genannten Parteien die reale Identität der Nutzenden, zumindest der Anschlussinhaberin oder des -inhabers, hinter einer IP-Adresse kennen.

Ein weiteres Problem sind Anbieter von Webangeboten, die man zwar benutzt, aber denen man keine personenbezogenen Daten anvertrauen möchte. Ohne Selbstschutzmaßnahmen erfahren die Anbieter die IP-Adressen, Kommunikationsinhalte und -zeitpunkte der Nutzenden.

Im Folgenden wird gezeigt, wie man sich vor der Überwachung der eigenen Kommunikation schützen kann. Zuerst werden Möglichkeiten aufgezeigt, wie man seine eigene Internetadresse vor dem zu nutzenden Webangebot und gegenüber Dritten schützen kann. Danach wird erläutert, wie man sich gegen die Technik der sog. Cookies schützen kann, die es Anbietern erleichtert, Nutzende wiederzuerkennen. Alle diese Techniken des informationellen Selbstschutzes gewinnen angesichts der voraussichtlich ab Anfang 2009 geltenden Pflicht zur verdachtsunabhängigen Speicherung aller Internet-Verkehrsdaten stark an praktischer Bedeutung.

2.2.1 Anonymisierung der Netzverbindung

Will man die Kommunikationsbeziehung, d. h. den Zusammenhang zwischen Quelle und Ziel von Nachrichten, vor Beobachtung sichern, bietet sich die Nutzung von „Anonymisierungsdiensten“ an. Solche Dienste schützen Kommunikations-

verbindungen, indem der Datenstrom über Zwischenstationen umgeleitet und zumindest über ein Teil des Wegs verschlüsselt übertragen wird.

Anonymisierende Proxies

Die einfachste, schnellste, aber auch stark eingeschränkte Möglichkeit, sich vor Beobachtung seiner Kommunikationsbeziehungen zu schützen, ist die Nutzung anonymisierender Proxy-Server, kurz „*Anon-Proxies*“. Für das World Wide Web haben solche Systeme, z. B. Anonymouse.org oder Behidden.com, bereits einen recht hohen Bekanntheitsgrad erlangt. Ihr größter Vorteil besteht darin, dass auf dem eigenen PC keine zusätzlichen Programme installiert werden müssen: Es wird im Webbrowser die Adresse des Anon-Proxy aufgerufen und in das angezeigte Formularfeld die gewünschte Zieladresse eingetragen. Der Anon-Proxy ruft beim Zielserver die Daten in seinem eigenen Namen ab, als wäre er der Benutzer, und verschleiert so die Adresse der tatsächlich nutzenden Person.

Anon-Proxies haben zwei strukturelle Nachteile: Erstens schützen sie keine Anfrage vor dem Betreiber des Anon-Proxies, d. h., dieser weiß genau, wer bzw. welche IP-Adresse sich hinter der Anfrage verbirgt. Zweitens schützen Anon-Proxies nicht gegen „professionelle“ Überwacher. Wer große Teile des Netzes beobachtet, weiß (zumindest theoretisch) genau, zu welchem Zeitpunkt eine Anfrage in den Anon-Proxy eingegangen ist. Da dieser die eingehenden Anfragen sofort bearbeitet, d. h. den Zugriff auf die gewünschte Adresse ausführt, können Beobachtende beides leicht miteinander verketten, selbst wenn die Nachrichteninhalte verschlüsselt sind.

Auf dem gleichen Konzept basieren sog. *VPN-Anonymisierer*. Auf dem Nutzerrechner wird dazu ein VPN-Programm[35] installiert, welches eine verschlüsselte Verbindung zum Proxy-Server aufbaut. Da auch hier nur ein einzelner Proxy-Server verwendet wird, treten die schon für Anon-Proxies beschriebenen Probleme analog auf. Einziger Vorteil ist, dass grundsätzlich eine Verschlüsselung der Verbindung zwischen der nutzenden Person und Proxy erfolgt, sodass der Internet-Zugangsprovider keine Surf-Informationen erhält. Bei den oben vorgestellten Anon-Proxies wird diese unbedingt notwendige Verschlüsselung meist gar nicht oder nur optional angeboten.

[35] Virtual Private Network

Mixe

Eine Weiterentwicklung der Anon-Proxies stellen die sog. „*Mixe*“ dar, die David Chaum bereits 1981 publizierte[36]. Die Technik löst die Probleme der Anon-Proxies, indem jede Zwischenstation (Mix) immer erst eine Menge von Nachrichten sammelt, ehe diese in veränderter Reihenfolge weitergeleitet und immer über eine Folge von mehreren Mixen „umgeleitet“ werden, bevor sie ihr Ziel erreichen.

Wie funktioniert ein Mix?

Ein Mix sammelt zunächst die eingehenden Nachrichten und verhindert so, dass bei einer „professionellen“ Überwachung die in einem Mix eingehenden Nachrichten den ausgehenden Nachrichten zugeordnet werden können. Diese Zuordnung könnte aber auch anhand des Aussehens der Nachrichten erfolgen. Dies wird verhindert, indem die Nachrichten im Mix umkodiert werden. Nachdem die Nachrichten vor dem Senden mit einem vom Mix veröffentlichten Schlüssel asymmetrisch verschlüsselt wurden, entschlüsselt der Mix jede erhaltene Nachricht wieder und leitet sie unverschlüsselt, aber im Aussehen verändert, gemeinsam mit den anderen Nachrichten weiter.

Das Problem des Vertrauens in den einzelnen Mix löst Chaum, indem er mehrere Mixe zusammen einsetzt: Alle Nachrichten werden über eine Folge von Mixen transportiert, wobei die Nachrichten in jedem Mix umkodiert und gemischt werden. Dazu müssen die Nachrichten vor dem Ansenden *mehrfach* verschlüsselt werden, vergleichbar mit einer Postkarte, die in einen Briefumschlag gesteckt wird und dieser wiederum in einen weiteren Briefumschlag und so weiter. Jeder Mix entschlüsselt hingegen nur eine Schicht – entfernt einen Briefumschlag – und findet einen an den nächsten Mix adressierten Brief vor. Die Nachricht liegt erst dann im Klartext vor, wenn sie in der richtigen Reihenfolge von jedem Mix entschlüsselt wurde. Für diese spezielle Verschlüsselung von einer Folge von Mixen ist immer ein besonderes Programm auf dem Computer der nutzenden Person notwendig.

Leistungsfähige Anonymisierungsdienste wie z. B. JAP[37] oder TOR[38] basieren auf der Technik der Mixe. Der Datenstrom durchläuft zwischen nutzender Person und Ziel-Webseite nacheinander mehrere Zwischenstationen. Bei dem Dienst JAP stehen mehrere fest vorgegebene Folgen von Mixen zur Auswahl. Bei dem Dienst

[36] Chaum, David: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24/2 (1981) 84-88. http://world.std.com/~franl/crypto/chaum-acm-1981.html

[37] http://www.anon-online.de

[38] http://tor.eff.org/

TOR wird die Reihenfolge der Zwischenstationen nicht vorgegeben, sondern die Software auf dem Nutzerrechner wählt zufällig einige der aktiven TOR-Server für die zu übertragende Nachricht aus.

Im Idealfall werden die Mixe bzw. TOR-Server von unabhängigen Anbietern betrieben. Bei JAP wird dies schon bei der Zusammenstellung der Kaskade berücksichtigt. Zudem kann man sich genau informieren, wer jeden der Mixe betreibt. Bei TOR erfolgt die Wahl der Zwischenstationen zufällig. Durch die eingesetzte Technik der Mixe könnte eine nutzende Person nur dann beobachtet werden, wenn alle Zwischenstationen gemeinsam gegen sie agieren würden.

Vor kurzem war in der Presse über den Anonymisierungsdienst TOR zu lesen, dass es gelungen ist, Hunderte von Login-Kennungen und Passwörtern von TOR-Nutzenden zu ermitteln[39], indem der Beobachtende eigene TOR-Server betrieben hat. Dabei handelt es sich um ein typisches Problem: Anonymisierungsdienste wie TOR und JAP schützen zwar zuverlässig die Anonymität der IP-Adressen der Nutzenden, sind jedoch von sich aus nicht in der Lage, den Inhalt von Nachrichten zu schützen. Dazu ist zusätzlich eine Ende-zu-Ende-Verschlüsselung (vom Webbrowser der nutzenden Person bis zum Webserver des Anbieters) erforderlich. Mit aktuellen Webbrowsern ist dies möglich, wenn das besuchte Webangebot ebenfalls Verschlüsselung akzeptiert. Geschieht dies wie in den dokumentierten Fällen nicht, so können die übertragenen Daten auf dem Weg zwischen dem letzten TOR-Server bzw. dem letzten Mix abgehört werden.

Zwar entsteht das Problem, dass das Abhören von Passwörtern möglich ist, nicht erst durch Nutzung eines Anonymisierungsdienstes, sondern dies ist beispielsweise dem Internet-Zugangsprovider ebenso möglich, wenn keine Ende-zu-Ende-Verschlüsselung eingesetzt wird. Jedoch ist im Konzept von TOR der Umstand besonders problematisch, dass jedermann einen eigenen TOR-Server betreiben kann. Das Abhören von Kommunikationsinhalten ist damit für *alle* möglich: Notwendig ist nur eine Verbindung zum Internet und die Installation der TOR-Software, da das Tor-Netz Datenübertragungen quasi zum Beobachtenden „umleitet“.

Der Anonymisierungsdienst JAP ermöglicht hingegen niemandem, anonym einen Mix zu betreiben, und erwartet die Einhaltung einer Selbstverpflichtungserklärung, sodass ein vergleichbarer Angriff zwar nicht ausgeschlossen werden kann, aber unwahrscheinlicher ist.

[39] http://www.heise.de/newsticker/meldung/95770

2.2.2 Strafverfolgung trotz Anonymisierung

Oft wird argumentiert, dass durch Anonymisierungsdienste eine effektive Strafverfolgung verhindert würde. Dies muss aber nicht der Fall sein. Beispielsweise hat der Anonymisierungsdienst JAP eine datenschutzfreundliche Möglichkeit zur Strafverfolgung in seinen Dienst integriert[40]. Dabei hat man die in den Telefonnetzen vorgesehene Möglichkeit der Mitteilung bei einem bestimmten Anschluss ankommender Verbindungen (Fangschaltung) zum Vorbild genommen: Die Bedarfsträger können mit der notwendigen richterlichen Anordnung nach §§ 100 a, b Strafgesetzbuch jeden Betreiber einer anonymisierenden Zwischenstation (jeden Mixbetreiber) zur Überwachung bestimmter Internetadressen für die Zukunft verpflichten. Im Ergebnis werden nur die Aktionen der Nutzenden protokolliert, die derart überwachte Adressen aufrufen. Alle anderen Nutzenden bleiben geschützt – so wie eine Telefonüberwachung nur jeweils einen Telefonanschluss betrifft.

Technisch wird eine Überwachungsmaßnahme folgendermaßen umgesetzt: Ruft eine Nutzerin oder ein Nutzer die Internetadresse auf, so erkennt ausschließlich der letzte Mix die Zieladresse, da er die Anfrage direkt an sie weiterleitet. Im Falle des Aufrufes einer überwachten Adresse informiert der letzte Mix den vorletzten Mix und dieser wieder seinen Vorgänger usw. Der erste Mix schreibt nun die IP-Adressen der Nutzenden, die auf die überwachte Adresse zugegriffen haben, in eine Protokolldatei.

Eine Protokollierung aller Verkehrsdaten, wie im Gesetz zur Vorratsdatenspeicherung ab dem 1. Januar 2009 vorgesehen, wird von den Betreibern aus rechtlichen und technischen Gründen abgelehnt. Rechtlich betrachten sich die Betreiber von Anonymisierungsdiensten zutreffend als Anbieter von Telemedien, für die die Bevorratungspflicht nicht gilt. Technisch ist der notwendige Speicheraufwand viel höher als beispielsweise für einen Internet-Zugangsprovider. Während dieser nur die in einem Zeitraum an einen Nutzenden vergebene IP-Adresse speichern muss, müsste jeder Mix jede einzelne Verbindung protokollieren. Zudem würde eine solche Protokollierung den Zweck eines Anonymisierungsdienstes natürlich ad absurdum führen. Wird die Vorratsdatenspeicherung nicht gestoppt, so werden wohl JAP und andere Anonymisierungsdienste aus dem Ausland betrieben werden und damit die momentan angebotenen, moderaten Strafverfolgungsmöglichkeiten verloren gehen. Das zeigt, dass die Vorratsdatenspeicherung in diesem Zusammenhang die Strafverfolgung sogar erschwert, statt sie zu erleichtern.

[40] http://anon.inf.tu-dresden.de/strafverfolgung/index_de.html

2.2.3 Wiedererkennung durch Inhaltsdaten

Problematisch für ein unüberwachtes Surfen im Internet sind nicht nur die Verfolgungsmöglichkeiten der Nutzung auf Basis der IP-Adresse, sondern auch auf Basis der übertragenen Daten. Webbrowser übertragen neben dem Aufruf der gewünschten Webseite zusätzlich eine Reihe weiterer Daten. Für den Datenschutz besonders riskant sind dabei die weithin bekannten „Cookies".

Was ist ein Cookie?

Ein Cookie ist ein kleines, auf dem Rechner der Nutzenden abgelegtes Datenpaket, das in vielen Fällen eine eindeutige Referenz auf ein pseudonymes Nutzerprofil in der Datenbank des Webseitenanbieters enthält. Diese Referenz wird bei wiederholtem Besuch der Webseite mitunter jahrelang automatisch von Browser mitgesendet und identifiziert auf diese Weise die Besuchenden. Cookies werden einerseits i. S. d. Nutzenden eingesetzt, um aufeinanderfolgende Zugriffe der Nutzerin oder des Nutzers zu einer Einheit (einer Sitzung) zusammenzusetzen und so Dienste, wie z. B. einen Warenkorb, zu ermöglichen. Gleichzeitig kann durch Cookies eine nutzende Person detailliert verfolgt werden: *Welche Bücher habe ich mir in einem Web-Shop angeschaut, welche habe ich in den Warenkorb gelegt und welche Produkte habe ich erst bei einem späteren Besuch erworben.* Spätestens wenn der Webseite erstmalig Name und Adresse mitgeteilt wurde, beispielsweise um eine Postsendung zuzustellen, handelt es sich nicht mehr um ein pseudonymes, sondern um ein personenbezogenes Nutzungsprofil.

Insbesondere sog. Werberinge setzen Cookies ein, um umfassende Interessensprofile der Nutzerinnen und Nutzer zu erstellen. Dies ermöglicht ein einfacher Trick: Normalerweise wird ein Cookie nur an denjenigen Web-Server zurückgesandt, der den Cookie vorher im Browser abgespeichert hat. Werberinge umgehen diese „Schutzmaßnahme", indem sie Werbebanner auf verschiedenen Webangeboten einbinden, die von einem zentralen Server geladen werden. Dabei wird der Cookie dieses zentralen Servers jeweils mitgesandt. Anhand des angeforderten Werbebanners und des Cookies wird ermittelt, wer welche Webseiten besucht hat, und diese Informationen für angepasste Werbung verwendet. Der Cookie-Mechanismus ist somit eine der wesentlichsten und allgegenwärtigsten Überwachungstechniken im Internet.

Bekannt geworden sind auch sog. Web-Bugs. Dabei handelt es sich eigentlich um den gleichen Mechanismus wie bei den Werbebannern, nur dass die in andere Webseiten integrierten Objekte unsichtbar sind – Bilder, die nur ein Pixel groß

sind. Dadurch kann die Nutzerin oder der Nutzer nicht mehr erkennen, dass gerade Informationen an einen anderen Server gesendet wurden.

Auch Suchmaschinen verwenden Cookies, die teilweise jahrelang gültig sind. Unter dem Nutzungsprofil, auf welches der jeweilige Cookie verweist, werden beispielsweise alle bisherigen Suchanfragen (die eingegebenen Stichwörter) und die angeklickten Suchergebnisse gespeichert.

Die meisten Browser bieten heute die Möglichkeit, die Nutzung von Cookies zu konfigurieren. Einerseits ist oft eine unterschiedliche Behandlung von „gewöhnlichen“ Cookies, die von der besuchten Webseite im Webbrowser gespeichert werden, und Cookies von Dritten, wie beispielsweise dem Werbering, möglich. Des Weiteren kann man häufig festlegen, dass die Cookies nach kurzer Zeit (beispielsweise beim Schließen des Browsers) gelöscht werden sollen, selbst wenn der Webseitenanbieter eine längere Speicherdauer vorgeschrieben hat. Natürlich ist es auch möglich, den Webbrowser so zu konfigurieren, dass er überhaupt keine Cookies annimmt – leider führt dies dazu, dass viele Webseiten nicht nutzbar sind. Ideal ist daher, die Speicherdauer von Cookies allgemein auf die aktuelle Sitzung zu beschränken und nur einzelnen Webangeboten langfristige Cookies zu erlauben, wenn dies für die Nutzenden einen echten Vorteil bringt.

Mechanismen mit ähnlicher Wirkung wie die Cookies sind auch in einer Reihe von Erweiterungen der Webbrowser integriert. So bietet beispielsweise der Flash-Player Webseiten lokalen Speicherplatz an und der Windows Media Player enthält eine vom Webserver auslesbare weltweit eindeutige Identifikationsnummer.

Schon aus Gründen der Sicherheit sollten daher beim Surfen so wenig Erweiterungen und aktive Inhalte (JAVA, JAVA-Script, Active-X usw.) wie möglich aktiviert sein. Schließlich lässt sich ein Großteil der Sicherheitsprobleme im Internet auf aktive Inhalte, d. h. Programme, die ungefragt ausgeführt werden, zurückführen. Einige Browser bieten einfach zu bedienende Konfigurationsmöglichkeiten, mit denen man einerseits pauschal Erweiterungen ein- oder ausschaltet und zugleich für einzelne Seiten Ausnahmen festlegen kann. Wählt man als Standardvorgabe, dass keine aktiven Inhalte dargestellt werden, so kann man die Einstellungen für häufig besuchte, vertrauenswürdige Webseiten leicht so umkonfigurieren, dass diese im vollen Umfang nutzbar sind. Zugleich ist man beim normalen Surfen vor Ausforschung und auch vor Viren und Trojanern geschützt.

Zudem sollte man sich vor der Eingabe von persönlichen Daten im Internet gut überlegen, ob die jeweilige Webseite die geforderten Daten auch wirklich benötigt. Notfalls, wenn die Eingabe obligatorisch verlangt wird, kann man sich auch mit

selbst gewählten pseudonymen Angaben schützen. Wird eine E-Mail-Adresse verlangt, bieten sich Dienste wie *www.trashmail.net* oder *www.spamgourmet.com* an, die E-Mail-Adressen bereitstellen, die automatisch nach wenigen Tagen ungültig werden.

2.2.4 Rechtliche Bewertung

Die Aufzeichnung oder Protokollierung von Daten über die Nutzung bestimmter Internetdienste ist unzulässig. Der Einsatz von Cookies ist nur nach Aufklärung und mit Zustimmung der Nutzenden für einen konkreten Einsatzzweck zulässig[41]. Insbesondere die Art und Weise der Cookie-Nutzung durch Webseitenübergreifende Werberinge ist unzulässig, da hierfür i. d. R. keine Einwilligung der nutzenden Person und keine Geschäftsbeziehung zwischen ihr und dem Betreiber des Werberinges vorliegt.

Die IP-Adresse ist ein personenbezogenes Datum, dessen Aufzeichnung nur insoweit und nur so lange erlaubt ist, wie sie zur Diensterbringung erforderlich ist. Damit dürfen Betreiber von Internetangeboten nur protokollieren, welche IP-Adressen zu welchem Zeitpunkt welche Webseiten abgerufen haben, soweit dies für die Diensterbringung oder die Abrechnung erforderlich ist[42]. Für die Erbringung des Dienstes ist die Protokollierung in aller Regel nicht erforderlich. An der grundsätzlichen Unbeobachtbarkeit der Internet-Nutzung hat sich auch durch das Gesetz zur Vorratsdatenspeicherung nichts geändert. Zwar sollen danach ab Januar 2009 die Internetzugangsanbieter die an die Teilnehmenden vergebenen IP-Adressen für 6 Monate speichern und zum Abruf für Polizei, Strafverfolgungsbehörden und Nachrichtendienste bereithalten[43]. Die Datenschutzbeauftragten des Bundes und der Länder halten diese Regelung allerdings für unvereinbar mit deutschem Verfassungsrecht[44]. Selbst wenn das Gesetz der Überprüfung durch das Bundesverfassungsgericht standhalten sollte, verbietet es ausdrücklich die Speicherung von Kommunikationsinhalten und Daten über aufgerufene Internetseiten auf Vorrat[45].

---

[41] §§ 12, 13 Abs. 1 Satz 2 Telemediengesetz (TMG)

[42] § 15 Abs. 1, 4 TMG

[43] § 113 a Abs. 4 Telekommunikationsgesetz (TKG) i. d. F. Art. 2 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG v. 21. Dezember 2007, BGBl. I, 3198

[44] vgl. Dokumentenband 2007, S. 9

[45] § 113 a Abs. 8 TKG

Allerdings speichern in der Realität viele Webserver in Deutschland (rechtswidrig) und im Ausland, mit welcher IP-Adresse welche Internetseite zu welchem Zeitpunkt aufgerufen wurde. Suchmaschinen speichern Suchanfragen weltweit langfristig in personenbezogener Form (z. B. Google 18 Monate). Webangebote verfolgen mittels Cookies und anderer Mechanismen jede Bewegung ihrer teilweise identifizierbaren Nutzerinnen und Nutzer auf ihren Webseiten.

Dagegen hilft nur aktiver informationeller Selbstschutz. Die Nutzerinnen und Nutzer sollten sich genau über die Speicherpraxis der aufgerufenen Webseiten informieren und Seiten meiden, die keine oder unzureichende Informationen enthalten. Sie sollten nur solche Suchmaschinen nutzen, die die Suchergebnisse nicht langfristig speichern. Durch Konfiguration des Browsers können Cookies abgelehnt oder kontrolliert werden. Und schließlich ist es ratsam, Anonymisierungsdienste zu nutzen, die zumindest vor der Beobachtung durch private Dritte schützen.

Die Nutzung von Angeboten im Internet soll aus gutem Grund anonym und unbeobachtbar möglich sein. Sie ist in einer freiheitlichen Gesellschaft Teil der Informations- und Meinungsfreiheit. Gegen zunehmende Überwachungstendenzen von staatlicher und privater Seite sollten sich Surferinnen und Surfer zur Wehr setzen, indem sie die vorhandenen Werkzeuge zum informationellen Selbstschutz (z. B. Anonymisierungsdienste) verwenden.

2.3 Telefonieren im Internet (Voice over Internet Protocol – VoIP)

2.3.1 Die Technik des VoIP

Kaum eine Technik erlebte eine vergleichbar rasante Entwicklung, um sich dann in einem noch schnelleren Tempo als selbstverständlich in den Köpfen der Menschen zu manifestieren. Im Jahre 2005 gab es bereits zahlreiche Veröffentlichungen und Diskussionen, die Vorteile, Gefahren und Chancen dieser Technologie thematisierten. Inzwischen hat die Internet-Telefonie wie selbstverständlich ihren Einzug bei Wirtschaft und Privathaushalten gehalten. Es gibt keinen größeren Kommunikationsanbieter, der diesen Dienst nicht in seinem Angebot hat.

Internet-Telefonie/IP-Telefonie:

Unter Internet-Telefonie bzw. IP-Telefonie (Internet-Protokoll-Telefonie; auch Voice over IP (VoIP)) versteht man das Telefonieren über Computernetzwerke, die

nach Internet-Standards aufgebaut sind. Dabei werden für Telefonie typische Informationen, d. h. Sprache und Steuerinformationen, z. B. für den Verbindungsaufbau, über ein auch für Datenübertragung nutzbares Netz übertragen. Bei den Gesprächsbeteiligten können sowohl Computer, für IP-Telefonie spezialisierte Telefonendgeräte, als auch über spezielle Adapter angeschlossene klassische Telefone die Verbindung ins Telefonnetz herstellen.[46]

Bei der klassischen Telefonie im Festnetz wird nach der erfolgreichen Vermittlung ein für die Zeit der Verbindung fester Kanal zur Übertragung der Töne bereitgestellt. Die Vermittlung erfolgt zum Beispiel beim in Deutschland eingesetzten ISDN über das sog. D-Kanal-Protokoll „DSS1“. Dies ist jene Funktion, die in der Anfangszeit der Telefonie „Das Fräulein vom Amt“ wahrnahm, das die Verbindung manuell zusammenstöpselte.

Die Internet-Telefonie verfolgt dagegen einen anderen Ansatz. Grundlage für die Übertragung bei VoIP ist ein Datennetzwerk auf der Basis des Internet-Protokolls (IP). Das bekannteste und größte Netzwerk auf dieser Basis ist das Internet. Aber auch Firmennetze und sogar Netze in Privathaushalten verwenden Netze auf der Basis von IP.

Das Prinzip ist immer gleich. Die Sprachinformationen werden beim Sender in digitale Signale umgewandelt. Solche Wandlungsverfahren werden in der Fachsprache „Codec“ genannt. Die Empfängerin und der Empfänger müssen den gleichen „Codec“ verwenden, um die Daten wieder in hörbare Sprache umzuwandeln. Jetzt müssen die Daten in geeigneter Form über das Netz gesendet werden. Erschwerend ist der Umstand, dass über das Datennetzwerk im Gegensatz zur klassischen Telefonie eine Vielzahl anderer Dienste, wie beispielsweise E-Mail oder World Wide Web (WWW), die zur Verfügung stehende Bandbreite nutzt.

Die Realisierung von Voice over IP verlangt einige Übertragungsprotokolle, die auf die Besonderheiten der Telefonie im Internet eingehen, weil die Struktur des Internet-Protokolls nicht für die Übertragung von Daten in Echtzeit konzipiert ist.

Zur Umgehung dieser Probleme wurde speziell das *Real-Time Transport Protocol (RTP)* entwickelt, über das der eigentliche Transport der Sprachdaten erfolgt. Gesteuert wird das RTP durch das Real-Time Control Protocol (RTCP). RTP verwendet zur Übertragung in der Regel das User Datagram Protocol (UDP), welches allerdings nicht auf Zuverlässigkeit ausgelegt wurde. Dies bedeutet, dass der Emp-

[46] aus Wikipedia (http://de.wikipedia.org/wiki/IP-Telefonie), Stand: 7. Februar 2008

fang der Sprachpakete nicht bestätigt wird, also keine Übertragungsgarantie besteht. Der Vorteil von UDP ist aber dessen geringere Verzögerungszeit, da nicht auf eine Bestätigung gewartet werden muss und sich somit der Datenfluss insgesamt nicht verzögert. Eine vollkommen fehlerfreie Übertragung ist aufgrund der hohen Redundanz gesprochener Sprache und der Möglichkeit der verwendeten Codecs, Fehler zu korrigieren, nicht erforderlich.

Für eine störungsfreie Sprachübertragung ist trotzdem ein Mindestmaß an Leitungskapazität erforderlich. Ist die Kapazität zu gering, können einzelne Datenpakete verloren gehen oder nicht rechtzeitig zugestellt werden, sodass der Sprachempfang empfindlich gestört wird. Die Ursache dafür liegt meist im Datenstrom von der Teilnehmerin oder vom Teilnehmer zum Provider des genutzten DSL-Angebots (Upstream), der üblicherweise nur ca. 10 % des Datenstroms in umgekehrter Richtung (Downstream) beträgt.

Die Priorisierung der Sprachdaten hilft bei kleinem Upstream. VoIP-fähige Router und Adapter, die dem Sprachverkehr eine feste Bandbreite reservieren oder die Sprachpakete gegenüber Datenpaketen vorrangig behandeln, übernehmen diese Priorisierung. Die meisten Router, die von den VoIP-Anbietern zusammen mit den DSL-Anschlüssen vermarktet werden, unterstützen diese QOS[47] genannte Funktion.

Bevor ein Gespräch beginnt, muss eine Verbindung aufgebaut werden. Damit sie zu einem bestimmten VoIP-Endgerät aufgebaut werden kann, muss dessen Adresse eindeutig bekannt sein. Jedes VoIP-Endgerät benötigt ein eindeutiges Identifizierungsmerkmal (vergleichbar dem Adressschild am Briefkasten). Für die hier betrachteten Netze ist dies die IP-Adresse.

Allerdings werden meistens keine festen IP-Adressen verwendet. Durch einen speziellen Dienst (DHCP – Dynamic Host Configuration Protocol) wird ihnen bei jedem Verbindungsaufbau mit dem Netzwerk eine neue dynamische IP-Adresse zugewiesen. Zusätzlich verwenden viele Nutzende Router, die Network Address Translation (NAT/IP Masquerading) beherrschen, womit mehrere Nutzende sich eine IP-Adresse im Internet teilen können. Es ist also nicht ohne Weiteres möglich festzustellen, unter welcher IP-Adresse das gewünschte VoIP-Endgerät zu erreichen ist.

[47] Quality of Service

2.3

Um diesem Problem zu begegnen, wurde das *Session Initiation Protocol (SIP)* entwickelt. Es erlaubt SIP-Endgeräten, wie beispielsweise einem SIP-Telefon, sich auf einem SIP-Server zeitlich befristet anzumelden.

SIP-Endgeräte, die eine Verbindung zu einem anderen SIP-Endgerät aufbauen wollen, können die aktuelle IP-Adresse beim SIP-Server erfragen. Die Adressierung findet über das vom E-Mail-Dienst bekannte Format[48] statt. Eine Teilnehmeradresse würde dann z. B. "sip:user@domain.land" lauten. Dies bietet die Möglichkeit, zukünftig über eine Adresse erreichbar zu sein, die dann sowohl für E-Mail als auch Telefonie Verwendung findet.

Das Design des SIP lehnt sich an das http-Protokoll (Hypertext Transfer Protokoll) an, das beim WWW zur Anwendung kommt. Um eine eigene SIP-Adresse (URI) zu bekommen, muss man sich bei einem Anbieter registrieren lassen. Viele Anbieter ermöglichen das Telefonieren im klassischen Telefonnetz (Festnetz/Mobilfunk). Meistens werden keine klar ersichtlichen SIP-Adressen vergeben, sondern hauptsächlich herkömmliche Rufnummern.

Mittlerweile implementieren immer mehr Hersteller SIP als Protokoll für den Verbindungsaufbau, sodass sich SIP zum Standard-Verbindungs-Protokoll für Voice over IP entwickelt.

Neben SIP existiert der Standard *H.323*, der funktional mit dem SIP-Protokoll vergleichbar ist. Es wurde für die Übertragung von Multimedia-Applikationen entwickelt und ist ein weiterer internationaler Standard für die Sprach-, Daten- und Videokommunikation über paketorientierte Netze. Der H.323-Standard besteht aus diversen Protokollen für die Signalisierung, zum Austausch von Endgerätefunktionalitäten, zur Verbindungskontrolle, zum Austausch von Statusinformationen und zur Datenflusskontrolle. Inzwischen liegt die dritte Version dieses Standards für die Übertragung von Leistungsmerkmalen vor.

Eine weit verbreitete und unentgeltlich erhältliche proprietäre Software für Internet-Telefonie und Instant Messaging[49] ist unter dem Name *Skype* bekannt. Für Skype spricht der Umstand, dass es auch hinter den meisten Firewalls und NAT-

[48] Uniform Resource Identifier (URI)

[49] sofortige Nachrichtenübermittlung

Routern[50] problemlos arbeitet. Entwickelt wurde die Software von Programmierern der Internettauschplattform KaZaA.

Ursprünglich ermöglichte Skype das kostenlose Telefonieren über das Internet zwischen zwei Rechnern. Mittlerweile ist aber auch das gebührenpflichtige Telefonieren zum Festnetz bzw. zu Mobilfunknetzen („SkypeOut“) möglich. Der ebenfalls gebührenpflichtige Dienst „SkypeIn“ ermöglicht die Erreichbarkeit aus dem herkömmlichen Telefonnetz. Auch zusätzliche Dienste wie beispielsweise die Konferenzschaltungen sind für bis zu zehn Gesprächsteilnehmerinnen und -teilnehmer möglich.

Zur Wahrung der Vertraulichkeit können Verbindungen von PC zu PC verschlüsselt werden. Da der Programmkode nicht öffentlich ist, kann über die Sicherheit des Verfahrens keine Aussage gemacht werden.

Da das Skype-VoIP-Protokoll nicht auf Standardprotokollen basiert, kann es nur mit der originalen Skype-Software genutzt werden. Über eine Programmierschnittstelle (Skype-API) ist es auch externen Programmen möglich, auf Funktionalitäten des Skype-Clients und auf Teile des Skype-Netzwerkes zuzugreifen.

Dem Grunde nach ist Skype ein sog. Peer-to-Peer-Dienst. Das bedeutet, dass es keine zentrale Infrastruktur gibt, auf die die Teilnehmenden zugreifen. Die Rechner der Nutzenden sind zugleich Klient, Weiterleitungsknoten als auch Server. Nur bei Nutzung der gebührenpflichtigen Dienste „SkypeIn“ und „SkypeOut“ werden zentrale Knoten genutzt.

2.3.2 Der Datenschutz bei VoIP

Durch die Nutzung der IP-Technologie für das Telefonieren erbt VoIP alle Unzulänglichkeiten und Sicherheitsprobleme öffentlicher TCP/IP-basierter und lokaler Netzwerke[51]. So können Viren, Würmer, Trojaner und sog. „Denial of Service“-(DoS)-Attacken die Internet-Telefonie nicht nur betreffen, sondern sie können die Netzwerke der VoIP-Anbieter selbst nutzen, um Schaden anzurichten. VoIP besitzt

[50] Network Address Translation (NAT) ist der Sammelbegriff für verschiedene Verfahren, mit denen Adressinformationen in Datenpaketen durch andere ersetzt werden können. Sie werden auf Routern und Firewalls eingesetzt.

[51] Sie waren das Thema beim Internationalen Symposium „Datenschutz und Datensicherheit bei Internet-Telefonie“ 2006, vgl. JB 2006, 10.1.7.

aber auch Unzulänglichkeiten der konventionellen Telefonie, wie z. B. die unverschlüsselte Datenübertragung.

Wer bei der herkömmlichen Telefonie ein Telefonat abhören wollte, brauchte einen physikalischen Zugang zur Leitung oder zur Vermittlungstechnik. Für einen Angriff unter VoIP muss kein physikalischer Zugang mehr bestehen, es reicht ein logischer Zugang zu einer der beteiligten IP-Komponenten. Dies kann die IP-Infrastruktur der Teilnehmerin oder des Teilnehmers, wie z. B. ein DSL-Modem oder ein Switch in einem Hotel sein, aber auch eine IP-Komponente des VoIP-Anbieters oder im Internet.

Die zum Standard gewordenen VoIP-Kommunikationsprotokolle SIP und RTP verschlüsseln die Daten nicht. Die Daten können daher von sog. Snifferprogrammen[52] abgehört werden, die im Internet in vielfältiger Weise verfügbar sind. Oft ist es nicht einmal erforderlich, die Datenleitungen dauerhaft abzuhören. Man muss nur einmalig die Anmeldedaten in Erfahrung bringen, die das VoIP-Telefon gegenüber dem SIP-Server verwendet. Diese Daten sind oft auch im Menü des VoIP-Telefons einsehbar, sodass es ausreicht, kurz physischen Zugriff auf das Gerät zu haben. Dann kann man gegenüber dem SIP-Server als berechtigte Person auftreten, d. h. beispielsweise Telefonate auf fremde Kosten führen, Telefongespräche umleiten oder ggf. unbemerkt durch Aktivierung der Konferenzschaltung abhören. Die Möglichkeit des einfachen Fälschens der Rufnummer erfordert ein Umdenken bei der Nutzung der gesendeten Rufnummer zu Zwecken der Authentifizierung.

Es wurden allerdings Protokolle entwickelt, die die vermisste Sicherheit wiederbringen können. Mit dem Protokoll *SRTP (Secure RTP)* wurde RTP um Funktionen erweitert, die die Vertraulichkeit, Authentizität und Integrität der zu übertragenden Sprachdaten gewährleisten. Voraussetzung dafür ist, dass sich die Beteiligten vertraulich auf einen Sitzungsschlüssel einigen. Er ist nur für dieses eine Gespräch gültig. Die Sicherheit der Sprachdaten ist also von dem sicheren Austausch des Sitzungsschlüssels abhängig. Er kann z. B. als Teil der Signalisierungsnachricht beim Verbindungsaufbau übertragen werden. Das ist aber nur dann sinnvoll, wenn auch die Signalisierungsdaten verschlüsselt übertragen werden. Dazu kann das *TLS-Protokoll (Transport Layer Security)* verwendet werden, das auch bei der sicheren Übertragung von Webseiten eingesetzt wird. Es sichert allerdings nur den Übertragungsweg zwischen den beteiligten SIP-Servern und VoIP-Endgeräten. Die Signalisierungsdaten und damit auch der Sitzungsschlüssel liegen auf den SIP-Servern unverschlüsselt vor. Die Vertraulichkeit der Kommunikation hängt also

[52] Software, die den Datenverkehr eines Netzwerks heimlich empfangen, aufzeichnen, darstellen und ggf. auswerten kann

von der Vertrauenswürdigkeit der SIP-Server und damit vom VoIP-Betreiber ab. Eine Ende-zu-Ende-Sicherheit könnte man durch den Einsatz von Client-Zertifikaten und den Aufbau einer Public Key Infrastructure (PKI) zur Verwaltung der Zertifikate erreichen. Dieses stellt jedoch einen komplexen und aufwändigen Vorgang dar.

Phil Zimmermann, der Erfinder von PGP (Pretty Good Privacy), ein bei der E-Mail-Kommunikation weit verbreiteter Verschlüsselungsmechanismus, erweiterte RTP mit ZRTP um die Möglichkeit, über den Sprachkanal einen geheimen Sitzungsschlüssel auszuhandeln. Das wird mithilfe des nach seinen Erfindern benannten Diffie-Hellman-Schlüsselaustauschs realisiert. Durch Nutzung dieses Verfahrens ist es den Angreifenden unmöglich, den Schlüssel ebenfalls zu berechnen. Zur eigentlichen Verschlüsselung wird dann der Krypto-Algorithmus AES-128 (Advanced Encryption Standard mit 128 Bit Schlüssellänge) verwendet. Aber auch dieses Verfahren hat einen Wermutstropfen: Durch einen klassischen Man-In-The-Middle-Angriff[53] könnte es den Angreifenden gelingen, sich zwischen die miteinander Kommunizierenden zu schalten und den Schlüsselaustausch zu manipulieren. In diesem Fall würden zwei Schlüssel ausgehandelt werden, einer zwischen der anrufenden und der angreifenden Person und einer zwischen der angreifenden und der angerufenen Person. Da Angreifende beide Schlüssel kennen, wäre ein Mithören dann möglich. Um das zu verhindern, wird ein „Fingerabdruck“ des Sitzungsschlüssels verwendet. Dieser besteht aus vier alphanumerischen Zeichen und wird aus dem Sitzungsschlüssel berechnet. Die miteinander Kommunizierenden vergleichen den Fingerabdruck vorab: Ist er nicht identisch, sitzt ein angerufener „Mittelsmann“ dazwischen.

Neben der Vertraulichkeit ist beim Telefonieren natürlich auch die Verfügbarkeit ein wichtiges Merkmal. Die Verfügbarkeit kann in IP-Netzen durch sog. DoS-Attacken (Dienstverweigerung) grundlegend gestört werden. Dies bedeutet, dass – unabhängig von VoIP – das darunter liegende Netzwerk solchen Überlastangriffen ausgesetzt wird und seinen Dienst, die Datenübertragung, nicht mehr ausführen kann. Es sind aber auch VoIP-spezifische DoS-Attacken denkbar[54]. So könnte das Einschleusen massenhafter Verbindungsaufbauwünsche über das SIP-Protokoll einen SIP-Server lahmlegen oder zumindest signifikant verlangsamen, sodass die Qualität deutlich nachlässt.

---

[53] Ein Man-In-The-Middle-Angriff (MITM-Angriff) ist eine Angriffsform, bei der der Angreifer entweder physikalisch oder - heute meist - logisch zwischen den beiden Kommunikationspartnern steht, dabei mit seinem System komplette Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern hat und somit die Informationen nach Belieben einsehen und sogar manipulieren kann. Quelle: Wikipedia

[54] Der erste derartige Angriff wurde im Oktober 2007 bekannt.

2.3

Bedrohungen und Gefahren bestehen auch im Bereich der Endgeräte, also den eigentlichen Telefonen. Telefone für VoIP unterscheiden sich erheblich von den altbekannten Telefonen. Während bisherige Telefone vergleichsweise „dumm" sind, sind VoIP-fähige Telefone aktive Netzkomponenten und daher für übliche Angriffe anfällig. Neben VoIP-fähigen Telefonen gibt es auch noch sog. Softphones. Ein *Softphone* ist ein Computerprogramm, das Telefonie ermöglicht und häufig von Anbietern von VoIP-Diensten zur Verfügung gestellt wird. Softphones sind besonders gefährdet, da der das Programm verarbeitende Rechner und sein Betriebssystem mit üblichen Würmern, Trojanern und Viren angegriffen werden kann.

Die geringen Kosten für E-Mails im Internet haben zu einem starken Aufkommen von unerwünschten Nachrichten (SPAM-E-Mails) geführt. Der Anteil ist mittlerweile immens hoch und man versucht ihm mit SPAM-Filtern zu begegnen. Bei VoIP wird die gleiche Entwicklung erwartet. Mit zunehmender Verbreitung von VoIP wird die Anzahl der SPAM-Anrufe (*SPIT – Spam over Internet Telephony)* erheblich zunehmen. Wirkungsvolle Filter existieren zz. leider noch nicht. SPIT ist zudem besonders lästig, da Telefonieren im Gegensatz zur E-Mail eine Echtzeitanwendung ist und die Belästigung unmittelbar erfolgt.

Neben den oben dargestellten Risiken bei VoIP bringt die Nutzung von Skype zusätzliche Probleme. Der Umstand, dass Skype auf Basis eines Peer-to-Peer-Netzwerks arbeitet, macht die Überwachung durch Strafverfolgungsbehörden schwierig. Juristisch befindet sich Skype in einer rechtlichen Grauzone, da nicht klar ist, wer i. S. d. Gesetzgebung Provider ist.

Aufgrund seiner Funktionsweise sind nur wenige Firewall-Produkte in der Lage, Skype zu kontrollieren. Neben der Telefonie-Funktion beinhaltet Skype weitere Dienste, die ein Sicherheitsproblem darstellen können. So können z. B. Dateien ungefiltert übertragen werden. Auf diesen Umstand weist der Hersteller sogar in seiner Datenschutz-FAQ (Frequently Asked Questions) hin[55]. Diese zusätzlichen Funktionen gefährden im hohen Maße die Vertraulichkeit, Integrität und Verfügbarkeit.

Das Bundesamt für Sicherheit in der Informationstechnik hat eine umfangreiche Studie zur Sicherheit von Voice over Internet Protocol (VoIPSEC) herausgegeben. Unter https://downloads.bsi-fuer-buerger.de/literat/studien/VoIP/voipsec.pdf findet man diese zur weiteren Vertiefung.

[55] „Bei der Dateiübertragungsfunktion von Skype müssen Sie vorsichtig sein, wenn Sie Dateien von anderen empfangen."

VoIP beinhaltet all die Unzulänglichkeiten und Sicherheitsprobleme öffentlicher TCP/IP-basierter und lokaler Netzwerke und der konventionellen Telefonie. Bei der Auswahl des VoIP-Anbieters wie auch der Hard- und Software sollte darauf geachtet werden, dass sie Verschlüsselungstechniken unterstützen.

2.4 Biometrische Authentisierung

Zur Feststellung, ob eine Person bestimmte Berechtigungen nutzen kann, z. B. zum Zutritt in ein Gebäude oder einen Raum (Zutrittskontrolle)[56], zur Nutzung eines Computers (Zugangskontrolle)[57] oder zur Ausübung bestimmter Rechte auf einem IT-System (Zugriffskontrolle)[58] ist die Authentisierung der Person erforderlich. Diese erfolgt in zwei Schritten: Zunächst gibt die Person ihre Identität preis (Identifizierung) und im zweiten Schritt verifiziert sie ihre Identität durch einen entsprechenden Nachweis. Bei der Authentisierung einer Person durch eine andere Person, z. B. einen Polizeibeamten bei einer Personenkontrolle, erfolgen beide Schritte zusammen: Der Polizist lässt sich einen Ausweis zeigen, kann damit die Person identifizieren, indem er den Namen liest, und hat gleichzeitig ein Objekt in der Hand, das es ihm möglich macht festzustellen, ob die vor ihm stehende Person mit dem Ausweisinhaber übereinstimmt.

Die Authentisierung gegenüber einem automatischen System, wie z. B. einem Computer, führt im Erfolgsfall zur Erteilung einer Berechtigung (Acceptance), das System zu benutzen, anderenfalls zu einer Rückweisung (Rejection). In beiden Fällen sind Folgeaktionen möglich. So kann protokolliert werden, wer welche Rechte wann erhalten hat, aber auch wer sich vergeblich um die Rechte bemüht hat. Im letzteren Falle könnte auch eine Alarmierung erfolgen, weil sich möglicherweise eine unberechtigte Person die Rechte verschaffen wollte.

2.4.1 Methoden der Authentisierung

Es gibt verschiedene Prinzipien, mit denen eine automatische Authentisierung erfolgen kann. Man unterscheidet zwischen der Authentisierung durch Besitz, durch Wissen und durch körperliche Merkmale.

[56] Nr. 1 der Anlage zu § 9 Abs. 1 BDSG
[57] Nr. 2 der Anlage zu § 9 Abs. 1 BDSG
[58] Nr. 3 der Anlage zu § 9 Abs. 1 BDSG

2.4

Die Authentisierung durch Besitz erfolgt mit maschinenlesbaren Ausweisen, wobei eine Chipkartenlösung gegenüber einer Magnetstreifenkartenlösung aus Sicherheitserwägungen vorzuziehen ist. Weitere Möglichkeiten gibt es mit Hardwarekomponenten wie USB-Sticks oder RFID-Schlüsseln sowie mit der elektronischen Signatur.

Die Authentisierung durch Wissen erfolgt gemeinhin mittels geheim zu haltender Passwörter oder Persönlicher Identifikations-Nummern (PIN).

In vielen Fällen werden Authentisierungsverfahren mittels Besitz oder Wissen miteinander kombiniert. Bekannt ist dies zum Beispiel bei der Benutzung des Geldautomaten, bei der sowohl eine Scheck- oder Kreditkarte als auch eine PIN benutzt werden müssen.

An dieser Stelle stehen jedoch Authentisierungsverfahren mithilfe körperlicher Merkmale im Vordergrund des Interesses. Diese Authentisierung wird auch als *biometrische Authentisierung* bezeichnet. Dabei sind folgende biometrische Verfahren bekannt:

- Fingerabdruck
- Gesichtsgeometrie
- Handabdruck
- Stimmanalyse
- Unterschriftserkennung
- Iriserkennung
- Retinascanning (Netzhaut)
- Bewegungsanalyse
- Handvenenstrukturen (in Infrarotlicht)
- Genomanalyse.

Hinzu kommen Kombinationen dieser Verfahren wie z. B. Gesichtserkennung mit Stimmanalyse und Bewegungsanalyse der Mundpartie beim Sprechen.

Biometrische Merkmale, die zur Authentisierung taugen, sollen

- in der Grundausprägung gleich sein (also z. B. alle Fingerabdrücke),

- in der persönlichen Ausprägung einmalig sein (dies gilt z. B. nicht bei der Genomanalyse, weil die Genome eineiiger Zwillinge identisch sind),

- sich über das ganze Leben nicht verändern können und

- von technischen Systemen leicht erfasst werden können.

Die technische Realisierung eines biometrischen Authentisierungsverfahrens erfolgt stets in ähnlicher Weise:

Ausgangspunkt ist die Erfassung eines biometrischen Merkmals mittels optischer, thermischer, chemosensorischer, akustischer oder drucksensitiver Verfahren für spätere Vergleichszwecke. Aus den erfassten Rohdaten wird mittels geeigneter Algorithmen mithilfe des Computers ein sog. „Template“ (Muster) berechnet und zentral oder dezentral für spätere Vergleiche (z. B. auf einer Chipkarte) abgespeichert.

Beim eigentlichen Authentisierungsvorgang wird mit den gleichen Erfassungssystemen das biometrische Merkmal erfasst und ebenfalls mit den geeigneten Algorithmen berechnet. Das Ergebnis der Berechnung am aktuellen Merkmal wird als „biometrische Signatur“ bezeichnet. Diese Signatur wird mit dem hinterlegten Template computergestützt verglichen. Das Ergebnis dieses Vergleichs führt dann zur automatisierten Entscheidung, ob die Authentisierung zum Erfolg führt oder nicht.

2.4.2 Treffsicherheit biometrischer Verfahren

Die Treffsicherheit biometrischer Verfahren folgt Gesetzen der Wahrscheinlichkeit. Es ist stets davon auszugehen, dass Signatur und Template nie gleich sind. Wären sie es, sollte von einer Manipulation ausgegangen werden, weil dann denkbar ist, dass anstelle einer aktuellen Signatur eine illegal verfügbare Kopie des Templates zum Vergleich herangezogen worden wäre. Der Vergleich zwischen Signatur und Template kann daher allemal nur einen Grad von Ähnlichkeit ermitteln.

Je nach den Anforderungen an die Treffsicherheit des biometrischen Erkennungssystems muss ein Schwellenwert für die Ähnlichkeit festgelegt werden, über dem die Berechtigung vergeben und unter dem sie verweigert wird. Je höher (oder geringer) der Schwellenwert gewählt wird, desto geringer (oder höher) ist die Wahrscheinlichkeit, dass eine Berechtigung unzutreffend erteilt wird. Andererseits steigt (sinkt) mit dem Schwellenwert die Wahrscheinlichkeit, dass jemand unberechtigt abgewiesen wird.

2.4

Die Treffsicherheit von biometrischen Erkennungsverfahren wird mit verschiedenen Kenngrößen beschrieben, den sog. Rates.

Die Wahrscheinlichkeit, dass jemand unrichtigerweise zurückgewiesen wird, wird als „False Rejection Rate“ (FRR) bezeichnet; die Wahrscheinlichkeit, dass jemand unberechtigterweise eine Berechtigung erteilt bekommt, wird als „False Acceptance Rate“ (FAR) bezeichnet. Die „Equal Error Rate“ ist der Schwellenwert, für den FRR=FAR gilt, und der damit einen sinnvollen Kompromiss hinsichtlich der Sicherheitskalibrierung darstellt. Von den vielen übrigen „Rates“, die etwas über das biometrische System aussagen, sei noch die „Failure to Enroll Rate“ (FTE) erwähnt, die die Wahrscheinlichkeit benennt, dass von einer Person aus medizinischen Gründen kein brauchbares Template zu späteren Vergleichszwecken gewonnen werden kann. Dies gilt vor allem für Fingerabdrücke, bei denen FTEs von ca. 2 % ermittelt worden sind.

FRR und FAR sind abhängig

- von der Qualität des biometrischen Systems hinsichtlich der Genauigkeit der Erfassung, der Qualität der Template- und Signatur-Berechnung sowie der Genauigkeit des Vergleichs,

- von der Kalibrierung des biometrischen Systems, also der Wahl der Schwellenwerte und

- der Kooperation der Betroffenen.

Bei allzu genauer Kalibrierung wird die FRR zu groß, d. h. z. B., bei einem Zutrittskontrollsystem bleiben zu viele Berechtigte vor der Tür. Dagegen führt eine zu ungenaue Kalibrierung zu einer großen FAR, d. h. zu viele Unberechtigte durchschreiten die Tür.

An dieser Stelle ist eine Gegenüberstellung von Authentisierungsverfahren auf der Grundlage von Besitz und Wissen einerseits und auf der Grundlage körperlicher Merkmale andererseits angebracht: Verfahren aufgrund von Besitz und Wissen sind in ihrer Aussagestärke kausal, d. h., nach dem Einsatz des Authentisierungsmittels steht eindeutig fest, ob jemandem eine Berechtigung erteilt werden darf oder nicht. Dagegen ist die Aussagestärke eines biometrischen Verfahrens wahrscheinlichkeitsgesteuert, d. h., nach dem Einsatz des Authentisierungsmittels besteht die Klarheit nur mit einer bestimmten, meist deutlich unter 100 % liegenden Wahrscheinlichkeit.

Dieser Schwäche biometrischer Verfahren steht gegenüber, dass sie kaum kompromittierbar (fälschbar) sein dürften. Eine Fälschung der biometrischen Merkmale bei der Authentisierung gilt zwar nicht als ausgeschlossen, dürfte jedoch einen übermäßigen Aufwand bei hoher krimineller Energie erfordern. Dies kann man bei den Verfahren mit Besitz oder Wissen nicht behaupten. Ein Passwort ist leicht verraten oder ausgespäht, ein maschinenlesbarer Ausweis ist leicht weitergegeben, gestohlen oder gar gefälscht.

Die Stärke biometrischer Verfahren kann sich daher nur entfalten, wenn sie durch eine Methode mit Besitz oder Wissen ergänzt wird und dabei den kausalen Verfahren höhere Sicherheit vor Kompromittierung verleiht. Die biometrischen Verfahren bedürfen also stets einer solchen Ergänzung, für sich allein sind sie wegen der FRR und der FAR wertlos.

2.4.3 Produkte im praktischen Einsatz

Eine aktuelle Produktübersicht[59] führt 33 Hersteller auf, die 38 Produkte anbieten. Die Produkte verteilten sich auf folgende biometrische Verfahren:

- 24 Systeme für Fingerabdrücke
- 8 Systeme mit Gesichtserkennung
- 2 Systeme mit Iriserkennung
- 1 System mit der Handvenenerkennung
- 3 kombinierte Systeme
  (Fingerabdruck / Handabdruck / Gesichtserkennung, Fingerabdruck / Gesichtserkennung / Iriserkennung, Fingerabdruck / Gesichtserkennung).

2.4.4 Datenschutz bei der biometrischen Authentisierung

- Die biometrische Authentisierung ergänzt die Authentisierung mit Besitz oder Wissen und führt zur wesentlich höheren Sicherheit gegen Identitätsdiebstahl durch Täuschung des Systems. Dies ist am Beispiel des biometrischen Reisepasses bzw. Personalausweises berechtigterweise in einer heftigen Diskussion eingewandt worden. Technisch-organisatorische Datenschutzziele wie die Zutritts-, Zugangs- und Zugriffskontrolle nach Nr. 1, 2 und 3 der Anlage zu § 9 BDSG sind nur mit sicherer Authentisierung zu erreichen, sodass die Biometrie hier erhebliche Fortschritte bringt.

[59] iX 10/2007, S. 52

2.4

- Als Sicherheitsrisiko gilt die missbräuchliche Verwendung von Templates durch den unbefugten Zugriff auf Systeme, auf denen die Templates gespeichert sind. Ein solches System ist das eben erwähnte biometrische Ausweispapier, welches das Template selbst enthält. Wenn es gelingt, das Template auszulesen, so kann es zur Fälschung von Ausweisen und somit zum Identitätsdiebstahl kommen[60].

- Die bei der Gewinnung der biometrischen Vergleichsdaten (Template, Signatur) zuerst erfassten Rohdaten enthalten Überschussinformationen, die z. B. Auskunft über Geschlecht, Alter, Ethnie oder Krankheiten geben. Es muss sichergestellt werden, dass diese Daten unmittelbar nach der Errechnung der Vergleichsdaten gelöscht werden.

- Biometrische Authentisierungsysteme, die der Verdachtsgewinnung dienen sollen, können auch Unverdächtige treffen. Gleiches gilt für Systeme, die aus der Masse heraus gesuchte Personen identifizieren können (z. B. der Feldversuch auf dem Mainzer Hauptbahnhof von Oktober 2006 bis Januar 2007[61]).

- Die permanente Aufzeichnung von biometrischen Authentisierungen kann zu Bewegungsprofilen führen und dann – mit Zusatzwissen – auch zu Persönlichkeitsprofilen.

- Die Aufnahme biometrischer Merkmale in Ausweispapiere wird zu Begehrlichkeiten führen, sie auch zu vielen anderen Zwecken als nur der Grenzkontrolle oder der polizeilichen Personenkontrolle zu verwenden. Dadurch bergen diese Verwendungen die Gefahr der Totalüberwachung.

Die biometrische Authentisierung folgt anderen Gesetzen als die klassischen Verfahren mit Wissen oder Besitz. Für sich allein ist sie daher nur höchst eingeschränkt für die Authentisierung tauglich. Dagegen kann sie in Kombination mit den genannten kausalen Verfahren deren Probleme mit der Fälschbarkeit oder der unberechtigten Nutzung der echten Authentisierungsmittel mit hoher Effizienz beheben. Allerdings bietet die biometrische Authentisierung beim breiten Einsatz für die unbemerkte Erkennung von Personen in der Öffentlichkeit erhebliche Risiken für die Persönlichkeitsrechte.

---

[60] Bekanntlich haben holländische Hacker bereits vor zwei Jahren den holländischen Reisepass auslesen und dabei die – relativ schwache – Verschlüsselung brechen können. Der deutsche Reisepass ist etwas besser gesichert, aber auch nicht so, dass der Bruch der Verschlüsselung ausgeschlossen werden kann (http://www.netzeitung.de/internet/380265.html).

[61] vgl. dazu 11.4.2

2.5 Datenschutz in Berliner Banken

Wir haben im Berichtszeitraum vier Berliner Banken nach § 38 Abs. 4 BDSG kontrolliert. Es handelte sich um routinemäßige, nicht anlassbezogene Prüfungen. Auch wenn das datenschutzrechtliche Niveau bei zwei der geprüften Banken zufriedenstellend war, überraschte insgesamt doch die hohe Fehlerquote bei der Umsetzung datenschutzrechtlicher Vorgaben.

Zwei der vier kontrollierten betrieblichen Datenschutzbeauftragten verfügten nicht über die für diese Aufgabe erforderliche Fachkunde[62]. Eine Datenschutzbeauftragte konnte die erforderliche Fachkunde durch Nachschulungen erlangen, bei dem zweiten Datenschutzbeauftragten werden wir im Rahmen einer Nachkontrolle prüfen, ob seine Bestellung zum Datenschutzbeauftragten nach § 4 f Abs. 3 Satz 3 BDSG zu widerrufen ist. Einem betrieblichen Datenschutzbeauftragten fehlte die erforderliche Zuverlässigkeit, da er gleichzeitig als Geldwäschebeauftragter arbeitet. Die gleichzeitige Tätigkeit als Geldwäsche- und als Datenschutzbeauftragter ist wegen Interessenkonflikten ausgeschlossen, da der Geldwäschebeauftragte umfangreiche Zugriffe auf personenbezogene Daten hat und sich als Datenschutzbeauftragter in seiner Funktion als Geldwäschebeauftragter selbst kontrollieren müsste.

Banken sind wie alle verantwortlichen Stellen gesetzlich[63] verpflichtet, ein Verfahrensverzeichnis zu führen. Keines der uns von den Banken vorgelegten Verzeichnisse erfüllte die gesetzlichen Vorgaben. So differenziert der Gesetzgeber nicht zwischen einem internen und einem externen Verfahrensverzeichnis, es wurde außerdem nicht beachtet, dass auch das jedermann verfügbar zu machende Verzeichnis die Informationen nach § 4 e Nr. 1 - 8 BDSG vollständig enthalten muss. Teilweise wurden ganze Verfahren, wie z. B. Personaldatenverwaltung und Videoüberwachung, vergessen, nur eine Bank hatte Angaben über geplante Datenübermittlungen in Drittstaaten gemacht, obwohl jede Bank am SWIFT-Verfahren teilnimmt. Nach § 4 e Nr. 7 BDSG muss das Verfahrensverzeichnis die Regelfristen für die Löschung der Daten enthalten. Hierbei reicht ein von einigen Banken gegebener Hinweis, dass die personenbezogenen Daten nach den gesetzlichen Bestimmungen gelöscht werden, nicht aus. Das Verfahrensverzeichnis muss vielmehr die tatsächlichen Regelfristen für die Löschung der Daten enthalten.

Eine der Banken hat mit ihrer Muttergesellschaft einen Geschäftsbesorgungsvertrag abgeschlossen und im Rahmen der Umsetzung dieses Vertrages wurden in größerem Umfang personenbezogene Daten an die Muttergesellschaft weitergelei-

[62] vgl. § 4 f Abs. 2 Satz 1 und 2 BDSG

[63] § 4 g Abs. 2 i. V. m. § 4 e Satz 1 Nr. 1 – 8 BDSG

tet. Hierbei hatte die Bank völlig übersehen, dass das Bundesdatenschutzgesetz kein Konzernprivileg kennt und deshalb nicht jede Datenübermittlung an die Muttergesellschaft rechtmäßig ist. Unproblematisch waren die Datenweitergaben an die Muttergesellschaft, soweit diese im Rahmen einer Auftragsdatenverarbeitung nach § 11 BDSG möglich waren. Wir haben der Bank aufgegeben, bei Vorliegen einer Funktionsübertragung jede Datenübermittlung an die Muttergesellschaft daraufhin zu überprüfen, ob diese durch eine Rechtsvorschrift gedeckt ist[64].

Als überraschend problematisch erwies sich bei zwei der geprüften Banken ihre starke Einbindung in eine Verbandsstruktur. Die Verbände erstellen für ihre angeschlossenen Banken Formulare, Rechtsgutachten, stellen ein Rechenzentrum zur Verfügung etc. Die Banken sind auf diese Hilfe angewiesen und übernehmen in der Praxis die Vorgaben des Verbandes, ohne diese zu hinterfragen bzw. hinterfragen zu können. Dies führt dazu, dass die Banken bei datenschutzrechtlichen Problemen auf ihre Verbände verweisen, die aber nicht selbst nach § 3 Abs. 7 BDSG verantwortliche Stellen sind. Hier einige Beispiele zu den aufgetretenen Problemen:

1. Fehlerhafte Formulare können von den Banken nicht problemlos umgeändert werden, eine Änderung ist nur mit Zustimmung des Verbandes möglich.

2. Die Banken sehen sich auch verpflichtet, datenschutzrechtlich zweifelhafte Rechtspositionen des Verbandes – etwa zu SWIFT oder zur Geldwäsche – umzusetzen.

3. Datenverarbeitungen, die in besonderem Maße das informationelle Selbstbestimmungsrecht berühren, wie z. B. Scoringverfahren oder Geldwäsche-Researchsysteme, sollten nach den von den Aufsichtsbehörden festgelegten Kriterien von dem betrieblichen Datenschutzbeauftragten vorab kontrolliert werden. Eine Vor-abkontrolle findet aber nicht statt bzw. verliert ihren Sinn, wenn die Banken von ihrem Verband fertige Systeme übernehmen, deren Funktionsweise ihnen zum Teil nicht einmal hinreichend bekannt ist.

Banken sind verpflichtet, bei Überweisungen ins Ausland Kundinnen und Kunden vorab darüber zu informieren, dass das von ihnen angewandte Überweisungssystem SWIFT die Überweisungsdaten in den USA, einem Land ohne ausreichendes Datenschutzniveau, spiegelt. Es reicht nicht aus, dass die Kundinnen und Kun-

[64] vgl. § 4 Abs. 1 BDSG

den diese Information erst nach erfolgter Überweisung erhalten oder nur dann, wenn sie die Internet-Seite ihrer Bank aufmerksam lesen. Keine der geprüften Banken hat Kundinnen und Kunden hinreichend – etwa durch eine Information auf dem Kontoauszug – über die Probleme bei Auslandsüberweisungen informiert. Eine Bank hat den gerügten Fehler inzwischen beseitigt.

Keine der kontrollierten Banken hat die Kundinnen und Kunden zudem darüber informiert, dass sämtliche Kontobewegungen mithilfe eines Research-Systems auf geldwäscherelevante Besonderheiten überprüft werden. Die von den Banken angewandten Geldwäschesysteme führten teilweise zu so geringen Anzeigequoten bei der Staatsanwaltschaft, dass sich die Frage stellte, ob die im Rahmen der Researchsysteme durchgeführten umfangreichen Datenverarbeitungen noch verhältnismäßig sind. Es wurde beanstandet, dass die Geldwäschebeauftragten der Banken teilweise mit anderen Geldwäschebeauftragten Informationen am Telefon austauschten, ohne dass vorab geklärt wurde, ob die anfragende Bank ein berechtigtes Interesse an der Kenntnis der personenbezogenen Daten der Bankkundin oder des Bankkunden hat. Hier haben wir eine sorgfältigere Prüfung von Datenflüssen – im schriftlichen Verfahren – gefordert.

Überraschend war, dass vorgelegte SCHUFA-Einwilligungserklärungen teilweise formungültig waren, da sie entgegen der gesetzlichen Regelung[65] im Text nicht besonders hervorgehoben wurden. SCHUFA-Anfragen erfolgten auch bei Personen, die aufgrund eines Negativdatums im SCHUFA-Datenbestand von Anfang an nur ein Konto für jedermann – ohne Überziehungsmöglichkeit – beantragt hatten, obgleich hier die Bank für die SCHUFA-Anfrage kein berechtigtes Interesse geltend machen kann. Auch dies haben wir beanstandet.

Eine Bank bietet den Service an, Darlehensanträge über das Internet zu stellen. Dabei willigt man online darin ein, dass eine SCHUFA-Abfrage (Kreditantrag – führt zu einer Verschlechterung des Scorewerts) durchgeführt wird. Mithilfe des von der SCHUFA übermittelten Scorewerts sowie eines eigenen Scoring-Verfahrens wird der Kundin oder dem Kunden schon im Internet die Information gegeben, ob ihr oder ihm ein Kredit gewährt und wie hoch der Zinssatz sein wird. Dieses Angebot der Banken führt dazu, dass Dritte bei Kenntnis weniger Grunddaten der Betroffenen die Möglichkeit haben, sich über ihre Bonität zu informieren. Dies verletzt nicht nur ihr informationelles Selbstbestimmungsrecht, auch ihr Scorewert bei der SCHUFA verschlechtert sich. Wir haben die Bank aufgefordert, den angebotenen Service so umzugestalten, dass eine Missbrauchsmöglichkeit ausgeschlossen ist. Eine Änderung im Bereich der Internetkredite war auch deshalb zu

[65] § 4 a Abs. 1 letzter Satz BDSG

fordern, da Einwilligungserklärungen in der Regel der Schriftform bedürfen. Ein besonderer Umstand, auf die Schriftform zu verzichten, liegt nicht vor. Grundsätzlich kann zwar eine besondere Eilbedürftigkeit den Verzicht auf die Schriftform der Einwilligung rechtfertigen, etwa bei telefonischer Erteilung eines sofort auszuführenden Auftrags. Der Auftrag zur Vergabe eines Kredites kann jedoch bereits aus Rechtsgründen (Identifikationspflicht) nicht sofort ausgeführt werden. Insofern fehlt es an der Eilbedürftigkeit.

In zwei der kontrollierten Banken wurde die rechtsfehlerhafte Auffassung vertreten, dass der bei ihnen gespeicherte SCHUFA-Scorewert den Betroffenen nicht mitgeteilt werden dürfe. Dieser Fehler basierte darauf, dass die SCHUFA den Banken untersagt, den SCHUFA-Scorewert an *Dritte* weiterzugeben. Die Banken übersahen allerdings, dass die Betroffenen nach § 3 Abs. 8 Satz 2 BDSG nicht *Dritte* sind.

Immer mehr Kreditentscheidungen werden nicht mehr von einer Banksachbearbeiterin oder von einem -sachbearbeiter, sondern maschinell im Rahmen eines Scoring-Verfahrens getroffen. Dies betrifft nicht nur die Frage, ob ein Kredit vergeben wird, sondern auch die Zinshöhe. Bei mehreren Bankkontrollen mussten wir darauf hinweisen, dass automatisierte Einzelentscheidungen zum Nachteil der Betroffenen – Nachteil i. S. d. Norm stellt auch ein höherer Zinssatz dar – nur dann rechtmäßig sind, wenn den Betroffenen das Recht eingeräumt wird, ihren gegenteiligen Standpunkt geldend zu machen[66]. Dies setzt aber voraus, dass die Kundinnen und Kunden auf dieses Recht hingewiesen werden und dass ihnen die Möglichkeit gegeben wird zu belegen, dass sie trotz des schlechten Scorewertes über eine ausreichende Bonität verfügen.

Insgesamt ist der Datenschutz bei den von uns überprüften Berliner Banken teilweise stark verbesserungsbedürftig.

2.6 Wofür steht BIS/IMI? – Neue E-Government-Infrastrukturen für die europaweite Verwaltungszusammenarbeit

Im Rahmen der EU-Binnenmarktgesetzgebung hat die Europäische Kommission im Jahr 2007 die Entwicklung eines IT-Netzwerks für den strukturierten Informationsaustausch zwischen den Behörden der Mitgliedstaaten vorangetrieben. Damit sollen – ausgehend von einem bestehenden Defizit - die tägliche Zusammenarbeit zwischen lokalen, regionalen und nationalen Verwaltungen bei der Um-

[66] vgl. § 6 a Abs. 1 und 2 BDSG

setzung und Anwendung der Binnenmarktvorschriften unterstützt und die Kosten für diese Zusammenarbeit verringert werden.

Mithilfe des webbasierten Binnenmarkt-Informationssystems (BIS) / Internal Market Information System (IMI) soll allen für die Anwendung der Binnenmarktvorschriften zuständigen Instanzen in den EU-Mitgliedstaaten unter einer einheitlichen Benutzeroberfläche der schnelle, sichere und verlässliche Informationsaustausch ermöglicht werden. Das System soll die Behörden eines Mitgliedstaats in die Lage versetzen, den geeigneten Ansprechpartner in einem anderen Mitgliedstaat ohne vorherige Kenntnis der dortigen Verwaltungsstrukturen ausfindig zu machen, gezielt Anfragen an ihn zu richten und diese Anfragen elektronisch zu verwalten (z. B. Statusabfrage, Fristenkontrolle, E-Mail-Benachrichtigung). Dabei kommen in 23 Sprachen vorübersetzte Bildschirmtexte und vorformulierte Fragenkataloge sowie auf spezifische Bereiche des Binnenmarktrechts zugeschnittene Software-Module zum Einsatz. Die Europäische Kommission liefert hierfür die entsprechende technische Infrastruktur und betreibt unter ihrer Verantwortung sämtliche Komponenten der IMI-Architektur (Web-Server, Application-Server, Datenbanken).

In einer ersten Stufe wird das Informations- und Kommunikationssystem IMI zur Unterstützung der Amtshilfevorschriften in der Richtlinie 2005/36/EG über die Anerkennung von Berufsqualifikationen vom 7. September 2005 zum Einsatz kommen. Ende 2007 wurde zunächst eine Pilotphase für vier Berufsgruppen (ärztliche Berufe, Apothekerinnen und Apotheker, physiotherapeutische Berufe und Steuerberatung) gestartet. 2008 soll eine Ausweitung auf die restlichen Berufe dieser Richtlinie und ab 2009 die Einbeziehung des Datenaustauschs auf der Basis der Richtlinie 2006/123/EG über Dienstleistungen im Binnenmarkt vom 12. Dezember 2006 erfolgen. Eine Öffnung des Systems für weitere Bereiche der Binnenmarktgesetzgebung ist geplant. Damit entstünde eine einheitliche Kommunikationsplattform für sämtliche Behörden in allen EU-Mitgliedstaaten mit weitreichenden Auswirkungen auf den Datenschutz.

Die zentralen Akteure des Systems sind die zuständigen Stellen in den Mitgliedstaaten der EU, die über IMI miteinander kommunizieren und untereinander Informationen austauschen sollen. Im Rahmen der Pilotierung wurden im Land Berlin bisher das Landesamt für Gesundheit und Soziales (ärztliche und physiotherapeutische Berufe), die Landesärztekammer (fachärzliche Qualifikation), und die Senatsverwaltung für Finanzen (Steuerberatung) als zuständige Stellen für Verfahren der Berufsanerkennung im IMI-System registriert.

2.6

Das IMI-System sieht neben den zuständigen Stellen auch die Einsetzung eines Nationalen Koordinators ("National IMI Coordinator – NIMIC") in jedem Mitgliedstaat vor. Er dient unter anderem als Hauptansprechpartner für die Kommission und die anderen Mitgliedstaaten in allen technischen Fragen. Die Rolle des Nationalen Koordinators hat die Bundesregierung der Bundesstelle für Informationstechnologie (BIT) als Teil des Bundesverwaltungsamtes übertragen.

Ob und in welchem Umfang auf der Ebene zwischen dem Nationalen Koordinator und den zuständigen Stellen sog. nachgeordnete Koordinatoren (Delegated IMI Coordinators – DIMIC) benannt werden, bleibt den Mitgliedstaaten grundsätzlich selbst überlassen. Aufgrund der föderalen Struktur Deutschlands und der folglich großen Anzahl an unterschiedlichen Behörden in den Ländern, die für die Umsetzung der oben genannten Richtlinien zuständig sind, haben sich Bund und Länder darauf verständigt, zumindest jeweils einen Koordinator auf Landesebene einzurichten. Dieser soll Organisations- und IT-Administrationsaufgaben innerhalb des Landes wahrnehmen, für die Registrierung und Authentisierung der zuständigen Stellen verantwortlich sein und als Ansprechpartner für den Nationalen Koordinator dienen. In Berlin wurde die Aufgabe des Landeskoordinators dem IT-Dienstleistungszentrum (ITDZ) übertragen.

Datenschutz und Amtshilfe

Die Nutzung des IMI-Systems bedingt den Umgang mit einer großen Menge personenbezogener Daten insbesondere der betroffenen Dienstleistungserbringer (z. B. Name, Telefonnummer, E-Mail-Adresse, Geburtsdatum, Nationalität, Daten in Bezug auf die berufliche Qualifikation, Informationen über die Rechtmäßigkeit der Niederlassung sowie Angaben über berufsbezogene disziplinarische oder strafrechtliche Sanktionen). Mit der Einführung des IMI-Systems werden aber keine hierauf bezogenen neuen Datenverarbeitungsbefugnisse für die beteiligten Instanzen geschaffen. Diese ergeben sich beispielsweise auch nicht aus den in der Berufsanerkennungsrichtlinie und der Dienstleistungsrichtlinie enthaltenen Vorschriften zur Verwaltungszusammenarbeit und zum Austausch von Informationen im Wege der Amtshilfe[67]. Amtshilfevorschriften als solche begründen keine eigenständige Befugnis für die personenbezogene Informationshilfe und können Eingriffe in die Grundrechtspositionen der Betroffenen nicht rechtfertigen.

[67] vgl. 8, 50, 56 der Richtlinie 2005/36/EG und Art. 28, 34 der Richtlinie 2006/123/EG

Für die Kommunikation über IMI gilt damit nichts anderes als für den bisher stattfindenden Informationsaustausch zwischen den Behörden der Mitgliedstaaten auch: Zum Schutz des Rechts auf informationelle Selbstbestimmung der Betroffenen müssen die Vorgaben der allgemeinen und bereichsspezifischen Datenschutzgesetze[68] beachtet werden. Danach ist die Verwendung personenbezogener Daten durch öffentliche Stellen der Länder im Grundsatz zulässig, soweit dies zur Erfüllung der ihnen gesetzlich zugewiesenen und in ihrer Zuständigkeit liegenden Aufgaben erforderlich ist. In diesem Rahmen kann das IMI-System sinnvoll zur europaweiten Kommunikation zwischen den zuständigen Stellen eingesetzt werden. Es kann sich sogar datenschutzfreundlich auswirken, wenn es die bisherige Praxis eines Ad-hoc-Austauschs personenbezogener Daten zwischen den Behörden per E-Mail, Fax oder Brief durch ein strukturiertes und transparentes Verfahren ersetzt und so zur Datensparsamkeit beiträgt.

Bei der Datenverarbeitung durch die zuständigen Stellen sind der Grundsatz der Datenerhebung bei den Betroffenen (Direkterhebung) und die besonderen Verarbeitungsvoraussetzungen beim Umgang mit sensitiven Daten zu beachten. Die Rechte der betroffenen Personen (Auskunft, Berichtigung, Löschung, Sperrung) sind zu gewährleisten. Zudem sind geeignete technische und organisatorische Maßnahmen vorzusehen, die eine Veränderung, einen Verlust oder eine unberechtigte Verarbeitung der Daten oder einen unberechtigten Zugang zu ihnen verhindern.

Auf diese Punkte hat auch die Art. 29-Datenschutzgruppe hingewiesen, die auf Ersuchen der Generaldirektion Binnenmarkt der Europäischen Kommission eine umfangreiche Stellungnahme zum Binnenmarkt-Informationssystem abgegeben hat[69]. Darin wird die generelle datenschutzrechtliche Zulässigkeit des Systems nicht in Frage gestellt, aber betont, dass aufgrund der Komplexität des Verfahrens die Erfordernisse des Datenschutzes hinsichtlich der Qualität der Daten, der Erforderlichkeit der Verarbeitung und der Zweckbindung strikt eingehalten werden müssen. Dies sollte in jeder Phase der Entwicklung vom IMI und von allen Instanzen im System berücksichtigt werden, etwa bei der Formulierung von standardisierten Anfragen oder aber bei der Auswahl der zuständigen Behörden.

---

[68] Derzeit werden zur Umsetzung der Berufsanerkennungsrichtlinie neue grenzüberschreitende Informationspflichten geschaffen. Vgl. auf Bundesebene das Gesetz zur Umsetzung der Richtlinie 2005/36/EG des Europäischen Parlaments und des Rates über die Anerkennung von Berufsqualifikationen der Heilberufe v. 2. Dezember 2007, BGBl. I, 2666, und auf Landesebene das Gesetz zur Umsetzung der Richtlinie 2005/36/EG im Recht der Gesundheitsberufe v. 15. Dezember 2007, GVBl., 617.

[69] Art. 29-Datenschutzgruppe: Stellungnahme 7/2007 zu Fragen des Datenschutzes im Zusammenhang mit dem Binnenmarkt-Informationssystem v. 21. September 2007

2.6

Datenverarbeitung durch die Europäische Kommission

Aus datenschutzrechtlicher Sicht nach wie vor kritisch zu bewerten ist die Rolle der Europäischen Kommission im Rahmen des IMI-System. Die Kommission stellt die Verfügbarkeit und Wartung der IT-Infrastruktur für IMI sicher. Sämtliche über das System ausgetauschten Informationen werden unter ihrer Verantwortung zentral auf einem Server im Rechenzentrum in Luxemburg gespeichert.

Ursprünglich war vorgesehen, dass die Kommission die Datenspeicherung im Auftrag der Mitgliedstaaten vornimmt. Diese Konstruktion wird aus nachvollziehbaren Gründen nicht weiterverfolgt. Problematisch ist es jedoch, dass nicht die Mitgliedstaaten selbst die für die Datenverarbeitung verantwortlichen Stellen i. S. d. Datenschutzrechts darstellen, sondern die jeweils zuständigen Stellen in den Mitgliedstaaten. Diese wären als Auftraggeber für die Einhaltung der datenschutzrechtlichen Vorschriften durch die Kommission verantwortlich. Die Kommission dürfte personenbezogene Daten nur nach ihren Weisungen verarbeiten und müsste sich entsprechenden Kontrollen unterwerfen.

Die Kommission selbst geht nun vielmehr von einer gemeinsam mit den zuständigen Behörden in den Mitgliedstaaten ausgeübten datenschutzrechtlichen Verantwortlichkeit aus – zumindest für die Phasen der Speicherung und Löschung personenbezogener Daten der Dienstleistungserbringer im IMI-System. Diese Konstruktion einer „Joint Controllership“ stützt sich auf eine funktionale Auslegung des Begriffs des „für die Verarbeitung Verantwortlichen“ im europäischen Datenschutzrecht[70]. Damit wird erreicht, dass in den Fällen, in denen für einzelne Abschnitte eines einheitlichen Datenverarbeitungskomplexes unterschiedliche Stellen über die Zwecke und Mittel der Verarbeitung zu entscheiden haben, diese nebeneinander als Verantwortliche der Verarbeitung angesehen werden können.

Diese Überlegungen werden von der Art. 29-Datenschutzgruppe mitgetragen. Ähnlich wurde bereits im Hinblick auf die Datenverarbeitung durch SWIFT argumentiert[71]. Die Datenschutzgruppe betont in ihrer Stellungnahme aber zugleich, dass eine gemeinsame Verantwortung für die Datenverarbeitung klare Festlegungen der Datenschutzrechte und -pflichten der Instanzen hinsichtlich der einzelnen Verarbeitungsschritte voraussetze, was bisher nicht in ausreichendem Maße erfolgt sei. Daher sei eine spezifische Kommissionsentscheidung zu IMI erforderlich. Nur

[70] vgl. Art. 2 d) Satz 1 EG-Datenschutzrichtlinie

[71] Stellungnahme 10/2006 zur Verarbeitung von personenbezogenen Daten durch die Society für Worldwide Interbank Financial Telecommunication (SWIFT) v. 22. November 2006, vgl. „Dokumente zu Datenschutz und Informationsfreiheit 2006“, S. 55. Dazu auch JB 2006, 8.1.

so könne jede einzelne Datenverarbeitungsmaßnahme einer konkreten Rechtsgrundlage zugewiesen werden.

Eine Datenverarbeitungsbefugnis für die Kommission ist bislang gerade nicht gegeben. Die sich aus Art. 5 der insoweit einschlägigen Verordnung 45/2001 ergebenden Voraussetzungen für die Rechtmäßigkeit der Datenverarbeitung durch Organe und Einrichtungen der Gemeinschaft sind nicht erfüllt. Der Kommission ist weder eine Aufgabe durch Rechtsakt übertragen worden, für deren Wahrnehmung die hier fragliche Datenspeicherung erforderlich wäre, noch besteht hierzu eine rechtliche Verpflichtung.

Entscheidung der Kommission

Um der Forderung der Art. 29-Datenschutzgruppe nachzukommen, hat die Kommission am 12. Dezember 2007 eine Entscheidung nach Art. 249 EG-Vertrag über den Schutz personenbezogener Daten bei der Umsetzung des Binnenmarktinformationssystems (IMI) angenommen[72].

Darin werden zwar die datenschutzrelevanten Funktionen und Zuständigkeiten der IMI-Instanzen sowie deren Zugangsrechte zu personenbezogenen Daten definiert. Es fehlt allerdings an einer konkreten und praktikablen Zuordnung der Datenschutzpflichten (etwa zur Benachrichtigung, zur Auskunftserteilung oder zur Datensicherung) zu den verschiedenen für die Verarbeitung Verantwortlichen[73]. Insoweit bleibt es bei einer generellen Aussage.

Im Hinblick auf die Kommission wird bestimmt, dass sich diese an einem Informationsausstausch zwischen den Mitgliedstaaten nur in den Fällen beteiligen kann, die im hier relevanten Gemeinschaftsrecht, d. h. in der Berufsanerkennungs- oder der Dienstleistungsrichtlinie, ausdrücklich vorgesehen sind. Ansonsten besteht für die lokalen Datenverwaltungen der Kommission kein Zugang zu personenbezogenen Daten der betroffenen Dienstleistungserbringer. Sie können diese Daten löschen, aber nicht einsehen.

Die personenbezogenen Daten der Betroffenen, die zwischen zuständigen Stellen ausgetauscht werden, sollen der Entscheidung zufolge regelmäßig sechs Mona-

[72] ABl. L 13/18 v. 16. Januar 2008

[73] vgl. Stellungnahme der Europäischen Datenschutzbeauftragten zur IMI-Entscheidung der Kommission v. 22. Februar 2008

te nach formellem Abschluss eines Informationsaustauschs auf dem Server der Kommission gespeichert bleiben. Dieser Zeitraum wird als notwendig erachtet, um Nachfragen zwischen den zuständigen Behörden zu ermöglichen und auf Situationen vorbereitet zu sein, die entstehen, wenn betroffene Personen gegen eine im Anschluss an den Informationsaustausch getroffene, negative Verwaltungsentscheidung Einspruch erheben möchten. Diese Argumentation ist nicht nachzuvollziehen, da der dem jeweiligen Informationsaustausch zugrunde liegende Amtshilfevorgang nicht mit dem eigentlichen Verwaltungsvorgang der zuständigen nationalen Behörde gleichzusetzen ist. Nur für Letztere bestünde daher die Berechtigung einer längerfristigen Speicherung außerhalb des Systems.

Wie die Löschpflichten und die Zugriffsbeschränkungen technisch und organisatorisch umgesetzt und deren Einhaltung sichergestellt werden soll, wird in der Entscheidung nicht ausgeführt. Die Datenschutzbeauftragten von Bund und Ländern haben daher die Durchführung einer Risikoanalyse und die Erstellung eines entsprechenden Datenschutz- und Sicherheitskonzepts gefordert. Die Kommission hat diese Dokumente nunmehr zum Teil vorgelegt. Auf deren Grundlage kann eine Vorabkontrolle des Verfahrens hinsichtlich möglicher Gefahren für das Recht auf informationelle Selbstbestimmung nach § 5 Abs. 3 Berliner Datenschutzgesetz (BlnDSG) durch die behördlichen Datenschutzbeauftragten der in Berlin zuständigen Stellen erfolgen.

Für europaweite Verwaltungsvorgänge setzt die Europäische Kommission verstärkt auf interoperable E-Government-Dienste. Ihr Einsatz birgt aber die Gefahr, dass große personenbezogene Datenbestände anwachsen, von ihrem eigentlichen Verwendungszusammenhang getrennt und über das Maß des Erforderlichen hinaus zentralisiert werden. Es besteht das Risiko, dass neue Kommunikationsinfrastrukturen ohne ausreichende Berücksichtigung von Datenschutzaspekten zu Standards ausgebaut werden, die von den nationalen Behörden faktisch genutzt werden müssen. Wir werden uns bei der Einführung des IMI-Systems dafür einsetzen, dass die Behörden im Land Berlin die Umsetzung dieses Systems möglichst datenschutzfreundlich gestalten.

3 Öffentliche Sicherheit

3.1 Polizei

3.1.1 Änderung des Gesetzes über das Bundeskriminalamt (BKA)

Mit dem Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus will die Bundesregierung die Möglichkeiten bei der Bekämpfung des internationalen Terrorismus durch das BKA verbessern. Dazu soll es in bestimmten Fallgruppen die – neue – Aufgabe und entsprechende Befugnisse erhalten.

Der Bund hat seit der Föderalismusreform 2006 die ausschließliche Gesetzgebungskompetenz für die Abwehr von Gefahren des internationalen Terrorismus durch das BKA in den Fällen, in denen eine länderübergreifende Gefahr vorliegt, die Zuständigkeit einer Landesbehörde nicht erkennbar ist oder die oberste Landesbehörde um eine Übernahme ersucht[74]. Der Entwurf dient der Umsetzung dieser neuen Gesetzgebungskompetenz des Bundes. Das BKA wird damit in diesem Bereich nicht nur für die Strafverfolgung, sondern auch für die Gefahrenabwehr zuständig.

In Abweichung zu einem ersten Referentenentwurf sind in der überarbeiteten Fassung vom 6. November 2007 die obersten Landesbehörden unverzüglich zu benachrichtigen, wenn das BKA die Aufgabe übernimmt. Dabei ist ein gegenseitiges Benehmen herzustellen.

Wichtigster Punkt des Gesetzentwurfs ist die Einfügung der §§ 20 a bis 20 y in das BKA-Gesetz, die die Möglichkeiten des BKA zur Abwehr von Gefahren des internationalen Terrorismus regeln sollen.

Hiervon betroffen wird ein weitgefasster Personenkreis sein, der verdächtigt wird, terroristische Anschläge zu planen oder vorzubereiten. Zwar soll nur der internationale Terrorismus berücksichtigt werden, jedoch wird der Begriff sehr weit ausgelegt. Ähnlich wie bei der Antiterrordatei ist auch hier die unscharfe Begrifflichkeit der „Kontakt- und Begleitperson“ zu kritisieren. Die Befugnisse sind sehr weitgehend und teils ausgesprochen eingriffsintensiv. Der Entwurf regelt die – im Einzelnen noch umstrittene – Online-Durchsuchung[75] und sehr weitge-

[74] Artikel 73 Abs. 1 Nr. 9 a Grundgesetz (GG)

[75] vgl. dazu 2.1

hende Formen der Wohnraumüberwachung (Großer Lauschangriff) und der präventiven Telekommunikationsüberwachung.

Die Löschfristen sind nur für die Fälle klar geregelt, dass die Maßnahmen abgeschlossen sind oder keinen Erfolg bringen konnten. Die Dauer der Maßnahmen ist zwar je nach Anordnung auf in der Regel einen Monat begrenzt, kann aber beliebig oft verlängert werden. Der Schutz von Personen, die ein Zeugnisverweigerungsrecht haben, soll erheblich eingeschränkt werden. Die Regelungen technischer Überwachung sind stets technikoffen und damit teils sehr pauschal gehalten, sodass ihre Verhältnismäßigkeit zu hinterfragen ist. Dies gilt vor allem für Fälle, in denen verschiedene Maßnahmen kombiniert zum Einsatz kommen.

Die Auswirkungen des BKA-Gesetzes auf die Zusammenarbeit von BKA und Landespolizeibehörden sind derzeit ebenso wenig absehbar wie die Veränderung der damit verbundenen Datenverarbeitungen. In der Diskussion über den Gesetzesentwurf wird bislang übersehen, dass die nach 1945 geschaffene informationelle Gewaltenteilung zwischen dem Bundeskriminalamt und den Polizeien der Länder auch dem Schutz der Bürgerinnen und Bürger dient. Ob neue Parallelzuständigkeiten der Kriminalämter des Bundes und der Länder und die Abkoppelung des Bundeskriminalamtes von der Sachleitungsbefugnis der Generalbundesanwälte die Terrorismusbekämpfung verbessern können, wird von Praktikern bezweifelt. Auch ist nicht nachvollziehbar, welche Aufgabe die Verfassungsschutzämter noch erfüllen sollen, wenn das Bundeskriminalamt derart weitreichende nachrichtendienstliche Befugnisse erhalten würde. Aus gutem Grund sind den Polizeien des Bundes und der Länder nach 1945 andere Aufgaben und Befugnisse zugewiesen worden als den Geheimdiensten.

Insgesamt würde eine Verabschiedung des BKA-Gesetzes in dieser Form die Sicherheitsarchitektur in Deutschland grundlegend verändern. Es gibt weder einen Bedarf noch – selbst nach der Föderalismusreform – eine Verfassungspflicht, das Bundeskriminalamt mit derart weitreichenden nachrichtendienstlichen Befugnissen auszustatten. Es darf keine neue zentrale Geheimpolizei geben.

3.1.2 Änderung des Allgemeinen Sicherheits- und Ordnungsgesetzes und des Berliner Datenschutzgesetzes

Die Regierungsparteien hatten sich in ihrer Koalitionsvereinbarung unter anderem darauf verständigt, dass die Polizei in den öffentlich zugänglichen Räumen des Personennahverkehrs (insbesondere auf U-Bahnhöfen) Videoaufzeichnungen fertigen oder von anderen angefertigte Videoauf-

zeichnungen verarbeiten darf. Weiterhin sollten die Vorschriften der Rasterfahndung entsprechend der Rechtsprechung des Bundesverfassungsgerichtes eingeschränkt und die Befugnisse der Polizei, suizidgefährdete oder vermisste Personen über die Ermittlung der Standortdaten eines Mobilfunktelefones orten zu können, auf eine gesetzliche Grundlage gestellt werden.

Nachdem die BVG die mit uns abgestimmte Evaluation der Videoüberwachung auf drei U-Bahnlinien durch einen anerkannten Wissenschaftler[76] abgebrochen hatte, ohne aussagekräftige Ergebnisse abzuwarten, beschloss das Abgeordnetenhaus im November 2007 das Gesetz zur Änderung des Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG) und des Berliner Datenschutzgesetzes. Dabei wurden unsere Vorschläge berücksichtigt, die Regelungen zur Videoüberwachung zur Eigensicherung und bei Großveranstaltungen sowie zur Übermittlung von Daten an die im Antiterrordateigesetz genannten Stellen zu präzisieren und den Kreis der Behörden zu verkleinern, die Errichtungsanordnungen zu fertigen haben. Ferner ist unsere Empfehlung bei der neu geschaffenen Regelung zur Datenerhebung in öffentlichen Verkehrseinrichtungen umgesetzt worden, dass diese erst stattfinden darf, wenn sich nach einer nachvollziehbar dokumentierten Lagebeurteilung ein Anlass für die Datenerhebung ergibt. Für die Videoaufzeichnung im öffentlichen Personennahverkehr ist die BVG nach der Novelle zum Berliner Datenschutzgesetz verpflichtet, ein Sicherheitskonzept mit der Polizei abzustimmen. Darüber hinaus ist bei der Umsetzung dieser neuen Regelung sicherzustellen, dass das im Auftrag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit entwickelte Schutzprofil zur datenschutzgerechten Videoüberwachung beachtet wird, das das Bundesamt für die Sicherheit in der Informationstechnik zertifiziert hat[77].

Mittlerweile ist offenbar auch der Senat der Auffassung, dass letztlich nur der vermehrte Einsatz von Zug- und Buspersonal das Unsicherheitsgefühl vieler Fahrgäste im öffentlichen Personennahverkehr effektiv verringern kann[78].

Unsere Vorschläge zur Schaffung einer Befugnis zur Herstellung und Nutzung von Videoaufzeichnungen im Personennahverkehr, die sich an der auf Berliner

---

[76] JB 2005, 3.1

[77] vgl. Beschlussempfehlung mit Bericht des Innenausschusses des Deutschen Bundestages zum Entwurf eines Dritten Gesetzes zur Änderung des Bundespolizeigesetzes (betr. Videoüberwachung bei der Deutschen Bahn AG), BT-Drs. 16/7148, S. 6

[78] vgl. Mitteilung – zur Kenntnisnahme – Wirkungsvolle Videoüberwachung auf U-Bahnhöfen, Schlussbericht Abgh.-Drs. 16/1057, S. 20 f.

3.1

Fernbahnhöfen (wie auch bundesweit bei der Deutschen Bahn AG) geltenden Regelung orientierten, zur Anordnung der medizinischen und molekulargenetischen Untersuchung und zur Standortermittlung bei Telekommunikationsendgeräten sind allerdings ebenso wenig aufgegriffen worden wie der Vorschlag zur Schaffung einer normenklaren Befugnis zu Akkreditierungsverfahren bei Großereignissen (wie beispielsweise Fußball-Weltmeisterschaft, Staatsbesuche) oder Zuverlässigkeitsüberprüfungen von Personen, die als Lieferanten oder Dienstleister Zutritt bei der Deutschen Bundesbank benötigen[79].

Im Übrigen hat der Senat leider bislang auch unsere Anregung nicht aufgegriffen, die Pflicht zum Schutz des Kernbereichs privater Lebensgestaltung auch auf den Einsatz verdeckter Ermittler zu erstrecken[80].

Bei der Einführung der flächendeckenden Videoaufzeichnung auf U-Bahnhöfen ist die Chance vertan worden, den objektiven Nutzen einer solchen Maßnahme für die Sicherheit im öffentlichen Personennahverkehr von unabhängiger Seite überprüfen zu lassen.

3.1.3 Wie im Fernsehen ...

Ein Hausmeister hatte wegen eines Wasserschadens die Wohnung des Mieters geöffnet, dort Drogen gefunden und die Polizei gerufen. Diese durchsuchte die Wohnung ohne richterlichen Beschluss und erschlich sich eine DNA-Probe bei einer Verkehrskontrolle. Dabei wurde das bei einem Alkoholtest verwendete Mundstück einbehalten und dem Betroffenen auf seinen Rückgabewunsch hin ein unbenutztes Austauschstück übergeben. Danach verschwanden Beweismittel und einem der Verdächtigen wurde bei seiner Befragung zu Unrecht erklärt, dass er keinen Anwalt benötigen würde.

Der Beschuldigte beschritt den Rechtsweg. Der Bundesgerichtshof hat in seiner Entscheidung[81] eine nachhaltige Missachtung der Verfahrensvorkehrungen durch die Berliner Staatsanwaltschaft und Polizei gerügt. Er hat weiterhin festgestellt, dass in diesem Fall „schon die Annahme außerordentlich nahe liegt, dass die Polizeibeamten den Richtervorbehalt bewusst ignoriert und die Inanspruchnahme der Eilkompetenz des Staatsanwaltes provoziert haben“. Der Entscheidung lässt sich weiterhin der Vorwurf entnehmen, dass der Staatsanwalt weder die Einholung

[79] vgl. dazu JB 2006, 2.2

[80] JB 2006, 3.1.1

[81] Urteil v. 18. April 2007, NJW 2007, 2269

einer fernmündlichen Genehmigung des Ermittlungsrichters erwogen noch die Voraussetzungen der von ihm in Anspruch genommenen Eilkompetenz dokumentiert habe.

Der Polizeipräsident in Berlin hat uns auf Nachfrage mitgeteilt, dass der Sachverhalt, der dieser Entscheidung zugrunde liegt, in der Zwischenzeit geprüft und ausgewertet wurde. Sowohl die Staatsanwaltschaft als auch die Polizei sind zu dem Ergebnis gekommen, dass es sich hierbei um einen Einzelfall handele und es insofern keiner organisatorischen Veränderungen bedürfe. Der Vorgang wurde allerdings zum Anlass genommen, nochmals alle Polizeidienststellen auf den Ausnahmecharakter der Gefahr im Verzug und die Notwendigkeit einer genauen Dokumentation der Umstände, aus der sie sich im Einzelfall ergibt, hinzuweisen.

Entsprechendes geschah auch bei der Staatsanwaltschaft. Soll ein Staatsanwalt oder eine Staatsanwältin ein Ermittlungsverfahren auch i. S. d. Grundrechtsschutzes der Verdächtigen justiziell begleiten, muss hierfür ein gewisser Entscheidungsspielraum gegeben sein. Solche Entscheidungsspielräume eröffnen naturgemäß die Möglichkeit für menschliches Versagen im Einzelfall. Wir haben die Stellungnahmen deshalb akzeptiert.

Wohnungsdurchsuchungen stehen regelmäßig unter Richtervorbehalt. Gefahr im Verzug ist die Ausnahme von der Regel. Die Gründe für den ausnahmsweisen Verzicht auf die Herbeiführung einer richterlichen Entscheidung sind genau zu dokumentieren.

3.1.4 Einkauf mit Hindernissen – Anschauungsunterricht in Sachen „Rechtsstaat“

Zwei kolumbianische Politiker besuchten auf Einladung der Konrad-Adenauer-Stiftung Berlin, um hier Erfahrungen über die Funktionsweise eines Rechtsstaats zu sammeln. Nachdem sie an der Kasse eines großen Elektronikmarktes festgehalten worden waren, berichteten Berliner Tageszeitungen darüber, dass sie sich im Rahmen einer polizeilichen Durchsuchungsmaßnahme vor Polizeibeamten entkleiden mussten. Den Zeitungsberichten zufolge wollten die beiden Waren mit einem 500-Euro-Schein bezahlen. Das Geldlesegerät der Verkäuferin habe diesen Schein als Falschgeld angezeigt. Erst später stellte sich heraus, dass die Anzeige des Lesegeräts auf einem technischen Defekt beruhte. Der daraufhin verständigte Sicherheitsdienst habe den Betroffenen die Handys abgenommen und sie in eine Kammer gesperrt. Später wurden sie von Polizeibe-

amten in Zivil im Vernehmungsraum durchsucht und mussten sich dabei vor einer laufenden Kamera des Elektromarktes bis auf die Unterhosen entkleiden.

Der Geschäftsführer des Marktes hat uns bei einer sofort durchgeführten Ortsbesichtigung erklärt, dass die Zeitungsberichte das Geschehen im Wesentlichen korrekt wiedergegeben haben. Bei dem Bezahlvorgang habe das elektronische Lesegerät einer Verkäuferin den Wert eines Geldscheines mit 200 Euro angegeben, obwohl der Betroffene mit einem 500-Euro-Schein bezahlt habe. Daraufhin habe die Verkäuferin den Sicherheitsdienst alarmiert. Dieser habe bei den beiden Betroffenen ein ganzes Bündel von 500-Euro-Scheinen festgestellt. Deshalb sei die Polizei gerufen worden. Die Betroffenen seien in einen „Vernehmungsraum" des Marktes gebracht worden. Dort seien sie durchsucht worden und hätten sich entkleiden müssen. Die Videoaufzeichnungen erfolgten nach Darstellung des Marktleiters, weil der besagte Vernehmungsraum aus Sicherheitsgründen generell videoüberwacht werde. Die Bilder der Videoüberwachung (der Verkaufsräume und des Vernehmungsraums) würden in eine Sicherheitszentrale übertragen und dort von etwa 30 Monitoren aus live von Mitarbeiterinnen und Mitarbeitern der Sicherheitsfirma überwacht.

Der Polizeipräsident hat uns erklärt, dass die Betroffenen von zwei Polizeibeamten in Zivil wegen des Verdachts des Inverkehrbringens von Falschgeld vorläufig festgenommen worden seien. Sie seien dann in einem Nebenraum des Marktes „bis auf die Unterhose" durchsucht worden, um ggf. weitere Beweismittel (falsche Zahlungsmittel) aufzufinden. Diese Darlegung wurde später dahingehend ergänzt, dass die Betroffenen die Unterhosen herunterziehen, aber nicht ausziehen mussten.

Die Rechtsgrundlage für die Maßnahme sei § 102 Strafprozessordnung (StPO), wonach die Durchsuchung von Verdächtigen bis auf die Körperoberfläche zum Zweck des Auffindens von Beweismitteln zulässig sei. Die von dem Elektromarkt der Polizei zur Verfügung gestellte Kopie der Videoaufzeichnung hat der Polizei vorgelegen. Sie ist inzwischen gelöscht worden. Bei der Berliner Polizei ist lediglich ein Bericht mit den Personalien der beiden Betroffenen im polizeilichen Informationssystem POLIKS gespeichert, der Auskunft über das polizeiliche Tätigwerden gibt. Für die eingesetzten Polizeimitarbeiter hat nach Ansicht des Polizeipräsidenten keine Veranlassung bestanden, den Raum zu inspizieren oder gar nach einer Videokamera Ausschau zu halten.

Bei der Ermittlung des Sachverhaltes haben die beiden Zivilbeamten den Verhältnismäßigkeitsgrundsatz missachtet und insoweit gegen § 102 StPO verstoßen, als sie ohne sachliche Notwendigkeit den Intimbereich der beiden Betroffenen

durchsuchten. Diese Durchsuchung diente nach § 102 StPO ausschließlich dem Auffinden von Beweismitteln. Die Vorschrift sieht u. a. vor, dass eine Person und die ihr gehörenden Sachen durchsucht werden können, wenn zu vermuten ist, dass die Durchsuchung zur Aufwendung von Beweismitteln führen kann.

Bei der körperlichen Durchsuchung nach § 102 StPO muss jedoch der Verhältnismäßigkeitsgrundsatz besonders strikt beachtet werden. Insbesondere scheidet die Durchsuchung aus, wenn andere, weniger einschneidende Maßnahmen verfügbar sind oder die Maßnahme angesichts der näheren Umstände als unverhältnismäßig erscheint.

Im konkreten Fall war die Maßnahme offensichtlich unverhältnismäßig. Die handelnden Polizeibeamten hätten besonders sorgfältig prüfen müssen, ob eine Durchsuchung „bis auf die Unterhose“ angesichts der näheren Umstände des Einzelfalls angemessen war. Bei der vorzunehmenden Abwägung hätte sich herausgestellt, dass die Durchsuchung nicht geboten war, um Beweismittel als solche aufzufinden. Zuvor war bereits ein ganzes Bündel, zumindest aber mehrere 500-Euro-Scheine gesichert worden. Die Beamten hätten demnach zunächst die Echtheit dieser Scheine überprüfen können, bevor sie mit einer grundrechtsintensiven Durchsuchung zusätzliche Beweismittel erheben.

Es liegt in diesem Zusammenhang auch ein Verstoß gegen den Verhältnismäßigkeitsgrundsatz vor, weil die Beamten die laufende Videoüberwachung nicht unterbunden haben. Die Videoübertragung und -aufzeichnung erhöht die Intensität des Grundrechtseingriffs. Die betroffene Person, die aufgrund eines Tatverdachts von Sicherheitspersonal in den Vernehmungsraum verbracht wird, befindet sich ohnehin in einer schwierigen Situation. Wie der Vorfall zeigt, wird sie von der verantwortlichen Stelle, nicht immer zu Recht, eines Vergehens bezichtigt und sieht sich regelmäßig mehreren Personen des Sicherheitsdienstes und der Polizei gegenüber. Das Vorhandensein einer Videokamera erhöht den ohnehin bestehenden psychischen Druck, der auf der betroffenen Person lastet.

Der Umstand einer Videoüberwachung im Vernehmungsraum war auch nicht zu übersehen. Der Vernehmungsraum bildet eine lange Flucht und ist äußerst karg ausgestattet. Die Videokamera war am Ende der Flucht auf der schmalen Querwand oben rechts angebracht, sodass man beim Öffnen der Tür zum Vernehmungsraum geradewegs auf sie blickte. Die Kamera war auch nicht so klein, dass man sie hätte suchen müssen. Sie fiel aufgrund der räumlichen Gegebenheiten förmlich ins Auge. Diesen räumlichen Umständen entsprechend geht auch die Geschäftsleitung des Marktes davon aus, dass die Beamten die Betroffenen in Kenntnis der Videoüberwachung durchsuchten.

3.1

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat den Vorgang förmlich beanstandet und empfohlen, bei der Durchsuchung von verdächtigen Personen vor einer Durchsuchung des Intimbereichs die Angemessenheit der Maßnahme besonders sorgfältig zu prüfen. Angesichts der hohen Eingriffsintensität der Durchsuchung des Intimbereichs sollte sie zugunsten milderer Maßnahmen zurückgestellt werden, wenn Zweifel an einer Täterschaft bestehen und bereits hinreichende Beweismittel sichergestellt sind, die eine nähere Sachverhaltsaufklärung gewährleisten. Ferner haben wir für den Fall, dass eine verdächtige Person in Vernehmungsräumen eines Warenhauses durchsucht werden soll und die Polizeibeamten vor Ort auch in Anbetracht der hohen Eingriffsintensität eine Durchsuchung des Intimbereichs als notwendig ansehen, empfohlen, dass sich die handelnden Beamten – ggf. durch Nachfragen bei der verantwortlichen Stelle – vergewissern, dass eine Videoüberwachung der betroffenen verdächtigen Person während der Durchsuchung nicht stattfindet.

Der Senator für Inneres hat in seiner Stellungnahme zur Beanstandung das Recht des Datenschutzbeauftragten prinzipiell in Zweifel gezogen, der Polizei bestimmte Fragen zur Rechtmäßigkeit polizeilichen Handelns im Rahmen der Strafprozessordnung zu stellen, die für die abschließende datenschutzrechtliche Bewertung des Vorgangs wesentlich waren. Der Polizeipräsident hat diese Fragen inzwischen beantwortet. Außerdem hat der Innensenator die Frage aufgeworfen, wer die Daten und die Ehre der beteiligten Polizeibediensteten vor dem Datenschutzbeauftragten schützt, nachdem dieser aufgrund der Prüfung vor Ort Zweifel an der Darlegung der Polizeibediensteten geäußert hatte, ihnen sei die Videokamera in dem Vernehmungsraum nicht aufgefallen.

Diese Reaktion des Innensenators ist weder verständlich noch akzeptabel.

Alle öffentlichen Stellen Berlins sind gesetzlich verpflichtet, den Berliner Beauftragten für Datenschutz und Informationsfreiheit und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere Auskunft zu ihren Fragen zu geben, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen[82]. Ob dieser Zusammenhang besteht, hat allein der Berliner Beauftragte für Datenschutz und Informationsfreiheit zu entscheiden, nicht aber die befragte öffentliche Stelle. Anderenfalls könnte sich jede Behörde ihrer Unterstützungspflicht schon dadurch entziehen, dass sie die Berechtigung der Fragen des Datenschutzbeauftragten bestreitet. Damit würde eine unabhängige Datenschutzkontrolle, wie sie das Berliner Datenschutzgesetz entsprechend der Europäischen Datenschutzrichtlinie vorschreibt, vereitelt. Auch hat der Datenschutzbeauf-

[82] § 28 Abs. 1 Berliner Datenschutzgesetz (BlnDSG)

tragte das Recht, die Aussagen von Bediensteten der verantwortlichen Stellen auf ihre Plausibilität hin zu überprüfen.

Der Elektronikmarkt hat entsprechend unserer Anforderung die Videoüberwachung in dem Vernehmungsraum beendet.

Wir haben der Konrad-Adenauer-Stiftung das Ergebnis unserer Überprüfung mitgeteilt und sie gebeten, die betroffenen kolumbianischen Politiker darüber zu informieren.

Sowohl beim Einsatz von Videotechnik als auch bei körperlichen Durchsuchungen – anders als in dem hier geschilderten Fall – ist der Grundsatz der Verhältnismäßigkeit strikt zu beachten. Selbst wenn ein Mensch die Durchsuchung seines Intimbereichs hinnehmen muss, darf dies in aller Regel nicht mit Videokameras beobachtet oder aufgezeichnet werden. In einer derart entwürdigenden Weise – wie in diesem Fall – darf in einem Rechtsstaat niemand behandelt werden, auch dann nicht, wenn er tatsächlich eine Straftat begangen hat.

3.1.5 Verfahrenseinstellungen nach § 170 Abs. 2 StPO und die polizeiliche Praxis

Ein Bürger teilte einer Polizeidienststelle seine Beobachtungen zu Rauschgiftdelikten mit. Nach einem Blick in das polizeiliche Informationssystem berichtete ihm der Polizeibeamte von zwei länger zurückliegenden Ermittlungsverfahren gegen seine Person. Weil die Vorwürfe seinerzeit haltlos waren und die Staatsanwaltschaft die Ermittlungsverfahren eingestellt hatte, bat der Petent uns, den Vorgang zu überprüfen.

Zunächst hatte uns der Polizeipräsident in Berlin mitgeteilt, dass der Ausgang des einen Strafverfahrens nicht bekannt und das andere nach § 170 Abs. 2 StPO eingestellt worden sei. Darüber hinaus wurde ganz allgemein erläutert, dass die weitere Speicherung der Daten zur vorbeugenden Straftatenbekämpfung so lange erforderlich sei, wie Tatsachen die Annahme rechtfertigten, dass die Betroffenen erneut kriminalpolizeilich in Erscheinung treten könnten. Bei der Prognose sei vor allem zu berücksichtigen, ob die Betroffenen bereits Straftaten begangen haben und ob nach kriminalistischer Erfahrung zu befürchten sei, sie werden weitere Straftaten begehen.

Die Staatsanwaltschaft stellt ein Verfahren nach § 170 Abs. 2 StPO jedoch nur dann ein, wenn die Ermittlungen keinen genügenden Anlass zur Erhebung der

öffentlichen Anklage bieten. Da in keiner Weise die Erforderlichkeit der weiteren Speicherungen in Bezug auf den Betroffenen erläutert wurde, haben wir die Polizei um eine erneute Stellungnahme gebeten. Auch diese enthielt nur allgemeine, formelhafte Erklärungen. Erst nach einer nochmaligen Bitte um Konkretisierung der Erforderlichkeit hat die Polizei nach der Auswertung der Akte der Amtsanwaltschaft mitgeteilt, dass wegen des fehlenden Resttatverdachtes eine weitere Speicherung in polizeilichen Informationssystemen nicht erforderlich ist. Die Daten zur Person des Bürgers sind gelöscht worden.

Diese Vorgehensweise des Polizeipräsidenten in Berlin ist unverständlich, weil in Dateien gespeicherte personenbezogene Daten nicht nur bei einer unzulässigen Speicherung zu löschen und die dazugehörigen Unterlagen zu vernichten sind, sondern auch dann, wenn aufgrund von nach bestimmten Fristen vorzunehmenden Überprüfungen oder aus Anlass einer Einzelfallbearbeitung festgestellt wird, dass ihre Kenntnis zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist[83].

Im vorliegenden Fall stellte bereits die Rückmeldung der Staatsanwaltschaft über die Einstellung des Verfahrens einen Anlass zur Einzelfallbearbeitung dar. Der Ausgang des Verfahrens wurde im Datensatz gleichwohl lediglich dazugespeichert. Diese Vorgehensweise ist datenschutzrechtswidrig. Vielmehr war zu prüfen, ob ein ausreichender Resttatverdacht besteht, der die kriminalistische Prognose, dass der Betroffene erneut auffällig werden könnte, trägt. Diesen klaren rechtlichen Vorgaben ist nur wegen unseres beharrlichen Nachfragens Rechnung getragen worden. Das ist vor dem Hintergrund der nicht seltenen Einstellungen nach § 170 Abs. 2 StPO unbefriedigend. Wir erwarten von der Polizei, dass künftig jeder Anlass – also bereits die Rückmeldung der Staatsanwaltschaft, aber auch Auskunftsersuchen der Betroffenen oder unsere Bitten um Stellungnahme – für eine Überprüfung der weiteren Erforderlichkeit der Datenspeicherung genutzt wird.

Rückmeldungen der Staatsanwaltschaft über Einstellungen, unsere Bitten um Stellungnahme oder Auskunfts- und Löschungsanträge sind eine „anlassbezogene Einzelfallbearbeitung“ und erfordern eine Prüfung für die Erforderlichkeit der weiteren Datenspeicherung.

[83] § 48 Abs. 2 ASOG

3.1.6 Auswertedatenbank „Polizeilicher Staatsschutz“

Der Polizeipräsident in Berlin hat uns die Errichtungsanordnung für seine Auswertedatenbank „Polizeilicher Staatsschutz“ vorgelegt. Diese Datei dient der Unterstützung der auf dem Gebiet des polizeilichen Staatsschutzes tätigen Mitarbeiterinnen und Mitarbeiter bei der Erfüllung ihrer Aufgaben im Zusammenhang mit der Verhütung und Aufklärung politisch motivierter Straftaten. Insbesondere dient die Datei dem Erkennen von Personen- und Sachzusammenhängen, der Dokumentation polizeilichen Handelns und der Unterstützung, Koordination und Anregung von Ermittlungen.

Die Datei beruht auf einem Verfahren, das in besonderer Weise dazu dient, verdeckte bzw. bislang nicht bekannte Zusammenhänge verschiedener Vorgänge aus unterschiedlichen Ermittlungsbereichen transparent zu machen. Das Anliegen des Polizeipräsidenten in Berlin bei dem Einsatz eines solchen komplexen und leistungsfähigen Verfahrens ist durchaus nachvollziehbar. Datenschutzrechtlich problematisch daran ist aber, dass mit der Anwendung wahrscheinlich die Mehrzahl, zumindest aber eine Vielzahl von Hinweisen allein deshalb genutzt werden können, weil diese Informationen auch zufällig in anderen Verfahren ebenso erfasst worden sind. Insoweit werden Personen teilweise aufgrund von Zufällen dem Risiko von gegen sie gerichteten Ermittlungen ausgesetzt, obwohl sie hierzu keinen zurechenbaren Anlass gesetzt haben. Mit anderen Worten, die Polizei bewegt sich mit dem Verfahren weit in den Bereich der Vorfeldermittlungen hinein. An solche Vorfeldermittlungen legt die Rechtsprechung besonders strenge Maßstäbe an.

Wenn man solche weitreichenden Eingriffe überhaupt im Grundsatz als zulässig bewertet, sind deshalb zumindest strenge Maßstäbe an die Verhältnismäßigkeit zu stellen. Daraus folgt, dass nicht pauschal Löschprüffristen „normaler“ Vorgänge angewendet werden können, die allein auf relativ konkreten Anhaltspunkten zu Gefahrenlagen bzw. Straftaten beruhen. Denn die Erforderlichkeit von ähnlich langen Prüffristen wie in POLIKS in lediglich unterstützenden Auswertedateien, deren Ergebnisse wiederum in POLIKS einfließen dürften, können wir nicht erkennen. Das gilt nicht nur für die Geschädigten und Tatverdächtigen sowie die Personen, deren Daten aufgrund der §§ 24 bis 26 ASOG erhoben werden[84], sondern insbesondere für Zeuginnen und Zeugen, Hinweisgebende oder sonstige Auskunftspersonen. Bei diesem Personenkreis ist die Erforderlichkeit der weiteren

[84] Datenerhebung a) bei öffentlichen Veranstaltungen und Ansammlungen, b) durch langfristige Observation und Einsatz technischer Mittel sowie c) durch Einsatz von Personen, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist, und durch Einsatz verdeckter Ermittler

Datenspeicherung nach einem Jahr zu prüfen und die Höchstspeicherfrist darf drei Jahre nicht überschreiten.

Unserer Rechtsposition hat sich der Polizeipräsident in Berlin nicht angeschlossen. Er will die (Höchst-)Prüffristen auch für – lediglich unterstützende – Auswertedatenbanken ausschöpfen.

An die Festlegung von Löschprüffristen sind bei Auswertedateien strenge Maßstäbe anzulegen.

3.1.7 Zuverlässigkeitsüberprüfungen bei der Deutschen Bundesbank

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit informierte uns darüber, dass die Deutsche Bundesbank seit 2004 in erheblichem Umfang Zuverlässigkeitsüberprüfungen des bei ihr eingesetzten Fremdpersonals für Bereiche durchführt, die nicht unter den Anwendungsbereich des Sicherheitsüberprüfungsgesetzes (Geheimschutz oder vorbeugender personeller Sabotageschutz) fallen. Aufgrund einer von den Betroffenen abzugebenden Einwilligungserklärung werden die Landeskriminalämter um die Übermittlung von Erkenntnissen gebeten. Hierzu hat die Deutsche Bundesbank mit dem Landeskriminalamt eine Vereinbarung abgeschlossen.

Die Datenübermittlungen an die Deutsche Bundesbank hat der Polizeipräsident in Berlin zunächst auf § 45 Abs. 1 Nr. 5 ASOG[85] gestützt. Auf unseren Hinweis, dass es sich bei der Deutschen Bundesbank um eine öffentliche Stelle des Bundes handelt und diese Vorschrift als Rechtsgrundlage ebenso wenig für eine Datenübermittlung in Betracht kommt wie § 44 Abs. 2 Nr. 2 ASOG[86], weil bei einem Massenverfahren der Tatbestand der im Einzelfall bestehenden – konkreten – Gefahr nicht erfüllt ist, hat der Polizeipräsident in Berlin die Datenübermittlung auf die Einwilligung[87] gestützt, die seiner Auffassung nach auch wirksam sei. Die Mitarbeiterinnen und Mitarbeiter der Fremdfirmen befänden sich in keinem Abhängigkeitsverhältnis zur Deutschen Bundesbank. Die Einwilligung beruhe daher auf einer freien Entscheidung. Im Übrigen entspreche die von den Betroffenen zu unterzeichnende Einwilligungserklärung in vollem Umfang den Anforderungen des § 6 Abs. 3 BlnDSG. Die Betroffenen werden über den Verwendungszweck

[85] Datenübermittlungen an Personen oder Stellen außerhalb des öffentlichen Bereiches

[86] Datenübermittlungen an Stellen innerhalb des öffentlichen Bereiches

[87] § 6 Abs. 1 Nr. 3 BlnDSG

(Zuverlässigkeitsüberprüfung), den Empfänger der Daten (Polizeipräsident in Berlin), die vom Polizeipräsidenten in Berlin im Rahmen der Überprüfung genutzten polizeilichen Dateien, Übermittlung möglicher Erkenntnisse an die Deutsche Bundesbank sowie über die Möglichkeit, eine umfassende Datenauskunft nach § 50 Abs. 1 ASOG zu beantragen, informiert. Darüber hinaus werden sie unter Darlegung der Rechtsfolgen darauf hingewiesen, dass sie die Einwilligung verweigern können.

Vorliegend will die Deutsche Bundesbank nicht ihr eigenes Personal auf seine Zuverlässigkeit hin überprüfen, sondern das bei ihr eingesetzte Fremdpersonal, zu dem sie in keiner unmittelbaren Rechtsbeziehung steht. Eine Rechtsgrundlage, die der Deutschen Bundesbank eine solche Zuverlässigkeitsüberprüfung des bei ihr eingesetzten Fremdpersonals erlaubt, ist nicht ersichtlich. Wir haben das Verfahren daher beanstandet.

Neben speziellen Rechtsgrundlagen, die das Verfahren von Sicherheits- bzw. Zuverlässigkeitsüberprüfungen regeln[88], stellen die §§ 30, 31 Bundeszentralregistergesetz (BZRG) geeignete, ausreichende und abschließende Möglichkeiten für den Arbeitgeber zur Überprüfung der Zuverlässigkeit seiner Belegschaft dar. Zu weiteren Datenerhebungen ist der Arbeitgeber nicht befugt.

Zu berücksichtigen ist weiterhin, dass die polizeilichen Auskunftssysteme nur für bestimmte, gesetzlich festgelegte Zwecke eingerichtet worden sind. Nach der Errichtungsanordnung für POLIKS ist das Informationssystem ein Datenverarbeitungssystem, das der Information der Dienstkräfte im Bereich des Vollzugsdienstes der Berliner Polizei dient. Mit seiner Hilfe sollen Schnellauskünfte zu Personen, Sachen, Institutionen und Vorgängen durch gezielte Anfragen zu beschaffen sein bzw. Recherchen ermöglicht werden. Das System soll den Bediensteten zu ihrer eigenen Aufgabenwahrnehmung dienen, schnelle und zuverlässige Auskünfte zum Vorteil der Bürgerinnen und Bürger ermöglichen, um deren Interessen schnellstmöglich wahrnehmen bzw. ihre Beeinträchtigung auf ein Mindestmaß beschränken zu können. Ein wesentlicher Anknüpfungspunkt ist die polizeiliche Aufgabenwahrnehmung. Hier handelt es sich nicht um eine Sicherheits-, sondern um eine Zuverlässigkeitsüberprüfung, die gesetzlich nicht geregelt ist. Es mangelt also an einer gesetzlich zugewiesenen Aufgabe, zu deren Erfüllung auf das polizeiliche Auskunftssystem zurückgegriffen werden soll.

[88] beispielsweise Sicherheitsüberprüfungsgesetz, § 5 Waffengesetz, § 38 Gewerbeordnung, § 8 a Sprengstoffgesetz, § 7 Luftsicherheitsgesetz

Die Datenübermittlung kann auch nicht auf die Einwilligung der betroffenen Person gestützt werden. Sie wäre zwar eine gleichberechtigte Alternative zur gesetzlichen Erlaubnis. Allerdings müsste hierzu die Datenverarbeitung für die ordnungsgemäße Aufgabenerfüllung erforderlich sein. Gerade daran mangelt es für die Polizei, um pauschal im Interesse von anderen Stellen Zuverlässigkeitsüberprüfungen durchzuführen. Auch mit einer Einwilligung darf eine öffentliche Stelle keine personenbezogenen Daten verarbeiten, für die ihr keine Aufgabe zugewiesen wurde. Öffentliche Stellen dürfen sich nicht Aufgaben mit einer Einwilligung erschließen, die ihr der Gesetzgeber bewusst vorenthält. Überdies ist die Einwilligung auch nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. Eine Freiwilligkeit liegt nur vor, soweit die Entscheidung nicht unter Druck oder in einer Zwangslage getroffen wird. Wenn die betroffene Person nicht einwilligt, kann diese Entscheidung erhebliche Auswirkungen auf ihr Arbeitsverhältnis zu ihrem Arbeitgeber (hier: der Fremdfirma) haben. Das dürfte beispielsweise dann der Fall sein, wenn die Deutsche Bundesbank der Fremdfirma mitteilt, dass eine bestimmte Arbeitnehmerin oder ein bestimmter Arbeitnehmer keinen Zugang erhält (begrenzte Verwendbarkeit mit der möglichen Folge der Gehaltskürzung oder der Änderungskündigung).

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat die Datenübermittlung durch den Polizeipräsidenten an die Bundesbank in Ermangelung einer ausreichenden Rechtsgrundlage beanstandet.

Ohne eine gesetzliche Aufgabenzuweisung und normenklare gesetzliche Befugnisse sind Zuverlässigkeitsüberprüfungen zu unterlassen.

3.2 Verfassungsschutz

3.2.1 Vor-Ort-Kontrollen beim Verfassungsschutz

„Überwachung von Scientology – V-Mann-Affäre in Nordrhein-Westfalen – Observation von Kurnaz“. Die Tätigkeit der Verfassungsschutzämter ist im vergangenen Jahr vielfältig und bundesweit mit solchen Schlagzeichen Gegenstand der öffentlichen Presseberichterstattung geworden. In Berlin bewegte vor allem die Beobachtung einzelner Mitglieder des Berliner Sozialforums durch die Verfassungsschutzbehörde den Blätterwald. Dies und eine ungewöhnlich hohe Anzahl von Eingaben von Personen, die überwiegend dem linksextremen Spektrum zugerechnet werden, führten dazu, dass wir im Berichtszeitraum überdurchschnittlich

viele anlassbezogene Prüfungen bei der Berliner Verfassungsschutzbehörde durchgeführt haben.

Gegenstand der Eingaben waren zumeist Auskunfts- bzw. Akteneinsichtsgesuche der betroffenen Personen. Weiterhin wurde oft die Zulässigkeit der Datenspeicherung als solche bezweifelt.

Die Überprüfungen bei der Verfassungsschutzbehörde ergaben, dass die meisten Beschwerden im Grundsatz unberechtigt waren.

Abgesehen von dem Umstand, dass das Verfahren zur Auskunftserteilung bzw. zur Entscheidung über die Gewährung von Akteneinsicht einen sehr langen Zeitraum einnahm, war die Verfahrensweise der Verfassungsschutzbehörde im Wesentlichen datenschutzrechtlich nicht zu kritisieren. In einigen Fällen erreichten wir allerdings, dass den betroffenen Personen weitergehende Informationen mitgeteilt wurden.

Im Übrigen hat die Verfassungsschutzbehörde von einer weitergehenden Auskunftserteilung bzw. Gewährung von Akteneinsicht zu Recht abgesehen.

Nach § 32 Verfassungsschutzgesetz (VSG) besteht regelmäßig kein Anspruch auf Akteneinsicht. Allerdings hat die Verfassungsschutzbehörde die Pflicht, einen entsprechenden Antrag der Betroffenen auf Akteneinsicht ermessensfehlerfrei zu bescheiden. Soweit Geheimhaltungsinteressen oder schutzwürdige Belange Dritter einer Akteneinsicht nicht entgegenstehen, sind kaum Gesichtspunkte denkbar, eine solche Akteneinsicht zu verweigern. Ein solcher Verweigerungsgrund ist in § 32 Abs. 2 VSG vorgesehen, wonach die Einsichtnahme in Akten insbesondere dann zu versagen ist, wenn die Daten der Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen sonstigen Informationen eng verbunden sind. In einem solchen Fall – dies dürfte nicht selten der Fall sein – bedeutet die Trennung von Aktenteilen, die sich auf die betroffene Person beziehen, einen unverhältnismäßig großen Aufwand. Dann ist zu prüfen, ob der Antrag stellenden Person eine zusammenfassende Auskunft über den Akteninhalt erteilt werden kann.

Demgegenüber steht den betroffenen Personen grundsätzlich ein Anspruch auf Auskunftserteilung gegenüber der Verfassungsschutzbehörde zu. Gemäß § 31 VSG erstreckt sich die grundsätzliche Auskunftspflicht der Verfassungsschutzbehörde nicht auf Informationen, die nicht ihrer alleinigen Verfügungsberechtigung unterliegen, sowie auf die Herkunft der Informationen und den Empfängerkreis von Übermittlungen. Die Berliner Verfassungsschutzbehörde verfügt damit zum Beispiel nicht allein über Informationen, die von anderen Verfassungsschutzämtern in

das gemeinsame Nachrichtendienstliche Informationssystem (NADIS) gespeichert worden sind. Entsprechendes gilt für Datenmaterial, das die Verfassungsschutzbehörde von Polizeibehörden erhalten hat. In solchen Fällen muss die Berliner Verfassungsschutzbehörde Einvernehmen mit der anderen Behörde über die Auskunftserteilung erzielen, bevor sie die begehrte Auskunft erteilen kann.

Im Übrigen darf die Verfassungsschutzbehörde einen Antrag auf Auskunftserteilung ablehnen, wenn das öffentliche Interesse an der Geheimhaltung ihrer Tätigkeit oder ein überwiegendes Geheimhaltungsinteresse Dritter das Interesse der Antrag stellenden Personen an der Auskunftserteilung überwiegt. In einem solchen Fall hat die Berliner Verfassungsschutzbehörde die Antrag stellende Person darauf hinzuweisen, dass sie sich an den Berliner Beauftragten für Datenschutz und Informationsfreiheit wenden kann. Mitteilungen des Berliner Beauftragten für Datenschutz und Informationsfreiheit an die Antrag stellende Person dürfen keine Rückschlüsse auf den Erkenntnisstand der Verfassungsschutzbehörde zulassen, soweit diese nicht einer weitergehenden Auskunft zustimmt.

Die Prüfungen führten im Berichtszeitraum jeweils dazu, dass zwischen der Berliner Verfassungsschutzbehörde und dem Berliner Beauftragten für Datenschutz und Informationsfreiheit im Ergebnis Meinungsverschiedenheiten über den zulässigen Umfang der zu erteilenden Auskunft an die Antrag stellende Person stets ausgeräumt werden konnten.

Was die Beschwerden über die Zulässigkeit von Datenspeicherungen anbelangt: In zwei Fällen konnten wir mit der Verfassungsschutzbehörde Einvernehmen darüber erzielen, dass eine weitere Speicherung der Petentendaten zumindest zum Zeitpunkt der jeweiligen Prüfung nicht mehr erforderlich sei. Die Daten wurden in einem Fall vollumfänglich gelöscht, in dem anderen Fall auf Wunsch des Petenten gesperrt.

Insgesamt gesehen ergaben die Prüfungen durch den Berliner Beauftragten für Datenschutz und Informationsfreiheit keine Anhaltspunkte dafür, dass die Verfassungsschutzbehörde nicht verantwortungsvoll mit den ihr eingeräumten gesetzlichen Überwachungsbefugnissen umgeht.

3.2.2 Die Antiterrordatei – Ein Zwischenbericht

Im vergangenen Jahr haben wir bereits auf die erheblichen verfassungsrechtlichen Bedenken der Datenschutzbeauftragten des Bundes und der Länder gegenüber dem Antiterrordateigesetz (ATDG) hingewiesen[89]. Gegen das Gesetz ist nun-

[89] JB 2006, 3.2

mehr Verfassungsbeschwerde eingelegt worden. Das Bundesverfassungsgericht hat im Rahmen dieses Verfahrens den Datenschutzbeauftragten des Bundes und der Länder Gelegenheit zur Stellungnahme gegeben.

Dieser Bitte sind wir in einer gemeinsamen Stellungnahme der Landesbeauftragten für Datenschutz nachgekommen und haben im Wesentlichen auf folgende Gesichtspunkte hingewiesen:

Das ATDG soll einen gemeinsamen Datenbestand verschiedenster Sicherheitsbehörden (insbesondere Verfassungsschutzämter, Bundesnachrichtendienst, Kriminalämter des Bundes und der Länder und andere Polizeibehörden) ermöglichen. In seiner konkreten Ausgestaltung genügt es bereits nicht dem sog. Trennungsgebot. Dieses Gebot besagt, dass die Polizeibehörden und die Nachrichtendienste in ihren Funktionen und in ihrer Aufgabenwahrnehmung zu trennen sind.

Diese Trennung ist kein Selbstzweck. Sie ist Ausdruck geschichtlicher Erfahrungen des extremen Machtmissbrauchs im Dritten Reich und dient dem Schutz der Freiheit der Bürgerinnen und Bürger. Eine Geheime Staatspolizei oder ein Ministerium für Staatssicherheit, die unbegrenzte Befugnisse zur Datensammlung mit exekutiven Kompetenzen in sich vereinigen, darf es in unserem freiheitlich orientierten Rechtsstaat nicht geben. Dazu ist es wichtig, sich die unterschiedlichen Funktionen von Nachrichtendiensten und Polizeibehörden vor Augen zu führen: Nachrichtendienste dürfen nahezu voraussetzungslos Daten über Bürgerinnen und Bürger sammeln und auswerten, weil und wenn dies zur Gewinnung von Erkenntnissen über die nationale Sicherheitslage dient. Ein Nachrichtendienst kann deshalb auch Personen erfassen, die sich rechtstreu verhalten bzw. gegen die kein Verdacht besteht, dass sie Straftaten begangen haben oder begehen werden. Dies ist aufgrund ihrer Aufgabe der strategischen Aufklärung und nur deshalb gerechtfertigt, weil die Nachrichtendienste keine Befugnis haben, die Freiheit von Menschen einzuschränken oder gar mit Waffengewalt gegen sie vorzugehen. Demgegenüber haben die Polizeibehörden den Auftrag, Gefahrensituationen abzuwenden, Störungen zu beseitigen bzw. Straftaten zu verfolgen. Sie haben Befugnisse, die in Extremfällen zur Tötung von Menschen führen können. Dementsprechend müssen die Anforderungen an die Datenbeschaffung durch die Polizeibehörden relativ streng sein.

Das Bundesverfassungsgericht hat in einer Entscheidung angedeutet, dass das Rechtsstaatsprinzip, das Bundesstaatsprinzip und der Schutz der Grundrechte es verbieten können, bestimmte Sicherheitsbehörden miteinander zu verschmelzen oder sie mit Aufgaben zu befassen, die mit ihrer verfassungsrechtlichen Aufgaben-

stellung unvereinbar sind[90]. Nach unserer Auffassung sprechen auch Wortlaut und Funktion von Art. 87 Abs. 1 Satz 2 GG für den Verfassungsrang des Trennungsgebots.

Dieses Prinzip schließt Datenübermittlungen zwischen den Sicherheitsbehörden nicht völlig aus. Aufgrund der unterschiedlichen Aufgabenstellungen von Nachrichtendiensten und Polizeibehörden müssen sie jedoch die Ausnahme bleiben und sind auf Einzelfälle zu beschränken. Insbesondere darf es nicht zu einer planmäßigen Zusammenführung von Erkenntnissen kommen, durch die die grundsätzlich bestehende Funktionentrennung aufgehoben würde[91]. Genau dies geschieht jedoch in der Antiterrordatei.

Sieht man von der Verletzung des Trennungsgebots ab, sind die Vorschriften des ATDG auch nicht hinreichend bestimmt und normenklar. Nach den verfassungsrechtlichen Grundsätzen der Normenbestimmtheit und Normenklarheit müssen betroffene Personen anhand einer gesetzlich vorgesehenen Datenverarbeitungsbefugnis zumindest im Grundsatz erkennen können, ob sie mit einer staatlichen Erfassung rechnen müssen und von welchen Stellen sie erfasst werden. Dem wird das ATDG nicht gerecht: Die Regelungen schaffen einen gemeinsamen Datenbestand der beteiligten Sicherheitsbehörden, ohne dass die sehr weit gefassten Zugriffsregelungen eine hinreichende Bindung an den Zweck der Datenerhebung einer vorherigen Speicherung vorsehen. So ist weiterhin unklar, unter welchen Voraussetzungen eine Person als Angehörige, als Unterstützerin, als Befürworterin oder als Kontakt- und Begleitperson von Angehörigen, Unterstützern oder Befürwortern von terroristischen Vereinigungen anzusehen ist. Es ist weiterhin fraglich, ob der große Umfang der gespeicherten Daten erforderlich ist. Die Grundrechtseingriffe werden auch nicht ausreichend durch verfahrensrechtliche Vorkehrungen abgefedert, insbesondere fehlen klare Regelungen zu Lösch- und Aussonderungsprüffristen.

Schließlich räumt das ATDG zwar dem Wortlaut nach ein Auskunftsrecht den betroffenen Personen ein, in der Praxis kann dieses Recht jedoch kaum durchgesetzt werden. Denn das ATDG sieht vor, dass „die Auskunft zu verdeckt gespeicherten Daten ... sich nach den für die Behörde, die die Daten eingegeben hat, geltenden Rechtsvorschriften“ richtet. Im Klartext heißt dies: Obwohl die Antiterrordatei einen zentralen Datenbestand darstellt, haben die betroffenen Personen keine einheitliche Stelle, der gegenüber sie ihre Datenschutzrechte geltend machen können. Um beispielsweise sicher zu gehen, dass ein Auskunftsersuchen vollstän-

[90] BVerfGE 97, 198, 217

[91] so auch der ehemalige Richter am BVerfG Dieter Grimm, Die Zeit v. 29. November 2007

dig beantwortet wird, müsste eine betroffene Person also ihren Anspruch gegenüber sämtlichen (!) der derzeit etwa vierzig beteiligten Behörden durchsetzen. Verweigern die verantwortlichen Stellen die Auskunft, machen sie es der betroffenen Person unmöglich, etwaige Erfolgsaussichten eines Widerspruchs- bzw. Verwaltungsgerichtsverfahrens abzuschätzen. Und wer strengt schon bei ungewissem Prozessausgang vierzig verschiedene Gerichtsverfahren an?

Unabhängig von dem noch anhängigen Verfassungsbeschwerdeverfahren hat der Polizeipräsident in Berlin wie alle anderen beteiligten Sicherheitsbehörden damit begonnen, die Antiterrordatei zu „befüllen“. Wir haben dies zum Anlass genommen, die Vorgehensweise einer ersten Vor-Ort-Prüfung zu unterziehen. Das Prüfverfahren ist noch nicht abgeschlossen.

Gegen das Gesetz über die Antiterrordatei bestehen gravierende verfassungsrechtliche Einwände. Unabhängig davon wird seine Anwendung in der Praxis datenschutzrechtlich überprüft.

3.2

4 Ordnungsverwaltung

4.1 Melde-, Personenstands- und Ausländerwesen

4.1.1 Eckpunkte der Datenschutzbeauftragten des Bundes und der Länder

Im Zuge der Föderalismusreform wurde das Meldewesen zum 1. September 2006 in die ausschließliche Gesetzgebungskompetenz des Bundes überführt. In Ergänzung der bisherigen kommunalen Register plant das Bundesministerium des Innern den Aufbau eines Bundesmelderegisters (BMR). Dies soll nach Angaben des Ministeriums das Meldeverfahren für Bürgerinnen und Bürger vereinfachen, die Nutzung der Melderegister für Wirtschaft und Verwaltung effizienter und kostengünstiger machen, die Qualität und Aktualität der Meldedaten verbessern und bundesweit einheitliche Online-Dienste ermöglichen.

Lösungen (beispielsweise elektronische Rückmeldung, vorausgefüllter Meldeschein, spezielle Auskunftsverfahren sowie Online-Auskunft) sind auf der Basis der geltenden Gesetzeslage in den Ländern bereits konzipiert und teilweise umgesetzt worden. Im Übrigen ist die Verwaltungskompetenz der Länder für das Meldewesen durch die Föderalismusreform nicht aufgehoben oder verändert worden.

In einem Gemeinsamen Eckpunktepapier haben die Datenschutzbeauftragten des Bundes und der Länder Folgendes gefordert:

1. Ein zentrales Bundesmelderegister und die damit verbundene mehrfache Datenhaltung sind nicht erforderlich. Die Modernisierung des Meldewesens kann durch eine Vernetzung der vorhandenen Melderegister erreicht werden. Hierfür hat man bereits 2002 auf Drängen des Bundes den Datenaustausch im Meldewesen standardisiert (inhaltlich mit XMeld und technisch mit OSCI-Transport V 1.2) und damit die Voraussetzungen für einen effizienten und sicheren Datenaustausch geschaffen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat den flächendeckenden Aufbau einer OSCI-basierten Infrastruktur mit Ende-zu-Ende-Sicherheit in ihrer Entschließung vom 15. Dezember 2005 ausdrücklich begrüßt.

2. Ein Bundesmeldegesetz hätte das verfassungsrechtliche Verbot eines einheitlichen und verwaltungsübergreifenden Identifikationsmerkmales zu beachten. Identifikationsmerkmale dürfen nur bereichsspezifisch gebildet, verwendet und gespeichert werden, jedoch nicht zur Zusammenführung von Daten aus unterschiedlichen Verwendungszwecken. Dies

schließt auch die Speicherung fremder bereichsspezifischer Identifikationsmerkmale (z. B. Steuer-ID) in den Melderegistern aus. Es muss untersucht werden, wie ein datenschutzgerechtes Identitätsmanagement unter Beachtung der verfassungsrechtlichen Vorgaben zu konzipieren ist.

3. Aus Datenschutzsicht muss der vollständige Meldedatenbestand bei den jeweiligen kommunalen Meldeämtern und unter ihrer Verantwortung verbleiben.

4. Eine Reform des Melderechts muss den Umfang der im Meldewesen gespeicherten Daten einer kritischen Prüfung unter den Gesichtspunkten der Erforderlichkeit und der Zweckbindung unterziehen. So steht die Anreicherung der Melderegister mit zusätzlichen, über ihre Kernaufgabe hinausgehenden Informationen (Waffenerlaubnis, Sprengstofferlaubnis, steuerliche Identifikationsnummer) im Widerspruch zu ihrem originären Zweck, Identität und Wohnsitz der Einwohner festzustellen und zu registrieren.

5. Es muss sichergestellt werden, dass jede Behörde nur die Daten erhält, die sie für ihre Aufgaben benötigt. Übermittlungen – auch im Wege des automatisierten Abrufes – aus dem Melderegister müssen unter inhaltlichen, regionalen und funktionalen Gesichtspunkten differenziert werden.

6. Eine Melderechtsreform muss auch Anlass sein, die Rechte der Meldepflichtigen deutlich zu stärken. Daher sollten bestehende Widerspruchsregelungen (beispielsweise Gruppenauskünfte an Parteien zur Wahlwerbung) zum Schutz der Betroffenen durch Einwilligungslösungen ersetzt werden. Zudem sind die Vorgaben des Bundesverwaltungsgerichtes (Urteil vom 21. Juni 2006) umzusetzen, wonach schutzwürdige Interessen der Betroffenen bei einer Weitergabe ihrer Meldedaten für Marketingzwecke besonders zu berücksichtigen sind.

7. Gerade weil das Melderegister in den zurückliegenden Jahren immer mehr zu einem multifunktionalen Informationspool für Wirtschaft und Verwaltung geworden ist, ist es notwendig, die Mechanismen der Fachaufsicht und der Datenschutzkontrolle sowie das Auskunftsrecht der Betroffenen im Melderecht zu stärken. Die Betroffenen können heute kaum noch erkennen, an welche Stellen Meldedaten fließen. Sie sollten deshalb grundsätzlich auch die Möglichkeit haben, Kenntnis über sie betreffende Datenabrufe, -übermittlungen und -auskünfte zu erhalten.

Wir haben die Senatsverwaltung für Inneres gebeten, sich bei den Beratungen zwischen Bund und Ländern für eine Berücksichtigung dieser Eckpunkte einzusetzen.

4.1.2 Wer nicht abwarten kann

Mit dem Steueränderungsgesetz 2003 wurde eine Rechtsgrundlage für die Einführung einer Steueridentifikationsnummer für alle Steuerpflichtigen von Geburt an geschaffen[92]. Flankierend dazu sind sowohl im Melderechtsrahmengesetz als auch im Landesmeldegesetz die Befugnisse zur Speicherung des Merkmals im Melderegister geschaffen worden.

In dieser Zeit hat uns die Senatsverwaltung für Inneres gefragt, ob wir Vorbehalte gegen eine Übermittlung der Meldedaten für Probeläufe beim Bundesamt für Finanzen haben. Die hatten wir, weil nach § 139 b Abs. 6 der Abgabenordnung (AO) die Übermittlung ab dem Zeitpunkt der Einführung des Identifikationsmerkmals erfolgt, der durch Rechtsverordnung des Bundesministeriums für Finanzen bestimmt wird. Es ist kein überzeugender Grund erkennbar oder geltend gemacht worden, der einen zwingenden Vorgriff auf die zu erwartende Rechtsverordnung erkennen lässt.

Mit der Verordnung zur Einführung dauerhafter Steueridentifikationsnummern im Besteuerungsverfahren und Veränderung der Zweiten Bundesmeldedatenübermittlungsverordnung[93] sind die Meldebehörden verpflichtet worden, abschließend festgelegte Daten dem Bundeszentralamt für Steuern für jeden in ihrem Zuständigkeitsbereich mit alleiniger oder mit Hauptwohnung im Melderegister registrierten Personen zu übermitteln. Das Bundeszentralamt für Steuern kann diese Daten von den Meldebehörden zum Zwecke der Erprobung des Verfahrens der Datenübermittlung, der vom Bundeszentralamt für Steuern einzusetzenden Programme und der Zuordnung zu den bei den Rechenzentren der Landesfinanzverwaltungen gespeicherten personenbezogenen Daten übermitteln.

Das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) hat die für die Durchführung der Testläufe vorgesehenen Meldedaten am 17. November 2006 erstellt. Am 22. November 2006 wurden die Daten verschlüsselt und auf Datenträger abgezogen. Der Datenträger wurde am 23. November 2006 von einer Mitarbeiterin des LABO einer Mitarbeiterin des Bundeszentralamtes für Steuern übergeben.

---

[92] JB 2004, 3.2

[93] BGBl. I, 2726

4.1

Nach der Vorgeschichte hat uns der Zeitpunkt der Übermittlung überrascht. Wir haben einen datenschutzrechtlichen Mangel festgestellt, weil die Verordnung erst am Tage nach der Verkündung in Kraft getreten ist. Die Veröffentlichung im Bundesgesetzblatt erfolgte am 6. Dezember 2006. Die Daten sind somit ohne Rechtsgrundlage (vorfristig) übermittelt worden. Das ist unzulässig. Die erbetene Mitteilung, ob wenigstens die Löschungsfristen der Verordnung eingehalten wurden, steht trotz mehrerer Erinnerungen noch immer aus.

Die Verarbeitung personenbezogener Daten darf nicht auf künftige, noch nicht in Kraft getretene Befugnisnormen gestützt werden.

4.1.3 Automatisierte Erteilung von Melderegisterauskünften

Bei der Novellierung des Meldegesetzes (MeldeG)[94] wurde u. a. die rechtliche Möglichkeit geschaffen, einfache Melderegisterauskünfte an Private auch über das Internet zu erteilen[95].

Technisch hatte das LABO dies über den Internet-Auskunftsserver für Privatpersonen (IASP) realisiert. Der IASP nutzt das Portal für Auskünfte an Behörden (PAB) und ermöglicht dadurch automatisierte Meldedatenübermittlungen aus dem Metropolitan Area Network (MAN) für Berliner Behörden. Im Rahmen dieses Projektes wurde das Informationsregister eingeführt. Das befindet sich in einer anderen Sicherheitsdomäne und wird einseitig vom Melderegister gespeist. Ein Durchgriff vom Informationsregister auf das Melderegister ist aus Sicherheitsgründen nicht möglich.

Wir haben festgestellt, dass das Informationsregister auch Daten enthält, die weder für Datenabrufe öffentlicher Stellen[96] noch für die automatisierte Erteilung von Melderegisterauskünften an Private[97] benötigt werden. Die Einstellung dieser Daten in das Informationsregister ist daher nicht erforderlich[98] und hat zu unterbleiben. Erst recht dürfen keine Daten in das Informationsregister eingespielt werden, für die nach dem Meldegesetz keine Speicherungsbefugnis besteht, wenn die Meldepflichtigen nicht ausdrücklich einwilligen.

---

[94] GVBl. 2006, 896

[95] § 28 a MeldeG

[96] Anlage 5 zu § 3 Nr. 2 DVO-MeldeG

[97] § 28 a MeldeG

[98] § 9 Berliner Datenschutzgesetz (BlnDSG)

Einfache Melderegisterauskünfte können auf automatisierten Datenträgern, durch Datenübertragung oder im Wege des automatisierten Abrufes über das Internet erteilt werden. Der Abruf ist nicht zulässig, wenn die oder der Betroffene dieser Form der Auskunftserteilung widersprochen hat. Die Auskunftserteilung auf konventionellem Wege bleibt davon unberührt. Die Antrag stellende Person muss die gesuchte Person mit Vor- und Familiennamen sowie mindestens zwei weiteren der in § 2 Abs. 1 MeldeG gespeicherten Daten bezeichnen. Außerdem muss die Identität der gesuchten Person durch einen Abgleich ihrer im Melderegister gespeicherten Daten eindeutig festgestellt worden sein[99]. In der vorgestellten Anwendung des IASP müssen neben den Pflichtdaten „Vor- und Familienname“ zwei weitere Merkmale aus den drei Möglichkeiten „Berliner Anschrift“, „Geschlecht“ oder „Geburtsdatum“ angegeben werden.

Die Beschränkung auf drei Merkmale aus dem umfassenden Katalog der nach § 2 Abs. 1 MeldeG zu speichernden Daten halten wir für nicht gerechtfertigt. Der Gesetzgeber hat nicht nur den elektronischen Zugang zum Melderegister bei der einfachen Melderegisterauskunft zugelassen, sondern er hat auch die Voraussetzungen dafür festgelegt. Wenn die Meldebehörde auskunftsberechtigten Personen die Möglichkeit eröffnet, auf elektronischem Wege eine einfache Melderegisterauskunft einzuholen, dann hat sie auch sicherzustellen, dass eine Auskunft erteilt wird, wenn die betroffene Person neben dem Vor- und Familiennamen mit zwei weiteren nach § 2 Abs. 1 MeldeG gespeicherten Daten bezeichnet wird. Das Verfahren, das auf einem Fertigprodukt der Firma HSH basiert, bildet die gesetzlichen Vorgaben nicht ausreichend ab und ist somit mangelhaft. Hier ist das nachzuholen, was bei der Beschaffung des Produktes hätte bereinigt werden müssen. Das LABO will dem nicht folgen. Wir haben in der Sache einen Dissens festgestellt.

Wenn die meldepflichtige Person nicht ausdrücklich einwilligt, dürfen im Melderegister nur die vom Gesetzgeber zugelassenen Merkmale gespeichert werden. Im Informationsregister dürfen nur die zur Aufgabenerfüllung erforderlichen Daten gespeichert werden. Die Meldebehörde darf die vom Gesetzgeber vorgegebenen Voraussetzungen für den elektronischen Zugang nicht verkürzen.

4.1.4 Funktion „go archiv“

Das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) hat vor Jahren die Software „go archiv“ zur retrograden Erfassung der Passanträge angeschafft, die nicht nur die Archivierung der Reisepässe – und später der Personalausweise – stark vereinfacht, sondern auch die

[99] § 28 a MeldeG

Recherchen optimiert. Durch die digitale Archivierung stehen die Antragsdaten am Arbeitsplatz zur Verfügung. Lagerkapazitäten werden nicht mehr in Anspruch genommen.

Nach Darstellung des LABO werden die Passdaten in einem sog. „halbautomatisierten" Abrufverfahren anderen Behörden zur Verfügung gestellt. Die Polizei – nicht aber die Bußgeldstelle – hat im Einzelfall nur Zugriff, wenn die Anfragenden der Passstelle auf Nachfrage die Passnummer mitgeteilt haben.

Allerdings ist hier die gesetzlich vorgeschriebene förmliche Unterrichtung[100] des Berliner Beauftragten für Datenschutz und Informationsfreiheit unterblieben. Überdies ist unklar geblieben, warum die Passnummer einziges Suchkriterium ist. Ohne Kenntnis der Passnummer kann kein automatisierter Zugriff auf die im Passregister gespeicherten Daten erfolgen. Nach den uns bis Redaktionsschluss vorliegenden Unterlagen muss die Polizei dieses Merkmal zunächst entweder selbst dem Melderegister entnehmen oder bei einer Passstelle erfragen. Ferner ist offengeblieben, ob bei diesen Abfragen auch der Grund genannt wird, um die Rechtmäßigkeit der Datenübermittlung überprüfen zu können, oder bei einer entsprechenden Anfrage die Passdaten (regelmäßig wird es sich um Passfoto handeln) pauschal übermittelt werden.

Bei wesentlichen Änderungen automatisierter Datenverarbeitung haben uns die Behörden und sonstigen öffentlichen Stellen vorab zu informieren.

4.1.5 Datenerhebung vor Erteilung einer Niederlassungserlaubnis

Darf die Ausländerbehörde zur sachgerechten Prüfung einer Niederlassungserlaubnis verlangen, dass der deutsche Ehegatte einer Antragstellerin einen Prüfbericht vom Steuerberater vorlegt? Mit dieser Frage wandte sich ein Bürger an uns. Seine Ehegattin, eine chinesische Staatsbürgerin, sei bislang Inhaberin einer befristeten Aufenthaltserlaubnis. Sie hatte beim Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) als Ausländerbehörde die Erteilung einer unbefristeten Niederlassungserlaubnis beantragt.

Das LABO hatte die Antragstellerin aufgefordert, mit umfangreichen Unterlagen persönlich vorzusprechen. Diesem Verlangen waren die Antragstellerin und ihr Ehemann nachgekommen. Wenig später forderte das

[100] § 24 Abs. 3 Satz 3 BlnDSG

LABO die Antragstellerin erneut auf, weitere Unterlagen auch ihres Ehegatten vorzulegen. Für die Petenten brachte insbesondere die Forderung nach Vorlage des Prüfberichts von einem Steuerberater das Fass zum Überlaufen. Fraglich war überdies, ob das LABO Informationen über den Ehegatten der Antragstellerin einziehen durfte.

Auf unsere Bitte zur Stellungnahme hin hat die Senatsverwaltung für Inneres und Sport selbst eine Stellungnahme des LABO eingeholt und anschließend dessen Rechtsposition uneingeschränkt geteilt.

Dies wäre an und für sich nicht zu beanstanden gewesen, wenn die Senatsverwaltung die Stellungnahme des LABO kritisch überprüft hätte. Aus den Begleitumständen ergab sich jedoch, dass die Senatsverwaltung sich die Rechtsposition des LABO ohne jegliche inhaltliche Überprüfung zu eigen gemacht hatte.

Im Rahmen der Unterstützungspflicht hat die Senatsverwaltung als Fachaufsichtsbehörde gemäß § 8 Abs. 2 Aufenthalts- und Zuwanderungsgesetz (AZG) auch in datenschutzrechtlichen Fragen die recht- und ordnungsgemäße Erledigung der Aufgaben und die zweckentsprechende Handhabung des Verwaltungsermessens *zu überprüfen*. Die Senatsverwaltung für Inneres und Sport hat entgegen dieser Vorschrift die uneingeschränkte Bereitschaft gegenüber der ihrer Fachaufsicht unterliegenden Ausländerbehörde gezeigt, sich *ohne* Prüfung der Recht- und Zweckmäßigkeit der oben genannten Praxis der Stellungnahme der Ausländerbehörde anzuschließen.

In der Sache legten das LABO und in seinem Gefolge die Senatsverwaltung dar, bei der Entscheidung über die Erteilung eines Aufenthaltstitels sei gerade das Einkommen von Ehegatten einzuberechnen. Die Antragstellerin sei hierfür darlegungs- und beweisbelastet gewesen. Es liege auch keine Missachtung des Verhältnismäßigkeitsgrundsatzes dar. Ein Prüfbericht vom Steuerberater werde immer dann gefordert, wenn auf andere Weise nicht verlässlich die gesetzlich geforderte positive Prognose abgegeben werden könne. Andere aussagekräftige Unterlagen könnten gerade nicht vorgelegt werden, weil unstrukturierte Belegsammlungen die Beurteilung nicht ermöglichen würden. Die Folge wäre, dass der fehlende Nachweis zulasten der jeweiligen Antrag stellenden Person gehen würde.

Sowohl im Hinblick auf den Umfang der Datenerhebung als auch hinsichtlich der Beschaffung von Unterlagen über den betroffenen Ehegatten unmittelbar bei der Antragstellerin sind die Ausführungen des LABO nicht nachvollziehbar.

4.1

Eine Pflicht zur Vorlage des Prüfberichts eines Steuerberaters ist dem Aufenthaltsgesetz nicht zu entnehmen. Das Verlangen der Ausländerbehörde verstößt damit in erheblicher Weise gegen die Grundsätze des Gesetzesvorbehalts und der Verhältnismäßigkeit.

Überdies ist die Vorlage eines Prüfberichts vom Steuerberater als Einkommensnachweis nicht erforderlich. Das Einkommen kann mit für die Betroffenen organisatorisch und finanziell weniger belastenden Mitteln überprüft werden. Zum Beispiel kann die Beibringung einer vom Finanzamt bestätigten persönlichen Erklärung über das Einkommen bzw. die Beibringung von Einkommensteuerbescheiden verlangt werden. Auch die Vorlage einer strukturierten Belegsammlung ist als Einkommensnachweis geeignet.

Die Maßnahme war in diesem Fall auch unverhältnismäßig, weil sie der Antragstellerin die Einholung eines kostenträchtigen Prüfberichts abverlangte, der gesetzlich nicht vorgesehen ist. Damit wälzte die Ausländerbehörde eigene Prüfaufgaben auf die Antragstellerin ab. Der Einwand der Senatsverwaltung, dass es nicht i. S. d. Datenschutzrechts sein könne, wenn eine Niederlassungserlaubnis nicht mehr erteilt werden könne, wenn die Einkommensverhältnisse des Ehegatten eines Ausländers nicht mehr überprüfbar seien, geht an der Sache vorbei: Es ist die Pflicht der Ausländerbehörde, selbst die vorgelegten Unterlagen zu überprüfen. Kann sie eine fachgerechte Prüfung aus Gründen der mangelnden Fachkompetenz bzw. mangelnder personeller Ressourcen nicht vornehmen, muss *sie* für ergänzende Hilfestellung sorgen. Soweit die vorgelegten Unterlagen geeignet sind, das Einkommen nachvollziehbar zu belegen, hat die Antrag stellende Person das Recht zur Wahl, wie sie ihre Einkünfte nachweist.

Hiervon abgesehen hat die Ausländerbehörde gegen den datenschutzrechtlichen Grundsatz der Direkterhebung bei Betroffenen verstoßen, indem sie von der Antragstellerin die Vorlage von diversen Unterlagen verlangte, die ihren Ehegatten betrafen. Dieser Grundsatz besagt, dass eine verantwortliche Stelle wie das LABO personenbezogene Daten bei der betroffenen Person selbst zu erheben hat. Das Berliner Datenschutzgesetz lässt eine Datenerhebung bei Dritten in § 10 Abs. 1 und Abs. 4 nur ausnahmsweise dann zu, wenn eine besondere Rechtsvorschrift dies erlaubt. Beschafft sich der Staat personenbezogene Informationen bei Dritten, erhöht sich für die betroffene Person das Risiko, nichts von der staatlichen Datenverarbeitung zu erfahren.

Der vom LABO als Rechtsgrundlage genannte § 82 Abs. 3 Aufenthaltsgesetz (AufenthG) sieht *nicht* vor, dass bei der Entscheidung über die Erteilung einer Niederlassungserlaubnis von dem Grundsatz der Direkterhebung bei Betroffenen

abgewichen werden kann. § 82 Abs. 1, 3 AufenthG stellt seinem Wortlaut nach unmissverständlich auf die Mitwirkungspflichten *der ausländischen Person* ab. Über die Art und Weise der Erhebung von Daten über deutsche Ehegatten sagt § 82 Abs. 1, 3 AufenthG nichts aus, sodass es bei dem allgemeinen Grundsatz der Direkterhebung bei der betroffenen Person bleibt.

Wir haben das Vorgehen der Senatsverwaltung als Verletzung der Unterstützungspflicht nach § 28 BlnDSG beanstandet. Weiterhin waren der Verstoß gegen das Prinzip der Direkterhebung und die gesetzlich nicht erlaubte Datenerhebung zu beanstanden.

In einer abschließenden Stellungnahme hat die Senatsverwaltung angekündigt, dass sie unsere Empfehlungen in die regelmäßig stattfindenden Gespräche mit der Leitung der Ausländerbehörde mit einfließen lassen werde.

Im Rahmen ihrer Unterstützungspflicht nach § 28 BlnDSG darf sich eine Senatsverwaltung nicht damit begnügen, die Stellungnahme einer nachgeordneten verantwortlichen Stelle einzuholen und sich deren Rechtsposition ohne jegliche Überprüfung zu eigen zu machen. Das Aufenthaltsgesetz sieht im Zusammenhang mit der Erteilung von Aufenthaltstiteln nicht die Pflicht zur Vorlage eines Prüfberichts vom Steuerberater vor, wenn die betroffene Person diesen Bericht nur aufgrund des Verlangens der Ausländerbehörde erstellen lassen müsste. Auch die Ausländerbehörde muss das Prinzip der Direkterhebung bei der betroffenen Person beachten.

4.2 Verkehr

4.2.1 „Mann“ ist nicht gleich „Mann“

„Er“ sitzt am Steuer und fährt und fährt ... mit ihrem Wagen ... – da, ein Blitz von vorn reißt „ihn“ aus dem gedankenlosen Rasen – eine Geschwindigkeitsüberschreitung auf der Autobahn wurde festgestellt. Der Anhörungsbogen im Ordnungswidrigkeitenverfahren geht zunächst an „sie“, die Kraftfahrzeughalterin, weil auf „sie“ das Auto zugelassen ist. „Sie“ räumt den Verstoß ein. Doch die Ermittlungsbehörde meint, auf dem Blitzfoto sei ein Mann abgebildet – nicht eine Frau, so ginge das nicht –, kein schnelles Schuldeingeständnis für eine nicht begangene Tat. Doch wer mag der Mann wohl sein? Die Ermittlungen laufen auf Hochtouren, die Halterin hüllt sich in Schweigen – kurzerhand holt sich die Ermittlungsbehörde mit Amtshilfe vom Landesamt für Bürger und Ord-

nungsangelegenheiten (LABO) aus der Personalausweisdatei ein Foto von „ihm“, dem Ehemann der Halterin. Sie gleicht die Fotos ab, meint Ähnlichkeiten festzustellen: „Er könne der Täter wohl sein“ und schickt ihm den Anhörungsbogen. Der Beschuldigte beschwert sich über den schnellen Fotoabgleich, ohne ihn vorher anzuhören.

Noch im Jahr 2003 war zwischen dem Polizeipräsidenten in Berlin und dem Berliner Beauftragten für Datenschutz und Informationsfreiheit Einvernehmen darüber erzielt worden, dass Betroffene erst anzuhören seien, *bevor* Kopien ihrer Passfotos zu Abgleichszwecken besorgt werden können, damit der Bildabgleich nicht „hinter dem Rücken“ der Bürgerin oder des Bürgers geschehe – auch dann, wenn nicht die Halterin selbst, sondern deren Ehepartner das Fahrzeug, von dem die Ordnungswidrigkeit ausging, geführt hatte. In diesem Fall aus dem Jahr 2003 stand jedoch von Anfang an schon fest, dass der Ehepartner der Fahrzeugführer war und weitere Ermittlungen zur Identität eines anderen Täters nicht erforderlich waren. Hier aber konnte die Ermittlungsbehörde überhaupt nicht wissen, wo der männliche Täter zu suchen sein könnte. Fest stand nur, dass die Kraftfahrzeughalterin nicht die Täterin war. Ob statt ihrer einer der Freunde oder ihr Ehepartner als Täter in Frage käme, war völlig offen.

Es ist hinnehmbar, das Vorhandensein eines Ehepartners oder eines anderen nahen Verwandten zu ermitteln, um deren Täterschaft zu überprüfen. Denn es ist nicht unwahrscheinlich, dass z. B. ein Ehemann, wenn er eine Fahrerlaubnis hat, sich auch einmal an das Steuer des Fahrzeugs seiner Ehefrau setzt. Der hier erfolgte Fotoabgleich ist jedoch ein schwererer Eingriff als eine Anhörung. Der Angehörige einer Kraftfahrzeughalterin ist ebenso schutzwürdig wie die Halterin selbst, zu der der Bildabgleich vor einer Anhörung auch nicht „vorsorglich“ durchgeführt werden darf. Wenn die Polizei den Ehepartner (oder einen anderen nahen Angehörigen) als möglichen Täter einer Verkehrsordnungswidrigkeit ins Auge fasste, konnte sie ihn ebenso vor dem Bildabgleich anhören wie die Kraftfahrzeughalterin selbst. Es drohte auch keine Verjährung, weil mit der Zusendung des Anhörungsbogens an den verdächtigten Ehepartner die Verjährung unterbrochen wurde[101].

Auf unsere Anfrage hin teilte uns der Polizeipräsident in Berlin mit, dass es nur versehentlich versäumt worden sei, den in Verdacht geratenen Angehörigen auf die Möglichkeit eines Fotoabgleichs hinzuweisen und ihn zuvor anzuhören. Der Polizeipräsident sicherte zu, aufgrund dieses Vorfalls seine Verfahrensweise zu überprüfen und die erforderlichen Regelungen zu treffen, um ein solches Vorkommnis künftig zu vermeiden.

[101] vgl. § 32 Nr. 1 Ordnungswidrigkeitengesetz (OWiG)

Der Fotoabgleich ist gegenüber anderen Ermittlungsformen ein Eingriff, der erst dann verhältnismäßig ist, wenn sich geringere Eingriffe als nicht ausreichend erwiesen haben. Der Anhörungsbogen ist ein geeignetes Ermittlungsinstrument und deshalb bei Verkehrsdelikten vorrangig vor dem Fotoabgleich einzusetzen, erst recht dann, wenn ein Tatverdacht auf allgemeine Erwägungen statt auf konkrete Hinweise der Kraftfahrzeughalterin gestützt wird. Allerdings ist die beschuldigte Person vor der Durchführung des Fotoabgleichs anzuhören.

4.2.2 Ein verwunderlicher Fehlgriff

Ein Bürger teilte uns mit, er sei wegen eines Verkehrsverstoßes (Überschreitung der Geschwindigkeit) belangt worden. Er sei jedoch weder Beteiligter noch Halter des betreffenden Kraftfahrzeuges gewesen, er kenne das Fahrzeug und den betreffenden Halter gar nicht. Es sei ein Foto „geblitzt" worden, auf dem die Silhouette eines Fahrers männlichen Geschlechts und das polizeiliche Kennzeichen eines ihm unbekannten Fahrzeuges abgebildet sei. Darüber hinaus sei bereits eine andere Person angehört worden, die den Verkehrsverstoß zugegeben habe, jedoch weiblichen Geschlechts und gleichen Nachnamens wie er sei, was er durch Akteneinsicht habe feststellen können. Halter des Kraftfahrzeuges sei eine namensverschiedene männliche Person. Der Bürger bat um datenschutzrechtliche Unterstützung bei der Aufklärung der Personenverwechslungen und weiterer ermittlungstechnischer Fehlgriffe. Der Tatbestand, dass eine weibliche Person den Verkehrsverstoß zugegeben habe, obwohl offensichtlich ein Mann am Steuer saß, hatte bereits im Vorfeld unserer Tätigkeit zu erheblichen Irritationen bei den Ermittlungen geführt.

„Irrtümlich" – so der Polizeipräsident in Berlin – seien im Rahmen der Sachbearbeitung in der Bußgeldstelle die Personalien der weiblichen Person in ein Schreiben an das LABO eingetragen worden, mit dem eine Kopie des Lichtbildes aus der Ausweisdatei angefordert worden war. Bei der Sachbearbeitung im LABO sei ein weiterer Fehler unterlaufen, weil anstelle der angeforderten Lichtbildkopie der sich selbst bezichtigenden Kraftfahrzeugführerin die Lichtbildkopie des nicht beteiligten, aber namensgleichen Petenten übermittelt wurde. Der Bußgeldstelle sei dieser Fehler im Rücklauf nicht aufgefallen. Vielmehr habe sich der Irrtum aufgrund einer zufälligen Ähnlichkeit zwischen dem „geblitzten" Frontfoto und dem Lichtbild aus der Ausweisdatei verfestigt. Erst im gerichtlichen Verfahren, zu dem der zu Unrecht Beschuldigte einen Verteidiger hinzuziehen musste, seien die Irrtümer aufgedeckt und das Verfahren daraufhin eingestellt worden.

4.2

Der Zugriff auf die Daten des nicht beteiligten Bürgers und deren Übermittlung an die Bußgeldstelle waren datenschutzrechtlich unzulässig. Diesen Mangel hätte aber bereits das LABO erkennen können, da der Vorname des Bürgers nicht mit den angeforderten Daten übereinstimmte. Das LABO hätte das Antragsformular und die Daten zu den Bildern genauer lesen und auf Unterschiede des Geschlechts sowie auf Abweichungen der Vornamen untersuchen müssen.

Gleichwohl liegt die Verantwortung für diese Fehlerserie bei der Bußgeldstelle, denn sie wurde als verfahrensleitende Behörde tätig. Die Bußgeldstelle setzte zudem nach der Übermittlung des falschen Lichtbildes und des falschen Vornamens ihre eigene fehlerhafte Sachbearbeitung fort. Wir haben von einer Beanstandung dieser schwerwiegenden Fehlgriffe von gleich zwei Behörden nur deshalb abgesehen, weil die Bußgeldstelle sich bei der Aufklärung des Sachverhaltes als kooperativ erwies. Hervorzuheben ist allerdings, dass es der Einschaltung eines Verteidigers und des Berliner Beauftragten für Datenschutz und Informationsfreiheit bedurfte und dass dieser Fehler nicht im Wege einer gründlichen Sachbearbeitung und Fachaufsicht erkannt und vermieden wurde. Bereits im Einspruchsverfahren hätten die Namensunterschiede erkannt werden müssen.

Wir haben die Bußgeldstelle aufgefordert, uns zur Vermeidung künftiger Irrtümer und Fehler dieser Art über die mit dem LABO auszuhandelnden Maßnahmen zu berichten. Im Zuge dieser Ursachenbeseitigung regte der Polizeipräsident an, künftig bei Abweichungen oder Unstimmigkeiten bei Anfragen zwischen LABO und Bußgeldstelle die personenbezogenen Daten deutlich hervorzuheben. Es wurde erkannt, dass die Zusendung der Ausweiskopie in der bisherigen Form, mit aufgetragenen Bußgeldaktenzeichen, zu fehleranfällig sei. Zur Verbesserung wurde vorgeschlagen, den Vor- und Familiennamen von Betroffenen aus dem Anforderungsantrag zu übernehmen und nicht nur auf das Aktenzeichen abzustellen. In der Erwartung, dass diese Vorschläge das Erkennungsverfahren verbessern, haben wir die datenschutzrechtliche Überprüfung abgeschlossen und erwarten, dass bei den Massenverfahren wie Verkehrsverstößen unbeteiligte Bürgerinnen und Bürger nicht fälschlich mit lästigen Verfahren überzogen werden.

Der hier wegen eines Verkehrsverstoßes durchgeführte Abgleich mit der Ausweisfotodatei bestätigt die Richtigkeit unserer Auffassung, dass der Fotoabgleich erst nach der Anhörung ein geeignetes Mittel sein kann. Er muss mit Sorgfalt und Umsicht durchgeführt werden. Denn was nützen die schönsten Fotos, wenn sie den falschen Personen zugeordnet werden.

4.2.3 Die Menge macht's – Wie aus Knöllchensammlern Fußgänger werden

Eine Anwaltskanzlei trug für ihren Mandanten vor, von 2004 bis 2006 seien etwa 75 Verkehrsordnungswidrigkeiten ihres Mandanten festgestellt und gespeichert worden, die einer besonderen Auswertung unterzogen und deren Ergebnis an die Fahrerlaubnisbehörde übermittelt worden sei. Auf die Persönlichkeit des Mandanten und sein Verkehrsverhalten bezogen sei dessen charakterliche Eignung zum Führen von Kraftfahrzeugen langfristig und zielgerichtet, aber unzulässig überwacht und ausgewertet worden. Bei den meisten dieser Verkehrsverstöße handele es sich, neben anderen strittigen, überwiegend um Parkverstöße und gebührenpflichtige Verwarnungen, die stets pünktlich bezahlt worden seien.

Im Hinblick auf die Besorgnis des Rechtsanwalts des Kraftfahrzeughalters, hier habe eine umfassende, auf die Persönlichkeitsstruktur ausgerichtete Überwachungsmaßnahme stattgefunden, haben wir eine Überprüfung bei dem Polizeipräsidenten in Berlin – Referat Verkehrsordnungswidrigkeiten – eingeleitet. Uns wurde versichert, eine elektronisch gesteuerte Kraftfahrzeughalterüberwachung dieser Art finde nicht statt. Die technischen Voraussetzungen seien dafür nicht gegeben und eine solche Maßnahme werde schon aus grundsätzlichen Erwägungen auch seitens der Polizei abgelehnt. Vielmehr handele es sich bei solchen Vorfällen nur um „Zufallsfunde", die sich dann ergeben können, wenn Verkehrsverstöße über die Maßen häufig vorkommen.

Das Referat Verkehrsordnungswidrigkeiten und Bußgeldeinziehung hat die Befugnis, aus sachlichen Gründen im Einzelfall auch die abgegoltenen Verwarnungen für einen bestimmten Zeitraum abzurufen. Dieser Abruf kann im Einzelfall genutzt werden, um z. B. die Fahrtauglichkeit zu überprüfen. Die Fahrtauglichkeit wird vom LABO überprüft, das über die bekannt gewordenen Verkehrsverstöße zu informieren ist. Nach Prüfung durch das LABO kann die Fahrerlaubnis entzogen werden, wenn die Eignung des Fahrerlaubnisinhabers nicht mehr feststeht.

Wir haben allerdings mit der Polizei Einvernehmen darüber erzielt, dass die Daten aus bezahlten Verwarnungsgeldverfahren nur für einen angemessen begrenzten Zeitraum, nämlich für zwei Jahre, gespeichert und im Rahmen anderer Verfahren genutzt werden dürfen. Dem stehen keine datenschutzrechtlichen Bedenken entgegen. Die Entziehung der Fahrerlaubnis ist zwar kein Ordnungswidrigkeitenverfahren, die Übermittlung der erforderlichen Daten ist aber nach § 49 a Abs. 2 OWiG in Verbindung mit § 14 Abs. 1 Nr. 7 b Einführungsgesetz zum Gerichtsverfassungsgesetz gleichwohl zulässig. Die beträchtliche Anzahl von 75 Verkehrsverstößen – wenn auch zum großen Teil im Bereich des ruhenden Verkehrs – ließ die Fahrtauglichkeit als zweifelhaft erscheinen. Ausgangspunkt war

die Rechtsprechung des Bundesverwaltungsgerichtes[102], wonach zwar bei der Eignungsprüfung zur Fahrerlaubnis geringfügige Verkehrsordnungswidrigkeiten wie Verstöße gegen Vorschriften des ruhenden Verkehrs wegen ihres geringen Gefährdungspotenzials außer Betracht zu bleiben haben, davon jedoch Ausnahmen zu machen sind. Zuwiderhandlungen dieser Art schließen die Eignung zum Führen von Kraftfahrzeugen dann aus, wenn jemand die Rechtsordnung über den ruhenden Verkehr offensichtlich nicht anerkennt sowie nicht willens ist, Ordnungsvorschriften einzuhalten, und diese hartnäckig missachtet, wenn es seinen persönlichen Interessen entspricht. Dieser Auffassung haben sich die Berliner Verwaltungsgerichte[103] angeschlossen. Aus Gründen der Verhältnismäßigkeit kommt es darauf an, dass der letzte Regelverstoß nicht länger als zwei Jahre zurückliegt. Diese Frist ist angemessen, denn sie entspricht den gesetzlichen Tilgungsfristen für Ordnungswidrigkeiten.

Aus technischen Gründen wird diese Frist teilweise sogar noch unterschritten. Denn die Verfahren, die 14 Monate lang als abgeschlossen gelten (Verfahrenseinstellungen und bezahlte Vorgänge), werden wöchentlich maschinell in ein elektronisches Langzeitarchiv übertragen, d. h. elektronisch „ausgelagert“, auf das bei der Sachbearbeitung kein unmittelbarer Zugriff mehr möglich ist. Nur Führungskräften (für Verfahrensentscheidungen) und Beschäftigten der Bußgeldstelle und der Kassenstelle ist der Zugriff auf das Langzeit-Archiv zum Zweck der Suche und Zuordnung nachfolgend eingehender Schriftstücke und Zahlungen möglich. Nach drei Jahren im Langzeitarchiv werden allgemeine OWi-Sachen gelöscht, OWi-Sachen mit Verkehrsunfällen nach fünf Jahren, Gebührenverfahren nach Kfz-Umsetzung nach sechs Jahren ab Datum des Verfahrensabschlusses. Wir haben dieser Regelung zugestimmt.

Die datenschutzrechtlich nicht zu bemängelnde Nutzung abgegoltener „Verwarnungen“ für die Prüfung eines möglichen Führerscheinentzugs mag den Betroffenen schmerzhaft erscheinen. Soweit sich dies im zeitlich angemessenen Rahmen bewegt, ist es jedoch vom Gesetz so gewollt.

4.2.4 Die Luftsicherheitsüberprüfung als Karrierehemmer

Ein Petent musste sich einer der üblichen Luftsicherheitsüberprüfungen durch die Obere Luftfahrtbehörde Berlin-Brandenburg unterziehen: der

[102] BVerwG, DÖV 1977, 602, 603

[103] OVG Berlin, Beschluss v. 28. April 2005 – 1 S 8.04; VG Berlin, Urteil v. 12. September 2006 – VG 20 A 211.06

Zuverlässigkeitsüberprüfung nach § 7 Luftsicherheitsgesetz. Der Petent war im Juli 1993 wegen geheimdienstlicher Tätigkeit zu einer Freiheitsstrafe von einem Jahr auf Bewährung verurteilt worden. In einer Auskunft, die er selbst im September 2005 aus dem Bundeszentralregister über sich eingeholt hatte, war die Verurteilung nicht mehr enthalten. Das Landeskriminalamt hatte ihm im Juli 2006 mitgeteilt, er sei in den kriminalpolizeilichen personenbezogenen Datensammlungen nicht erfasst. Jedoch habe das Landeskriminalamt bereits im September 2005 der Oberen Luftfahrtbehörde ohne sein Wissen mitgeteilt, es lägen „Erkenntnisse" (gemeint war die Verurteilung von 1993) über ihn vor.

Unsere Überprüfung ergab, dass die dem Petenten im Juli 2006 erteilte Auskunft, er sei in den kriminalpolizeilichen personenbezogenen Datensammlungen nicht erfasst, falsch war. Denn zu Verratsdelikten existierten beim Polizeilichen Staatsschutz Aktenrückhalte, unter denen sich auch die Verurteilung des Petenten befand. Er hatte jedoch nach § 50 Abs. 1 Allgemeines Sicherheits- und Ordnungsgesetz (ASOG) in Verbindung mit § 16 Abs. 1 BlnDSG einen Anspruch auf eine wahrheitsgemäße Auskunft.

Anhaltspunkte, die eine Verweigerung der Auskunft nach § 50 Abs. 2 ASOG erlaubt hätten, lagen nicht vor. Die falsche Auskunft machte es dem Petenten unmöglich, die Zulässigkeit der fortdauernden Speicherung zu überprüfen. Problematisch war erst recht, dass das Urteil aus dem Jahr 1993 überhaupt noch vorhanden war. Denn das Urteil hätte spätestens im Jahr 2003/2004 gelöscht werden müssen, weil der Lauf der zehnjährigen Aufbewahrungsfrist spätestens 1994 begonnen hatte. Das ASOG schließt zwar eine längere Speicherungsfrist nicht aus, jedoch kommen Verlängerungen nur aufgrund besonderer Anlässe in Betracht, die in einer besonderen Begründung hätten dokumentiert werden müssen. Diese Dokumentationspflicht ergibt sich aus § 4 Prüffristenverordnung. Eine Begründung sei aufgrund eines „Büroversehens unterblieben", wurde uns mitgeteilt. Die Aufbewahrung des Urteils war demnach unzulässig. Zwar sind nach § 5 Abs. 3 Nr. 2 Verordnung zur Regelung des Verfahrens der Zuverlässigkeitsüberprüfungen auf dem Gebiet des Luftverkehrs vom 8. Oktober 2001 (LuftVZÜV) auch Erkenntnisse zu überprüfen, die länger als zehn Jahre zurückliegen, wenn Zweifel an der Zuverlässigkeit der zu überprüfenden Person bestehen. Als „sonstige Erkenntnis" kann zwar der „*Verdacht der Tätigkeit für fremde Nachrichtendienste*"[104] in Betracht kommen. Die Verwertung und Nutzung solcher Daten ist datenschutzrechtlich jedoch nur dann zulässig, wenn die Speicherung und Aufbewahrung zulässig waren. Dies war nicht der Fall.

[104] § 5 Abs. 3 Nr. 2 LuftVZÜV

4.2

Wir haben bei unserer Beanstandung dieses gravierenden Verstoßes gegen datenschutzrechtliche Bestimmungen den Polizeipräsidenten und die Senatsverwaltung für Inneres aufgefordert sicherzustellen, dass alle Verfahrensdaten, die ohne besonderen Anlass und ohne die erforderliche rechtliche Begründung über die gesetzlichen Fristen der Prüffristenverordnung hinaus gespeichert sind, gelöscht werden. Wir haben empfohlen, bis dahin keine Auskünfte oder Mitteilungen aus diesen Dokumenten an die Obere Luftfahrtbehörde Berlin-Brandenburg oder andere Behörden zu erteilen – es sei denn, der besondere Anlass für eine zulässige Verlängerung der Speicherungsfrist sei im Einzelfall nachweislich dokumentiert und begründet. Wir hatten auch angeregt, die Folgen der unzulässigen Speicherung und Auskunft für den Betroffenen zu beseitigen. Glücklicherweise hatte sich jedoch die unzulässig gespeicherte und übermittelte Information auf die Entscheidung der Luftsicherheitsbehörde nicht nachteilig ausgewirkt.

Die Senatsverwaltung für Inneres und der Polizeipräsident in Berlin haben uns zugesichert, die wegen Fristüberschreitung unzulässig gespeicherten Datenbestände zu löschen bzw. zu vernichten und künftig für eine einwandfreie Dokumentation und Anlassbegründung bei den verlängerten Aufbewahrungsfristen zu sorgen.

4.2.5 Sicherheitskonzept für das Führerschein-Register

Seit Ende der 80er Jahre verfolgen wir den Weg des Verfahrens Führerschein-Register (FüReg) im Landesamt für Bürger- und Ordnungsangelegenheiten (LABO). Das Verfahren gliedert sich in die Teile Führerscheinwesen und Konzessionen. Mit dem Verfahren erfolgte damals eine Erstautomatisierung der bis dahin noch als Papierkartei geführten Führerscheinkartei. Neben einer Übertragung der auf Karteikarten registrierten Daten in ein automatisiertes Führerschein-Register konnte so die Sachbearbeitung bei den anfallenden Vorgängen durch ein Datenverarbeitungssystem unterstützt werden (z. B. durch das selbständige Erstellen von Schreiben mithilfe von Textbausteinen).

Im letzten Jahr erfolgten mit der Umstellung auf einen Rechnerverbund und mit dem Einsatz einer neuen Datenbanksoftware wesentliche Änderungen an dem Verfahren. Damit wurde die Überarbeitung und Fortschreibung des vorhandenen Sicherheitskonzeptes (SiKo) erforderlich. Dieses wurde erarbeitet und uns zur Stellungnahme vorgelegt. Das ansonsten professionell erstellte SiKo enthielt noch Mängel, die Risiken zur Verfügbarkeit des Systems betrafen. So war der Einbruchs- und Feuerschutz für den Serverraum, der wichtige Hardware- und Infrastrukturkomponenten erhält, durch die Verwendung einer einfachen Bürotür unzureichend gewährleistet, zumal auch Brandmelder fehlten. Da die Hardware teilwei-

se auf den Boden gestellt war, wurde sie auch gegen mögliche Wassereinbrüche nicht hinreichend geschützt.

Die Aufträge zur Abstellung der Mängel sind zum Teil bereits vergeben worden.

Welche Risiken für die IT-Sicherheit in einem IT-Verfahren und der dafür erforderlichen IT-Infrastruktur verborgen sind, kann nur aufgrund eines Sicherheitskonzeptes beurteilt werden. Dies allerdings reicht nicht für die Gewährleistung von IT-Sicherheit. Die als notwendig erkannten Maßnahmen zur Risikobeseitigung bzw. Risikominimierung müssen auch getroffen werden.

4.2

5 Justiz

5.1 Neuregelung zur Telekommunikationsüberwachung mit ungewisser „Haltbarkeit"

Trotz vielfacher Vorfeldkritik unter anderem von den Datenschutzbeauftragten des Bundes und der Länder[105] an den Vorentwürfen ist am 21. Dezember 2007 das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG verabschiedet worden[106]. Das Gesetz sieht umfangreiche Änderungen insbesondere zum Telekommunikationsgesetz (TKG)[107] und zur Strafprozessordnung (StPO) vor.

Die einhellige Kritik der Datenschutzbeauftragten und ihre Aufforderung, stattdessen verhältnismäßige Eingriffsregelungen zu schaffen, hat der Gesetzgeber weitgehend unbeachtet gelassen. Besonders ist es zu kritisieren, dass der Gesetzgeber nicht die Chance ergriffen hat, den verfassungsrechtlichen Schutz des Kernbereichs privater Lebensgestaltung einheitlich für alle verdeckten Ermittlungsmaßnahmen einzuführen. § 160 a Abs. 1 StPO sieht vor, dass eine Ermittlungsmaßnahme allein gegen Strafverteidiger, Geistliche und Abgeordnete grundsätzlich unzulässig ist. Ausnahmen sind nur vorgesehen, wenn die geschützten Geheimnisträger selbst einer einschlägigen Straftat verdächtig sind. In diesem Zusammenhang ist es nicht nachvollziehbar, dass die Gesetzesänderung andere Berufsgeheimnisträger wie Ärzte, Journalisten und Rechtsanwälte nicht in den besonderen Schutz vor Ermittlungsmaßnahmen einbezieht. Eine entsprechende Initiative des Landes Berlin vom 27. November 2007[108] fand im Bundesrat keine Mehrheit.

Nur zwei Wochen nach Inkrafttreten dieser unbefriedigenden Regelung wurden Pläne des Bundesinnenministeriums bekannt, für das Bundeskriminalamt eine Befugnis zur weitgehenden präventiven Überwachung der Telefongespräche von Strafverteidigern, Geistlichen und Abgeordneten zu schaffen. Man fragt sich, welche „Haltbarkeit" gesetzliche Begrenzungen staatlichen Handelns heute noch haben. Außerdem sehen die Regelungen zur Vorratsdatenspeicherung im TKG schon heute vor, dass die Verkehrsdaten über solche Telefonate, die auch dem Telekom-

[105] vgl. Entschließung der 73. Konferenz v. 8./9. März 2007 sowie Entschließung v. 8. Juni 2007, Dokumentenband 2007, S. 9 und 16

[106] BGBl. I 2007, 3198

[107] zur Änderung des TKG vgl. 12.1

[108] vgl. BR-Drs. 798/2/07

munikationsgeheimnis unterliegen, bereits ab dem 1. Januar 2008 lückenlos für 6 Monate zu speichern sind.

Demgegenüber ist die Liste der aus datenschutzrechtlicher Sicht erfreulichen Änderungen der strafverfahrensrechtlichen Bestimmungen im Gesetz vom 21. Dezember 2007 kurz geraten.

Positiv zu bewerten ist die Festschreibung in § 100 a Abs. 1 Nr. 2 StPO, dass die Telekommunikationsüberwachung nur zulässig ist, wenn die verfolgte Tat auch im Einzelfall schwerwiegend ist. Wie bisher ist die Anordnung einer Telekommunikationsüberwachung nur zulässig, wenn der Verdacht einer „Katalogstraftat" erfüllt ist. Dieser Katalog von Straftaten ist nun in § 100 a Abs. 2 StPO vorgesehen. Die Neueinführung des Tatbestandsmerkmals der „schwerwiegenden Straftat" kann nicht darüber hinwegtäuschen, dass der Straftatenkatalog erheblich ausgeweitet worden ist. Gleichzeitig hat der Gesetzgeber die Möglichkeit versäumt, im nennenswerten Umfang überflüssige Befugnisse zu reduzieren.

Die Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen wird nicht zu der erforderlichen Reduzierung, sondern zu einer Ausweitung derartiger einschneidender Maßnahmen führen.

5.2 Strafvollzug

5.2.1 Jugendstrafvollzugsgesetz

Das Bundesverfassungsgericht hat 2006[109] *festgestellt, dass die inhaltliche Ausgestaltung des Strafvollzugs für jugendliche und ihnen in der Entwicklung gleichstehende heranwachsende Straftäter besonderen verfassungsrechtlichen Anforderungen unterliegt, die auch für die Reichweite des Erfordernisses gesetzlicher Regelungen im Jugendstrafvollzug von Bedeutung sind. Insbesondere darf der Gesetzgeber „die Frage, inwieweit Besonderheiten, die einfachgesetzlich im Erziehungsgedanken des Jugendgerichtsgesetzes zum Ausdruck gebracht sind, einer Ordnung des Jugendstrafvollzugs nach den Regeln des Erwachsenenstrafvollzugs entgegenstehen, ... nicht den Gerichten zur Beantwortung ... überlassen, sondern musste sie selbst beantworten".*

[109] Urteil v. 31. Mai 2006 - 2 BvR 1673/04 und 2 BvR 2402/04, vgl. BVerfGE 116, 69 ff.

Der Senat von Berlin leitete dem Abgeordnetenhaus daraufhin den Entwurf eines Gesetzes über den Vollzug der Jugendstrafe in Berlin – Berliner Jugendstrafvollzugsgesetz (JStVollzG Bln) zu[110]. Dieser Gesetzentwurf hatte ausweislich seiner Begründung die Zielsetzung, den verfassungswidrigen Zustand des Jugendstrafvollzugsrechts zu beenden.

Wir haben versucht, auf eine datenschutzfreundliche Regelung des Jugendstrafvollzugsrechts hinzuwirken. Erfreulicherweise hat der Gesetzgeber einige unserer Anregungen aufgegriffen.

Beispielsweise wurde die Regelung gestrichen, wonach bei der Aufnahme von jugendlichen Gefangenen andere, „zuverlässige" Gefangene hinzugezogen werden können, um bei „unüberwindbaren sprachlichen Verständigungsschwierigkeiten" als Dolmetscher zu dienen. Der Gesetzgeber berücksichtigte dabei unseren Einwand, dass Gefangene sich häufig darüber beschweren, dass Mitgefangene wie auch immer erlangtes Sonderwissen über sie in der Anstalt verbreiten oder sie mit der Weitergabe solcher Informationen bedrohen.

Auch sah der Gesetzentwurf ursprünglich die für die Betroffenen bürokratische Regelung vor, nach ihrer Entlassung erkennungsdienstliche Daten wie Fingerabdrücke, Lichtbilder usw. nur auf Antrag zu vernichten. Unserer Empfehlung entsprechend ist nun vorgesehen, dass die Daten von Amts wegen gelöscht werden, sobald die betroffenen Strafgefangenen aus der Haftanstalt entlassen worden sind.

In einigen wesentlichen Punkten wurden wir allerdings nicht gehört. Insbesondere haben wir darauf hingewiesen, dass die jugendlichen Gefangenen auf ein Leben in sozialer Verantwortung vorzubereiten sind. Das Recht auf informationelle Selbstbestimmung und ihm verwandte Grundrechte dienen im besonderen Maße dazu, dem einzelnen Menschen Raum für Privatsphäre zu geben, innerhalb dessen er seine Individualität entwickeln und wahren kann[111]. Seine Beachtung trägt damit auch in besonderem Maße zur Persönlichkeitsentwicklung der jungen Gefangenen bei. Diese befinden sich im Rahmen des Vollzugs in einem Zustand der nahezu lückenlosen Überwachung. Es ist im Wesen des Strafvollzugs begründet und auch aus datenschutzrechtlicher Sicht im Grundsatz nicht zu kritisieren.

Umso dringlicher ist allerdings die Frage zu beantworten, wie der Schutz des absolut zu schützenden Kernbereichs privater Lebensgestaltung zu gewährleisten ist, wie er gemäß der ständigen Rechtsprechung des Bundesverfassungsgerichts

[110] Abghs.-Drs. 16/0677
[111] z. B. BVerfGE 79, 256, 268

jedem Menschen - also auch den jugendlichen Gefangenen - zuzubilligen ist. Das Bundesverfassungsgericht hat insoweit festgestellt, dass zur Menschenwürde aus Art. 1 Abs. 1 GG die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung gehört, der einer Abwägung mit anderen staatlichen Interessen nicht zugänglich ist und in den nicht eingegriffen werden darf[112].

Unsere konkret gefassten Anregungen, Schutzregelungen des Kernbereichs privater Lebensgestaltung in das Jugendstrafvollzugsgesetz einzufügen, nahm der Gesetzgeber nicht auf.

Erfreulicherweise bestand bei der Verabschiedung des Gesetzes im Parlament aber Einigkeit darüber, dass künftig jedenfalls im Jugendstrafvollzug das Informationsfreiheitsgesetz gilt. Für den Erwachsenenstrafvollzug kann nichts anderes gelten. Damit ist eine jahrelange Kontroverse mit der Senatsverwaltung für Justiz[113] i. S. d. Informationsfreiheit beigelegt worden.

Das neue Jugendstrafvollzugsgesetz enthält zwar die von Verfassungs wegen gebotenen Rechtsgrundlagen für den Jugendstrafvollzug in Berlin; die Chance für weitgehende Sicherungen der Privatsphäre von jugendlichen Gefangenen blieb allerdings ungenutzt. Immerhin ist jetzt geklärt, dass auch im Strafvollzug das Informationsfreiheitsgesetz gilt.

5.2.2 Der Gefangene als ungewollter Medienstar?

Ein ehemaliger Gefangener der Justizvollzugsanstalt Moabit beschwerte sich bei uns darüber, dass die Justizvollzugsanstalt eine Website betreibt, auf der er bei der Arbeit in der anstaltseigenen Buchbinderei abgebildet gewesen sei. Er habe weder zur Ablichtung seiner Person noch zur Veröffentlichung seines Abbildes sein Einverständnis erteilt. Als er seinen Gruppenleiter über diesen Sachverhalt informiert habe, sei das Foto von der Website entfernt worden.

Diese Darstellung steht in einem gewissen Widerspruch zu der Darstellung der Leitung der Justizvollzugsanstalt. Sie hat unter anderem ausgeführt, es treffe zu, dass bis Anfang Juli 2007 auf einer über die Homepage der Senatsverwaltung für Justiz (berlin.de) verlinkten Teilveröffentlichung des Webinhalts der JVA Moabit

[112] BVerfGE 109, 279 ff., BVerfGE 113, 348 ff.
[113] zuletzt JB 2005, 4.9.3

unter dem Titel „Buchbinderei“ ein Bild eingestellt gewesen sei, auf dem der Petent im hinteren Bildbereich zusammen mit zwei anderen Gefangenen schemenhaft zu erkennen gewesen sei. Würden Bildaufnahmen dieser Art von Gefangenen oder Bediensteten zum Zweck der Veröffentlichung genehmigt, so sei das Einverständnis der betreffenden Personen zwingend einzuholen.

Das ins Internet eingestellte Bild des Petenten sei während seines Aufenthalts in der Justizvollzugsanstalt Moabit zwischen 2001 und 2003 aufgenommen worden. Es könne jedoch nicht mehr mit Sicherheit festgestellt werden, ob der Petent seinerzeit die Veröffentlichung autorisiert habe. Hiervon sei wegen der beschriebenen Praxis auszugehen. Hierfür spreche auch die Tatsache, dass der Petent seit dem ersten Internetauftritt der Justizvollzugsanstalt Moabit im Jahr 2003 online gestellt gewesen sei und dies von ihm bisher nicht beanstandet worden sei. Auf unsere Nachfrage hin hat die Justizvollzugsanstalt erklärt, etwaige Einverständniserklärungen zur Weitergabe von Bilddaten würden sowohl bei Gefangenen als auch bei allen Personen in der Anstalt zum „anlassgebenden Vorgang“, nicht zur Gefangenenpersonalakte bzw. Personalakte genommen. Der anlassgebende Vorgang sei aber mit vertretbarem Aufwand nicht mehr aufzufinden.

Nach den Angaben der verantwortlichen Stelle ist es letztlich nicht mehr zu klären, ob der Petent seine Einwilligung in die Veröffentlichung seines Abbildes im Internet erteilt hat. Der Sachverhalt kann insoweit mit den beschränkten Ermittlungsbefugnissen des Berliner Beauftragten für Datenschutz und Informationsfreiheit nicht aufgeklärt werden.

Wir haben festgestellt, dass entsprechend den einander widersprechenden Sachvorträgen des Petenten und der Justizvollzugsanstalt praktisch nur zwei Sachverhalte denkbar sind, die beide jeweils einen datenschutzrechtlichen Mangel offenbaren:

Soweit die Justizvollzugsanstalt entgegen der von ihr dargestellten Übung keine schriftliche Einwilligung des Petenten eingeholt hat, hat sie gegen § 6 Abs. 4 Satz 1 Berliner Datenschutzgesetz (BlnDSG) verstoßen. Nach dieser Vorschrift bedarf eine datenschutzrechtliche Einwilligung der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Besondere Umstände, die eine andere Form als die Schriftform rechtfertigen könnten, sind nicht ersichtlich. Insbesondere kann aus einer mutmaßlichen Duldung der Veröffentlichung durch den Petenten keine wirksame Einwilligung abgeleitet werden, weil anderenfalls das gesetzliche Schriftformgebot sinnlos wäre.

5.2

Sofern – wie es die Justizvollzugsanstalt vorliegend vermutet – zwar eine schriftliche Einwilligung des Petenten in die Veröffentlichung seines Abbildes im Internet eingeholt worden ist, die Erklärung des Petenten aber nicht mehr auffindbar ist, liegt ein Mangel i. S. d. § 5 Abs. 1 Satz 1 BlnDSG vor. Danach hat die verantwortliche Stelle durch technische und organisatorische Maßnahmen sicherzustellen, dass das BlnDSG und sonstige datenschutzrechtliche Vorschriften ausgeführt werden (können). Dem ist die bisherige Aktenführung nicht gerecht geworden. Denn die Justizvollzugsanstalt hat es verabsäumt, durch organisatorische Maßnahmen sicherzustellen, dass die Rechtsgrundlage der Verarbeitung auch nach einiger Zeit zuverlässig benannt werden kann. Einmal abgesehen davon, dass sie selbst als verantwortliche Stelle nicht mit vertretbarem Aufwand eine hinreichende Rechtsgrundlage für die Veröffentlichung nachweisen kann, könnte sie dem Petenten nicht gemäß § 16 Abs. 1 Nr. 2 BlnDSG konkret Auskunft über die Rechtsgrundlage der Verarbeitung geben.

Weiterhin müsste sie in Bezug auf die Personalakten der Beschäftigten ihre Pflicht erfüllen, diesen jederzeit Einsicht in die *vollständige* Personalakte gewähren zu können[114]. Erklärungen, mit denen Beschäftigte ihre Einwilligung in eine Datenverarbeitung erteilen, gehören deshalb wenigstens in Kopie in die Personalakte. Aus datenschutzrechtlicher Sicht sollten diese Maßstäbe auch auf die Handhabung von Gefangenenakten übertragen werden.

Die Leitung der Justizvollzugsanstalt hat uns mittlerweile mitgeteilt, dass sie künftig unserer Empfehlung folgen wird, datenschutzrechtliche Einwilligungserklärungen von Gefangenen zumindest auch in der Gefangenenakte abzulegen.

Holt die Justizvollzugsanstalt von Gefangenen die Einwilligung ein, ihre personenbezogenen Daten zu Zwecken der Außendarstellung zu veröffentlichen, gehört eine Abschrift der Einwilligungserklärung in die Gefangenenakte.

5.2.3 Untersuchungsgruppe Medikamentenversorgung

Vor dem Hintergrund der Presseberichterstattung über angebliche Missstände beauftragte die Senatorin für Justiz eine Untersuchungsgruppe, die Frage der ordnungsgemäßen Medikamentenversorgung im Berliner Strafvollzug zu untersuchen. Die Untersuchungsgruppe setzte sich neben Bediensteten des Landes Berlin auch aus Beschäftigten zusammen, die nicht in einem Beamten- bzw. Anstellungsverhältnis zum Land Berlin stehen.

[114] vgl. § 56 c Abs. 1 Landesbeamtengesetz (LBG)

Damit ist die datenschutzrechtliche Frage aufgeworfen, inwieweit diesen Mitgliedern der Untersuchungsgruppe Einsicht in Unterlagen mit personenbezogenen Daten gewährt werden durfte.

Eine Übermittlung der erforderlichen personenbezogenen Daten von der Justizvollzugsanstalt an die Senatsverwaltung für Justiz zu Aufsichtszwecken ist datenschutzrechtlich nicht zu kritisieren, soweit dies zur Wahrnehmung von Aufsichtszwecken durch die Senatsverwaltung erforderlich gewesen ist.

Die Zulässigkeit einer Übermittlung zu Aufsichtszwecken an die Senatsverwaltung für Justiz bedeutet allerdings nicht notwendig, dass auch einer von ihr eingesetzten Untersuchungsgruppe dieselben Daten offenbart werden dürfen, wenn dieser Gruppe Personen angehören, die weder Bedienstete des Landes Berlin sind noch zur Senatsverwaltung für Justiz abgeordnet wurden. Eine Vorschrift, die eine Übermittlung von Patienten- und Mitarbeiterdaten im Wege der Akteneinsicht an die Untersuchungsgruppe ermöglichen würde, existiert genauso wenig wie ein Gesetz, in dem die Errichtung der Untersuchungsgruppe überhaupt vorgesehen ist. Sie als bloße Verwaltungshelferin der Senatsverwaltung zu betrachten, scheidet ebenfalls aus, weil die Untersuchungsgruppe ihre Aufgaben unabhängig von Weisungen wahrnehmen sollte.

§ 151 Abs. 2 des Strafvollzugsgesetzes sieht ausdrücklich vor, dass an der Aufsicht über das Arbeitswesen sowie über die Gesundheitsfürsorge und die sonstige fachlich begründete Behandlung der Gefangenen *eigene* Fachkräfte zu beteiligen sind. Sofern die Aufsichtsbehörde nicht über eigene Fachkräfte verfügt, erlaubt diese Vorschrift nicht etwa eine Datenweitergabe an Dritte, sondern lediglich eine „*fachliche Beratung*“. Eine fachliche Beratung setzt keine Weitergabe personenbezogener Daten voraus.

Erst recht dürfen Patientendaten, bei denen über datenschutzrechtliche Vorschriften hinaus noch auf die besondere berufliche Schweigepflicht Rücksicht zu nehmen ist, einer Untersuchungsgruppe mit externen Fachkräften nicht offenbart werden. Nur soweit die Untersuchungsgruppe mit anonymisierten Daten gearbeitet hat, war dies datenschutzrechtlich unproblematisch.

Es ist nachvollziehbar, dass die Senatsverwaltung bestrebt ist, wahrscheinlich bestehende Mängel im System des Maßregelvollzugs durch Hinzuziehung externer Experten zu untersuchen und Vorschläge zu ihrer Behebung machen zu lassen. Auch außerhalb Berlins sind in jüngster Vergangenheit in ähnlichen Situationen wiederholt "Sonderermittler" damit beauftragt worden, problematische Vorgänge in der Verwaltung aufzuklären. Dies kann aber – soweit dabei personenbezogene

Daten verwendet werden sollen – immer nur unter Beachtung des geltenden Datenschutzrechts geschehen.

Die Senatsverwaltung als Fachaufsichtsbehörde kann zur Wahrnehmung ihrer Aufgaben die erforderlichen personenbezogenen Daten verarbeiten, indem sie sich geeignete Bedienstete anderer Behörden abordnen lässt und ihnen zeitweise einen Dienstposten mit klarem Arbeitsauftrag und mit allen dienstrechtlichen Pflichten überträgt.

Personenbezogene Daten dürfen nur von solchen Personen und Stellen verwendet werden, die aufgrund ihrer dienstlichen Stellung oder einer besonderen gesetzlichen Bestimmung dazu befugt sind. Das gilt auch bei der Untersuchung von Missständen in der Verwaltung.

5.2.4 Eine Frage der Ehre

Bei der Vorstellung des Abschlussberichts der Untersuchungsgruppe zur Medikamentenversorgung im Berliner Strafvollzug[115] *schilderte der Vorsitzende der Untersuchungsgruppe, die den Bericht verfasst hatte, Mängel bei der Medikamentenversorgung der Gefangenen in der Justizvollzugsanstalt Moabit. Aufgrund der Pressekonferenz erschienen Meldungen in der Tagespresse, wonach die Moabiter Gefängnisverwaltung immer wieder auf Mängel hingewiesen habe, bei der verantwortlichen Ärzteschaft aber auf taube Ohren gestoßen sei. Die Verantwortlichen in der „Knastarzt-Geschäftsstelle" hätten offenbar mit Rückendeckung der Senatsverwaltung für Justiz gehandelt. „Wenn ein Arzt zum Telefon greift und den Staatssekretär anruft, ist man als Gefängnisverwaltung zweiter Sieger"*[116]*. Überdies sprach der Vorsitzende der Untersuchungsgruppe von einem „Organisationschaos" und die Senatorin für Justiz von „eklatanten Missständen". In einer Tageszeitung wurden diese Missstände mit einem angeblichen privaten Netzwerk in Verbindung gebracht, „das kurze Wege garantiert": ein „persönliches Dreiecksverhältnis zwischen dem entlassenen Staatssekretär, seiner Ehefrau, die als leitende Anstaltsärztin tätig war, und dem Leiter für die gesamte medizinische Versorgung in den Berliner Haftanstalten"*[117].

[115] vgl. 5.2.1
[116] taz v. 17. April 2007
[117] Tagesspiegel v. 18. April 2007

Der ehemalige Staatssekretär verlangte daraufhin Einsicht in die Akten der Untersuchungsgruppe, in denen er die Urheber der genannten Behauptungen zu finden hoffte, die er für sich und seine Ehefrau als rufschädigend empfand. Die Senatsverwaltung für Justiz lehnte seinen Antrag auf Akteneinsicht insoweit ab, als in den entsprechenden Vermerken die Namen der befragten Mitarbeiter geschwärzt wurden. Zur Begründung berief sich die Justizverwaltung auf ihre Fürsorgepflicht gegenüber diesen Mitarbeitern und darauf, dass ihnen vertrauliche Behandlung ihrer Angaben zugesichert sei. Daraufhin wandte sich der ehemalige Staatssekretär an den Berliner Beauftragten für Datenschutz und Informationsfreiheit. Auf dessen Intervention hin verwies die Justizverwaltung darauf, dass ihr Ablehnungsbescheid inzwischen bestandskräftig geworden sei.

Dieses Vorgehen der Justizverwaltung war als Verstoß gegen das Berliner Datenschutzgesetz zu beanstanden.

Zunächst ging die Senatsverwaltung zu Unrecht davon aus, dass hier das Informationsfreiheitsgesetz des Landes Berlin anzuwenden sei. Dagegen hat der Petent einen Anspruch auf Einsicht in Akten, die Informationen zu seiner Person enthalten, nach dem Berliner Datenschutzgesetz. Dieser wäre nur ausgeschlossen, wenn ihm überwiegende Geheimhaltungsinteressen Dritter aus zwingenden Gründen entgegengestanden hätten. Dies war aber nicht der Fall. Der ehemalige Staatssekretär hat ein berechtigtes Interesse daran festzustellen, wer Behauptungen über ihn aufgestellt oder Gerüchte wiedergegeben hat, die er als ehrenrührig und rufschädigend empfinden musste. Er und seine Ehefrau wurden aufgrund der öffentlichen Wiedergabe der fraglichen Äußerungen zum Gegenstand einer herabsetzenden Presseberichterstattung.

Weder die Tatsache, dass die befragten Personen, deren Identifizierung der Staatssekretär verlangt, ihre Angaben in dem Glauben gemacht haben, dass sie vertraulich behandelt würden, noch der Umstand, dass die fraglichen Vermerke im Hinblick auf mögliche dienstrechtliche Verfehlungen ausgewertet werden sollten, rechtfertigten die Geheimhaltung der Namen gegenüber dem Petenten. Denn die Zeugen hätten – falls es zu dienstrechtlichen Verfahren kommen sollte – nur in eng begrenzten Ausnahmefällen einen Anspruch auf Wahrung ihrer Identität. Zu diesen Ausnahmefällen zählt nach der Rechtsprechung des Bundesverwaltungsgerichts auch die Korruption, weil diese besondere Kriminalitätsform effektiv nur bekämpft werden kann, wenn die Identität von Informanten geheim gehalten wird. Um derartige Vorwürfe ging es aber im Fall des Petenten offenbar nicht. Falls sie erhoben worden wären, so hätten sie in einem geordneten Verfahren unter Einbeziehung

des ehemaligen Staatssekretärs geklärt werden müssen, bevor die ihnen zugrunde liegen Anschuldigungen öffentlich gemacht wurden.

Werden Anschuldigungen gegen eine Person erhoben und hat die Verwaltung diese Anschuldigungen personenbezogen dokumentiert, dann ist der betroffenen Person in aller Regel uneingeschränkt Einsicht in diese Dokumente zu gewähren. Anonymität darf die Verwaltung Hinweisgebern nur bei der Verfolgung bestimmter Kriminalitätsformen zusichern, die sonst nicht effektiv möglich wäre (z. B. Korruption). Selbst derartige Vorwürfe müssen aber in einem geordneten Verfahren unter Einbeziehung der Betroffenen geklärt werden, bevor sie öffentlich gemacht werden.

6 Finanzen

6.1 Das Ende der Lohnsteuerkarte

Mit dem Entwurf des Jahressteuergesetzes 2008[118] beabsichtigt die Bundesregierung, die bisherige Lohnsteuerkarte ab dem Jahr 2011 durch ein elektronisches Abrufverfahren (ElsterLohn II) beim Bundeszentralamt für Steuern (BZSt) abzulösen. Die Einführung dieses Verfahrens ist mit massiven datenschutzrechtlichen Risiken verbunden.

Durch den Gesetzentwurf[119] soll die anlässlich der Einführung der Steueridentifikationsnummer beim BZSt eingerichtete Datenbank um weitere sensitive Daten (z. B. die Religionszugehörigkeit, Ehepartner und Angaben über Steuerklassen und Freibeträge) ergänzt werden. Dabei sollen die lohnsteuerrechtlich bedeutsamen melderechtlichen Daten dem BZSt unabhängig davon mitgeteilt werden, ob Betroffene lohnsteuerpflichtig sind oder nicht. Diese vielfache Datenspeicherung auf Vorrat widerspricht dem verfassungsrechtlichen Erforderlichkeitsgrundsatz.

Durch die Erweiterung des Datenkataloges verfügt das BZSt zukünftig über einen aktuellen bundesweiten Datenbestand, in dem alle Bürgerinnen und Bürger mit ihren wesentlichen Meldedaten, Bankkontostamm- und Steuerdaten erfasst sind. Es ist davon auszugehen, dass dieser Datenpool auch für andere Behörden (z. B. Sozialleistungsträger, Strafverfolgungsbehörden usw.) von großem Interesse ist. Zahlreiche Beispiele aus der Vergangenheit – wie z. B. der Datenbestand im Mautverfahren – haben gezeigt, dass Daten, die zunächst nur für einen eingeschränkten Zweck gespeichert werden dürfen, später auch für andere Zwecke genutzt werden. Eine derartige nachträgliche Zweckerweiterung ist auch für den Datenbestand beim BZSt zu erwarten.

Nach § 39 f. Abs. 4 EStG-E hat der Arbeitnehmer seinem Arbeitgeber bei Eintritt in das Dienstverhältnis zum Zweck des Abrufs der Lohsteuerabzugsmerkmale seine Identifikationsnummer sowie den Tag der Geburt mitzuteilen. Der Arbeitgeber hat die Lohnsteuerabzugsmerkmale beim BZSt abzurufen und in das Lohnkonto für den Arbeitnehmer zu übernehmen. Für den Datenabruf hat sich der Arbeitgeber gegenüber dem BZSt zu authentifizieren und seine Wirtschaftsidentifikationsnummer sowie die Identifikationsnummer und den Tag der Geburt des Arbeitnehmers mitzuteilen. Ob dieses Authentifizierungsverfahren tatsächlich geeignet ist, einen missbräuchlichen Zugriff auf die Daten auszuschließen, ist zweifelhaft.

---

[118] BT-Drs. 16/6290

[119] § 39 f. Abs. 2 und 3 Einkommensteuergesetz-Entwurf (EStG-E)

Angesichts der bestehenden datenschutzrechtlichen Risiken haben die Datenschutzbeauftragten des Bundes und der Länder den Bundestag und den Bundesrat aufgefordert[120], das Vorhaben der Umstellung auf ein elektronisches Verfahren mit dem Jahresteuergesetz 2008 nicht zu beschließen.

6.2 Die Finanzverwaltung schlägt zurück: Steuerdaten im Internet

In den Jahren 2003 und 2004 befasste sich der Petitionsausschuss des Abgeordnetenhauses mit Eingaben von Beamten eines Finanzamts, die sich über Mobbing in ihrem Amt beschwert hatten. Ende 2004 erklärte der Vorsitzende des Petitionsausschusses gegenüber der Presse, dass nach seiner Einschätzung diese Mobbingvorwürfe berechtigt seien. Bereits zuvor hatte die Berliner Finanzverwaltung gegen drei Mitglieder des Petitionsausschusses sowie gegen einen Rechtsanwalt, der einen der Petenten vertrat, in zwei Fällen Betriebsprüfungen, in einem Fall eine Nachschau und in einem Fall eine Erinnerung an die Abgabe der Steuererklärung veranlasst. Im Juli 2007 wurde in einer Zeitschrift der Vorwurf erhoben, die Finanzverwaltung habe gegen die betroffenen Mitglieder des Petitionsausschusses Betriebsprüfungen als Tiefenprüfungen durchgeführt, um sich für die Rüge des Petitionsausschusses aufgrund der Mobbingvorwürfe zu revanchieren. Zum Teil erhoben die betroffenen Abgeordneten auch persönlich den Vorwurf in den Medien, die Finanzverwaltung habe sie schikanieren wollen.

Mit einer Presseerklärung vom 17. August 2007 wies die Finanzverwaltung diese Vorwürfe zurück und lehnte zunächst eine Offenlegung weiterer Einzelheiten unter Berufung auf das Steuergeheimnis ab. Nachdem in der Presse weiter darüber berichtet wurde, dass die betroffenen Abgeordneten mit schikanösen Prüfungen überzogen worden seien, befasste sich am 24. August 2007 der Ältestenrat des Abgeordnetenhauses mit der Angelegenheit. Er verständigte sich darauf, dass die beiden betroffenen Mitglieder des Petitionsausschusses (ein Dritter ist inzwischen nicht mehr Mitglied des Abgeordnetenhauses) Einverständniserklärungen vorlegen sollten, nach denen die Finanzverwaltung berechtigt sein sollte, den Präsidenten des Abgeordnetenhauses über Einzelheiten ihrer Steuerangelegenheiten zu unterrichten. Dieser wollte sodann über das weitere Vorge-

[120] Entschließung der 74. Konferenz v. 25./26. Oktober 2007 „Zentrale Steuerdatei droht zum Datenmoloch zu werden“, vgl. Dokumentenband 2007, S. 19

hen entscheiden. Dementsprechend bat der Präsident des Abgeordnetenhauses den Regierenden Bürgermeister um detaillierte Auskunft dazu, wer wann und aus welchem Grund in Steuerangelegenheiten Maßnahmen bei den beiden Abgeordneten veranlasst habe. Der Präsident bat außerdem darum, bei der Verarbeitung und Übermittlung entsprechender Vorgänge auf die Wahrung der Vertraulichkeit größte Sorgfalt zu legen.

Am 1. Oktober 2007 veröffentlichte die Senatsverwaltung für Finanzen eine Presseerklärung Nr. 07-058 („Richtigstellung unwahrer Tatsachenbehauptungen zur Tätigkeit der Finanzverwaltung"). Diese Presseerklärung war auch bei Redaktionsschluss noch im Internet abrufbar[121]*. In dieser siebenseitigen Erklärung nahm die Finanzverwaltung umfassend Stellung zu den gegen sie in der Öffentlichkeit erhobenen Vorwürfen. Die betroffenen Steuerschuldner seien zuvor gebeten worden, die Finanzverwaltung vom Steuergeheimnis zu befreien; dieser Bitte seien die Betroffenen jedoch „nicht in der erforderlichen Weise gefolgt". Deshalb sehe sich die Senatsverwaltung für Finanzen gezwungen, mit Einverständnis des Bundesministeriums der Finanzen nach § 30 Abs. 4 Nr. 5 c der Abgabenordnung (AO) auch ohne das Einverständnis der Steuerschuldner in der Sache Stellung zu nehmen. Die Presseerklärung enthält detaillierte Angaben über steuerliche Angelegenheiten der vier betroffenen Personen. Auch wenn keine konkreten Steuerrückstände beziffert werden, ist in einem Fall von „einem erheblichen Gesamtrückstand" die Rede. Auch weitere steuerlich relevante Sachverhalte wie die Nutzung eines ausgebauten Dachgeschosses, für das einer der Betroffenen einen Betriebskostenabzug geltend gemacht hatte, werden im Detail dargelegt. Insgesamt sollte mit der Presseerklärung vom 1. Oktober 2007 der Vorwurf entkräftet werden, die Maßnahmen der Finanzverwaltung gegen die vier betroffenen Steuerschuldner stünden in einem Zusammenhang mit der Prüfung von Mobbingvorwürfen durch den Petitionsausschuss.*

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat nach Veröffentlichung der Presseerklärung vom 1. Oktober 2007 die Finanzverwaltung um eine Stellungnahme dazu gebeten, aus welchem Grund eine derart extensive Veröffentlichung von personenbezogenen Daten, die dem Steuergeheimnis unterliegen, gerechtfertigt war. Die Senatsverwaltung für Finanzen teilte ihm daraufhin mit, die Abgabenordnung regelt den Umgang und die Erhebung von Daten im Besteuerungsverfahren abschließend. Die Datenschutzgesetze des Bundes und der Länder würden dadurch verdrängt. Dies habe auch der Bundesfinanzhof bestätigt.

[121] http://www.berlin.de/sen/finanzen/presse/2007.html

6.2

Zudem habe das Bundesministerium der Finanzen „dem Verfahren“ (gemeint ist offenbar die Veröffentlichung der siebenseitigen Presseerklärung) schriftlich zugestimmt. Es sei in jedem Einzelfall abgewogen worden, welche Informationen für eine verständliche Darstellung des zutreffenden Sachverhalts in der Öffentlichkeit erforderlich waren. Die Finanzverwaltung erklärte ihre Bereitschaft, auf gezielte Fragen des Datenschutzbeauftragten zu diesem Komplex zu antworten. Daraufhin übermittelte der Berliner Datenschutzbeauftragte der Finanzverwaltung eine Liste mit neun detaillierten Fragen. Als Reaktion hierauf übersandte die Senatsfinanzverwaltung dem Datenschutzbeauftragten den Beschluss des Finanzgerichts Berlin-Brandenburg vom 24. Oktober 2007[122], in dem dieses den Antrag eines der vier Betroffenen auf Erlass einer einstweiligen Anordnung wegen Verletzung des Steuergeheimnisses zurückgewiesen hatte. Außerdem fügte die Finanzverwaltung dem Datenschutzbeauftragten ein Schreiben der Staatsanwaltschaft Berlin bei, in dem diese ihre Absicht bekundete, ein Strafverfahren gegen den Finanzsenator und mehrere Mitarbeiter der Senatsverwaltung für Finanzen wegen Verletzung des Steuergeheimnisses einstellen zu wollen. Der Senator für Finanzen teilte dem Datenschutzbeauftragten mit, aus seiner Sicht bedürfe die Angelegenheit keiner weiteren Erörterung mehr. Die Fragen des Datenschutzbeauftragten beantwortete er nicht. Dieser bat im Dezember 2007 erneut um Stellungnahme zu den detaillierten Fragen, um eine unabhängige Prüfung der Angelegenheit vornehmen zu können, und wies auf die Unterstützungspflicht der Finanzverwaltung nach § 28 Abs. 1 Berliner Datenschutzgesetz (BlnDSG) hin. Dieses Schreiben blieb bis zum Redaktionsschluss unbeantwortet.

Auch wenn deshalb die Angelegenheit nicht abschließend bewertet werden kann, lässt sich doch Folgendes feststellen: Der Gesetzgeber hat in der Abgabenordnung eine Durchbrechung des Steuergeheimnisses ausnahmsweise dann zugelassen, wenn daran ein zwingendes öffentliches Interesse besteht. Dieses ist namentlich gegeben, „wenn die Offenbarung erforderlich ist zur Richtigstellung in der Öffentlichkeit verbreiteter unwahrer Tatsachen, die geeignet sind, das Vertrauen in die Verwaltung erheblich zu erschüttern; die Entscheidung trifft die zuständige oberste Finanzbehörde im Einvernehmen mit dem Bundesministerium der Finanzen; vor der Richtigstellung soll der Steuerpflichtige gehört werden“[123]. Das Bundesverfassungsgericht hat betont, dass die kontinuierliche Erfassung, Speicherung und ständige Abrufbarkeit von Angaben, die Steuerpflichtige nach dem Abgabenrecht machen müssen, denjenigen, die über diese Daten verfügen, „ein Wissen außerordentlichen Ausmaßes über die Betroffenen“ ermöglichen, „das unter den gegenwärtigen Lebensverhältnissen in entsprechende Macht über die Betroffe-

[122] 7 V 7357/07

[123] § 30 Abs. 5 c AO

nen umschlagen kann“[124]. Diese Macht darf nicht zu exzessiven Eingriffen in die Grundrechte der Steuerschuldner, insbesondere in ihr Recht auf informationelle Selbstbestimmung missbraucht werden. Auch sind die Ausnahmen vom Steuergeheimnis im Lichte dieser grundrechtlichen Gewährleistungen restriktiv auszulegen. Weder der Beschluss des Finanzgerichts Berlin-Brandenburg, der nur einen der vier betroffenen Steuerschuldner betrifft, noch die Absichtserklärung der Staatsanwaltschaft Berlin, das strafrechtliche Ermittlungsverfahren einstellen zu wollen, lassen eine abschließende und unabhängige Bewertung des Vorgangs aus datenschutzrechtlicher Sicht zu. Beide Stellen haben überdies nicht die Tatsache in ihre Überlegungen einbezogen, dass die umfangreichen Steuerinformationen der vier betroffenen Personen auch heute noch online weltweit abrufbar sind.

Aus datenschutzrechtlicher Sicht konnten die Zweifel an der Rechtmäßigkeit des Vorgehens der Senatsverwaltung für Finanzen in diesem Fall daher bisher nicht ausgeräumt werden. Auch ist es nicht hinnehmbar, dass die Senatsverwaltung für Finanzen die Beantwortung konkreter Fragen des Datenschutzbeauftragten ablehnt. Die Verletzung der gesetzlichen Pflicht zur Unterstützung des Datenschutzbeauftragten hat dieser inzwischen förmlich beanstandet und zugleich den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gebeten, das Vorgehen des Bundesministeriums der Finanzen in dieser Angelegenheit zu überprüfen.

Die Befugnis zur ausnahmsweisen Durchbrechung des Steuergeheimnisses ohne Einwilligung der Betroffenen, um Vorwürfe gegen die Finanzverwaltung in der Öffentlichkeit zu widerlegen, muss restriktiv und unter Beachtung des Grundrechtsschutzes der Betroffenen angewandt werden. Auch die Abgabenordnung rechtfertigt keinen „Notwehrexzess“. Jede Senatsverwaltung ist zudem gesetzlich verpflichtet, Fragen des Berliner Beauftragten für Datenschutz und Informationsfreiheit zu beantworten.

6.3 Fragebogen bei steuerlicher Geltendmachung eines PC

Eine Petentin wollte ihren Privat-PC, den sie auch beruflich nutzt, von der Steuer absetzen. Vom Finanzamt wurde sie gebeten, dazu einen Fragebogen auszufüllen. Da das Finanzamt sehr umfassende Auskünfte haben wollte, bat uns die Petentin, den Erhebungsbogen datenschutzrechtlich zu überprüfen.

[124] BVerfGE 67, 100, 142 f.

6.3

Mit dem Fragebogen werden umfangreiche personenbezogene Daten der Steuerpflichtigen erhoben. Eine derartige Erhebung von personenbezogenen Daten ist nach § 10 i. V. m. § 6 Abs. 1 BlnDSG nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder die Betroffenen darin eingewilligt haben. Von der Finanzverwaltung wurde die Datenerhebung auf die §§ 85, 88, 90 Abs. 1, 92, 93 AO gestützt.

Danach ist die Erhebung von personenbezogenen Daten jedoch nur zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist. Erforderlich ist die Kenntnis der Daten für die verantwortliche Stelle nur dann, wenn sie ihre Aufgabe im jeweiligen konkreten Einzelfall ohne diese Daten nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann. Außerdem müssen die Daten zur Aufgabenerfüllung geeignet und zweckmäßig sein. Dabei sind unter Beachtung des Verhältnismäßigkeitsgrundsatzes auch die schutzwürdigen Interessen der Betroffenen zu berücksichtigen.

In dem Fragebogen haben Steuerpflichtige anzugeben, welche (privaten bzw. beruflichen) Anwenderprogramme auf ihren Computern installiert sind. Mit der Beantwortung der Frage zu den privaten Anwenderprogrammen geben Steuerpflichtige eine Vielzahl von personenbezogenen Informationen preis. Die konkrete Bezeichnung der privaten Programme ist für die Ermittlung der beruflichen im Verhältnis zur privaten Nutzung des PC nicht erforderlich. Demgegenüber haben Betroffene ein erhebliches schutzwürdiges Interesse daran, dass diese Informationen aus ihrem Privatleben, die über die für das Finanzamt erforderliche Angabe des Umfangs der privaten Nutzung hinausgeht, nicht bekannt werden. Dieses schutzwürdige Interesse ist durch die konkrete Angabe der privaten Anwenderprogramme erheblich beeinträchtigt. Die Erhebung dieser personenbezogenen Daten ist nicht erforderlich und somit unzulässig. Wir haben vorgeschlagen, die Frage so zu formulieren, dass Steuerpflichtige keine weitergehenden personenbezogenen Daten preisgeben müssen.

Darüber hinaus werden die Steuerpflichtigen zur Nutzung von Online-Banking und Online-Brokerage befragt. Aufgabe des Finanzamtes ist es, den Anteil der beruflichen Nutzung eines privat angeschafften PC zu ermitteln. Die pauschale Frage zur Nutzung von Online-Banking und Online-Brokerage ist dazu nicht geeignet. Da diese Dienste – je nach Beruf der Betroffenen – sowohl privat als auch beruflich nutzbar sind, ist der Nutzungsanteil zu beruflichen Zwecken durch diese Fragestellung nicht zu ermitteln. Da die Steuerpflichtigen an anderer Stelle des Fragebogens ohnehin nach dem Nutzungsverhältnis (privat/beruflich) der Online-Nutzung gefragt werden, ist die Frage zum Online-Banking und Online-Brokerage nicht zulässig.

Die Steuerpflichtigen haben auch anzugeben, von welchen anderen haushaltszugehörigen Personen der PC zu welchem Zweck noch genutzt wird. Zur Ermittlung des Anteils der beruflichen Nutzung ist es unerheblich, von welcher Person konkret (außer dem Steuerpflichtigen) der PC noch genutzt wird. Ausreichend wäre hier die Frage: „Wird der PC auch von anderen Personen und wenn ja zu welchem Zweck genutzt?“ Die Erhebung von personenbezogenen Angaben über Dritte ist hier für die Aufgabenerfüllung der Finanzbehörden in keinem Fall erforderlich und damit unzulässig.

Die Senatsverwaltung für Finanzen hat sich unserer datenschutzrechtlichen Bewertung im Ergebnis angeschlossen und angekündigt, den Vordruck des Fragebogens entsprechend unseren Empfehlungen datenschutzgerecht zu ändern.

6.3

7 Sozialordnung

7.1 Jugend

Sprachlerntagebuch – Anforderungen erfüllt!

In unserem Jahresbericht aus dem Jahr 2006 haben wir über die Schwierigkeiten bei der Einführung des von der Senatsverwaltung für Bildung, Wissenschaft und Forschung (ehemals Senatsverwaltung für Bildung, Jugend und Sport) herausgegebenen Sprachlerntagebuchs berichtet[125]. Seit dem Sommer 2006 wird das Sprachlerntagebuch in allen Berliner Kindertagesstätten verwendet. Ziel dieses Instruments ist die Sprachförderung der Kinder. Um Sprachdefizite möglichst frühzeitig zu erkennen und geeignete Fördermaßnahmen einzuleiten, soll der Sprachstand der Kinder sowie ihre Fähigkeiten zur Kommunikation mit der Umwelt regelmäßig festgestellt werden.

Wir haben die Senatsverwaltung für Bildung, Wissenschaft und Forschung auf die bestehenden datenschutzrechtlichen Mängel hingewiesen und diese auch beanstanden müssen. Die Senatsverwaltung wurde aufgefordert, die Mängel zu beseitigen. Den Änderungsbedarf sahen wir insbesondere in folgenden Punkten:

- Die Eltern müssen in deutlich herausgehobener Form auf die Freiwilligkeit der Verwendung des Sprachlerntagebuchs unter Beteiligung ihrer Kinder an diesem Vorhaben hingewiesen werden. Dies gilt auch für einzelne Fragen im Sprachlerntagebuch, deren Beantwortung jederzeit im Einzelfall abgelehnt werden kann. Gleiches gilt auch für die Tonbandaufzeichnungen der Interviews. Die vorgegebene Erleichterung für die Erzieherinnen und Erzieher rechtfertigt es nicht, den Eltern und Kindern diese Form der Erfassung faktisch vorzuschreiben. Wenn die Eltern oder das Kind dies nicht wünschen, muss auf den Einsatz von Aufnahmegeräten verzichtet werden.

- Den Eltern gegenüber soll klargestellt werden, dass auf sie kein indirekter Druck zur Verwendung des Sprachlerntagebuchs ausgeübt werden darf. Qualitätssicherung i. S. d. § 13 des Kitaförderungsgesetzes (KitaFöG) sollte vielmehr gerade bedeuten, dass die Eltern umfassend über den Zweck und die Verwendung des Sprachlerntagebuchs informiert werden

[125] JB 2006, 6.3.1.

und ihnen auch die Option eröffnet wird, das Sprachlerntagebuch nicht zu verwenden, ohne Nachteile befürchten zu müssen.

- Von großer Bedeutung erschien uns eine eindeutige Information der Eltern über die mit dem Sprachlerntagebuch verfolgten Zwecke. Wenn das Sprachlerntagebuch neben der Feststellung der Sprachkompetenz von Kindern auch die Funktion eines Anmeldebogens für die Kindertagestätte erfüllen soll bzw. bei Verlassen der Einrichtung an die künftige Schule übergeben werden soll, so muss dies den Eltern ebenfalls deutlich gemacht werden.

Freundlicherweise haben wir in Gesprächen mit der Senatsverwaltung erreicht, dass unseren Bedenken Rechnung getragen wird: In einem Vorwort des Senators werden die Eltern künftig umfangreiche Informationen zu Ziel und Zweck des Sprachlerntagebuchs sowie zu seinen Inhalten und zum Umgang mit ihm erhalten. Insbesondere werden die Eltern nun darauf hingewiesen, dass der erste Teil des Buches, der die Fragen zum Kennenlernen des Kindes und seiner Familie beinhaltet, generell separat aufzubewahren ist.

Das Informationsschreiben an die Eltern und die Handreichungen an die Erzieherinnen und Erzieher sowie die Tagespflegepersonen werden gemäß unseren Empfehlungen überarbeitet. So erhalten die Eltern und die Erzieherinnen und Erzieher künftig die erforderlichen Informationen, um das Sprachlerntagebuch datenschutzgerecht handhaben zu können.

Daneben hat uns die Senatsverwaltung zugesichert, dass die Erzieherinnen und Erzieher in künftigen Fortbildungen zum Thema Sprachlerntagebuch mehr als bisher über die datenschutzrechtlichen Belange und die damit verbundenen gesetzlichen Anforderungen aufgeklärt werden.

Die Änderungen in den Hinweisen an die Eltern und an die Erzieherinnen und Erzieher schließen Schwierigkeiten mit der Handhabung der Tagebücher nicht völlig aus, sie stellen jedoch eine gute Grundlage dar, das eigentliche Ziel der Bücher, nämlich die Förderung der Kinder, im einvernehmlichen Zusammenwirken aller Beteiligten auch datenschutzgerecht zu erreichen.

7.2 Soziales

7.2.1 Hartz IV und Hausbesuche

Auch im vergangenen Jahr haben die Jobcenter *von der Möglichkeit des Hausbesuchs regen Gebrauch gemacht. Durch Hausbesuche wollen die Sozialleistungsträger ungerechtfertigten Leistungsbezug vermeiden und aufdecken. Trotz unserer stetigen Hinweise kam es auch im Jahr 2007 wiederholt zu Verstößen gegen die datenschutzrechtlichen Anforderungen.*

Wie bereits in unserem Jahresbericht 2005 ausgeführt, stellt der Hausbesuch nach der Rechtsprechung einen Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung dar[126]. Ein solcher Eingriff ist nur dann zulässig, wenn die Verhältnismäßigkeit gewahrt wird. Diese Voraussetzung ist erfüllt, wenn der Hausbesuch geeignet ist, zur Aufklärung des Sachverhalts beizutragen. Darüber hinaus muss er erforderlich sein. Insbesondere dürfen keine anderen in gleicher Weise geeigneten Mittel zur Verfügung stehen.

Zur Durchführung von Hausbesuchen sind in den Jobcentern spezielle Außendienste eingerichtet. Für die Beschäftigten bestehen strenge datenschutzrechtliche Grundsätze. Dies gebietet der besondere Schutz der Privatwohnung durch das Grundgesetz. Geschützt wird nach der Rechtsprechung des Bundesverfassungsgerichts die Privatheit der Wohnung als eines „elementaren Lebensraums“[127]. Es geht also um die Konkretisierung des allgemeinen Rechts jedes Menschen, „in Ruhe gelassen“ zu werden.

Vor diesem Hintergrund sollen Hausbesuche grundsätzlich nur bei konkretem Anlass, insbesondere bei bereits vorliegenden Verdachtsmomenten auf Missbrauch von Sozialleistungen durchgeführt werden. Der Ermittlungsauftrag muss genau definiert werden. Vor jedem Hausbesuch hat sich der Prüfdienst gegenüber den Betroffenen mit seinem Namen und der Angabe seiner Dienststelle auszuweisen. Er hat sie über den Zweck des Besuches zu informieren. Der Zutritt in die Wohnung darf nicht erzwungen oder mit falschen Angaben erreicht werden. Die Betroffenen sind darauf hinzuweisen, dass sie nicht verpflichtet sind, den Zugang zur Wohnung zu gestatten. Leistungsversagung darf bei Zutrittsverweigerung allenfalls dann angedroht oder realisiert werden, wenn die erforderliche Sachverhaltsermittlung ohne Zutritt zur Wohnung nicht durchführbar ist.

---

[126] JB 2005, 3.2

[127] BVerfGE 42, 212, 219

7.2

Trifft der Prüfdienst die Betroffenen bei einem Hausbesuch nicht an, dürfen grundsätzlich nicht andere Personen, wie Nachbarn oder Mitbewohner, befragt werden. Befinden sich lediglich minderjährige Kinder von Hilfeempfängern in der Wohnung, so ist der Hausbesuch unzulässig. Nur die wenigsten Minderjährigen besitzen die Fähigkeit, die Konsequenzen einer Einwilligung zum Zutritt in die Wohnung einzuschätzen. Bei Zweifeln, ob die angetroffene Person volljährig ist, muss vom Hausbesuch abgesehen werden.

Hausbesuche sollen stets angekündigt werden. Nur in besonderen Fällen kann auch ein unangekündigter Hausbesuch erforderlich sein, wenn eine hohe Wahrscheinlichkeit dafür besteht, dass bei einer Ankündigung Vorkehrungen getroffen werden, die den wahren Sachverhalt verdecken sollen. Nach dieser Grundregel verfahren bislang jedoch nur sehr wenige Jobcenter. Die meisten Sozialleistungsträger nehmen Hausbesuche generell unangekündigt vor. Nur dadurch ist ihrer Ansicht nach gewährleistet, dass die für die Aufklärung eines Sachverhalts notwendige Beurteilung der tatsächlichen Wohnverhältnisse objektiv und unverschleiert erfolge. Diese Ausnahme läuft dem Grundgedanken der grundrechtlich garantierten Unverletzlichkeit der Wohnung zuwider.

Um eine Entscheidung über den Zutritt zur Wohnung frei und unbeeinflusst treffen zu können, müssen Betroffene rechtzeitig und hinreichend aufgeklärt werden. Steht der Prüfdienst bereits vor der Tür, wird den Betroffenen angesichts des Überraschungseffekts eine Abwägung ihrer Möglichkeiten vielfach nicht mehr möglich sein. Insbesondere bei Besuchen in den frühen Morgenstunden besteht die Gefahr, dass Betroffene völlig überrumpelt den Zutritt zu ihrer Wohnung freigeben.

Datenschutzgerecht ist das Verfahren einiger Jobcenter, gegenüber den Leistungsempfängern Hausbesuche anzukündigen. Das konkrete Datum und die Uhrzeit werden dabei nicht genannt. Den Betroffenen ist es so möglich, sich auf den Besuch von Beschäftigten des Jobcenters einzustellen. Ein „Überrumpeln“ an der Haustür ist dadurch weitgehend ausgeschlossen.

7.2.2 Wie lebt ein Hartz-IV-Empfänger? – Hausbesuch mit Fernsehteam

Ein Bürger hat uns mitgeteilt, er habe unangemeldet Besuch vom Prüfdienst seines Jobcenters erhalten. An der Gegensprechanlage stellte der Mitarbeiter zunächst nur sich selbst vor. Als der Bürger die Wohnungstür öffnete, stand er jedoch auch zwei Vertretern eines privaten Fernsehsenders gegenüber. Erst auf Nachfrage habe der Mitarbeiter des Jobcenters

dies bestätigt. Obwohl der Bürger dem Fernsehteam Aufzeichnungen untersagte, habe er feststellen müssen, dass der Mitarbeiter mittels eines Tonaufzeichnungsgerätes, welches versteckt an seiner Lederjacke angebracht gewesen sei, die Aufzeichnung weiter fortsetzte.

Das Jobcenter hat dazu Stellung genommen und die Aufzeichnung durch den Mitarbeiter verneint. Generell weisen sich die im Ermittlungsdienst Tätigen, so teilt das Jobcenter mit, zu Beginn eines jeden Hausbesuchs aus. Die Entscheidung des Betroffenen, den Film- und Tonaufnahmen durch das Fernsehteam nicht zuzustimmen, sei akzeptiert worden. Sozialdaten des Bürgers seien nicht an das Fernsehteam weitergegeben worden. In der Wohnung sei es zu keinerlei Ton- oder Bildaufzeichnungen gekommen, das Kamerateam habe die Wohnung des Betroffenen nicht betreten.

Ein Fehlverhalten konnten wir dem Jobcenter in diesem Fall nicht nachweisen. Dennoch haben wir das Jobcenter darauf aufmerksam gemacht, dass hier sehr wohl Sozialdaten des Bürgers an das Fernsehteam weitergegeben wurden. Im Rahmen der Begleitung des Prüfdienstes durch das Fernsehteam werden beispielsweise der Name am Klingelschild und die Adresse des Betroffenen offenbart. Aus der Tatsache des Prüfbesuchs durch den Ermittlungsdienst eines Sozialleistungsträgers erfährt das Fernsehteam auch vom Leistungsverhältnis zum Bewohner.

Nach § 35 Abs. 1 Sozialgesetzbuch - Erstes Buch (SGB I) hat jeder Mensch Anspruch darauf, dass die ihn betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt erhoben, verarbeitet und genutzt werden (Sozialgeheimnis). Diese Verpflichtung soll verhindern, dass Betroffene unfreiwillig zum Gegenstand öffentlicher Berichterstattung werden. Sozialdaten dürfen deshalb nur mit vorherigem Einverständnis der betroffenen Person oder bei Vorliegen der Voraussetzungen der §§ 67 d ff. Sozialgesetzbuch – Zehntes Buch (SGB X) übermittelt werden. Eine gesetzliche Befugnis nach diesen Regelungen für die Offenbarung von Sozialdaten an das Fernsehteam bestand im vorliegenden Fall nicht. Ohne Einverständnis der betroffenen Person ist schon die Begleitung des Prüfdienstes zur Wohnung aus datenschutzrechtlicher Sicht unzulässig. Die Einholung des Einverständnisses erst an der Wohnungstür ist verspätet und rechtfertigt nicht die beschriebene Bekanntgabe der Daten auf dem Weg dahin.

Das Abgeordnetenhaus von Berlin hat bereits 2004 in einem Beschluss[128] die Behörden aufgefordert, bei Aufnahmen im häuslichen Bereich in Begleitung von Amtspersonen die Einwilligung der Betroffenen spätestens am Vortag der Film-

[128] Beschluss v. 13. Mai 2004, vgl. JB 2004, Anhang I., S. 168 f.

und Fernsehaufnahmen einzuholen. Dies gilt insbesondere auch für die Herausgabe personenbezogener Daten zur deren Vorbereitung (z. B. Anschrift der betroffenen Person).

Wir haben das Jobcenter aufgefordert, zukünftig von der Begleitung des Prüfdienstes durch Fernsehteams ohne rechtzeitige vorherige Zustimmung der Betroffenen abzusehen. Dieser Aufforderung ist das Jobcenter nachgekommen und hat entsprechende Hinweise in seine Dienstanweisung aufgenommen.

Die Durchführung eines Hausbesuches durch den Prüfdienst eines Sozialleistungsträgers in Begleitung von Presse- oder Medienvertretern bedarf der ausdrücklichen vorherigen Zustimmung der betroffenen Person spätestens am Vortag der geplanten Aufnahme. Eine Durchführung des Besuchs oder die Herausgabe von Anschriften ohne Zustimmung verstößt gegen das Sozialgeheimnis.

7.2.3 Schwärzungen im Mietvertrag

Von ihrem Jobcenter wurde eine Bürgerin aufgefordert, ihren Mietvertrag ungeschwärzt vorzulegen. Damit dieser Mietvertrag anerkannt werden könne, seien insbesondere der Name und die Unterschrift des Mietvertragspartners dringend erforderlich. Das Jobcenter vertrat uns gegenüber die Auffassung, bei dem vorgelegten Mietvertrag handele es sich um einen Formvordruck, der in jedem Kiosk erstanden werden und somit ohne Weiteres manipuliert werden könne. In anderen Leistungsfällen seien tatsächlich Manipulationen auf Mietverträgen festgestellt worden. Aus diesem Grund seien Mietverträge generell ungeschwärzt vorzulegen.

Gerade vor dem Hintergrund, dass die Jobcenter nach § 22 Abs. 4 Sozialgesetzbuch - Zweites Buch (SGB II) verpflichtet sind, im Fall nicht zweckentsprechender Verwendung der Kosten für die Unterkunft Direktzahlungen der Miete zu leisten, sei auch die Bankverbindung erforderlich. Seien weder der Vermieter noch die Bankverbindung bekannt, so sei es dem Jobcenter unmöglich, seinem gesetzlichen Auftrag nachzukommen. Schließlich, so argumentiert das Jobcenter, seien die Akten revisionsfähig zu führen. Deshalb sei es erforderlich, vorgelegte Mietbelege in Kopie zu den Akten zu nehmen. Nur auf diese Weise sei es im Fall von Streitigkeiten möglich, Entscheidungen hinsichtlich der Übernahme von Mietrückständen zu treffen.

Wir haben das Jobcenter darauf hingewiesen, dass es sich bei der Angabe von Daten zur Vermieterin oder zum Vermieter um freiwillige Angaben handelt. Unsere Auffassung wird gestützt durch die Ausfüllhinweise der Bundesagentur für Arbeit zum Antragsvordruck Arbeitslosengeld II. Darin heißt es: „Die Bankverbindung des Vermieters wird im Normalfall nicht benötigt, sie wird nur erforderlich, um im Bedarfsfall Unterkunftskosten direkt an den Vermieter zu überweisen. Bei Bedarf werden die erforderlichen Daten später erhoben. Entsprechendes gilt für Name und Anschrift des Vermieters."

Eine Rechtsgrundlage für die Anforderung einer ungeschwärzten Kopie des Mietvertrages von der Bürgerin besteht nicht. Nach dem Sozialgesetzbuch ist das Erheben von Sozialdaten nur zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle erforderlich ist. Mietverträge enthalten eine Vielzahl von Angaben, die für die Berechnung des Leistungsanspruchs nicht erforderlich sind. Hierzu gehören auch der Name und die Anschrift sowie die Angaben zur Bankverbindung der Vermieterin oder des Vermieters. Sofern das Jobcenter ausführt, die Anforderung ungeschwärzter Unterlagen sei erforderlich, da Mietverträge ohne Weiteres manipuliert werden könnten, so ist festzustellen, dass im Einzelfall konkrete Anhaltspunkte für einen Verdacht der Manipulation vorliegen müssen. Nur in diesen Fällen ist die Anforderung eines ungeschwärzten Mietvertrages zulässig.

Auch die Angabe der Bankverbindung der Vermieterin oder des Vermieters ist nicht erforderlich. Voraussetzung für die Direktzahlung an die Vermieterin oder den Vermieter bzw. andere Empfangsberechtigte ist, dass eine zweckentsprechende Verwendung durch die Hilfebedürftigen nicht sichergestellt ist[129]. Dies ist nur anzunehmen, wenn aufgrund eines mehrmaligen entsprechenden Geschehens die Gefahr weiterer zweckwidriger Mittelverwendungen besteht. Eine einmalige Zweckbindung reicht ebenso wenig aus wie ein bloßer auf eine drohende zweckwidrige Verwendung bezogener Verdacht.

Da eine Reaktion des Jobcenters auf unsere rechtlichen Einwände nicht erfolgte, haben wir das Verhalten des Jobcenters bei der Senatsverwaltung für Integration, Arbeit und Soziales beanstandet.

Daraufhin hat sich das Jobcenter unserer Rechtsauffassung angeschlossen. Uns wurde mitgeteilt, es werde eine neue Geschäftsanweisung erarbeitet, die unseren Vorgaben zur Anforderung ungeschwärzter Unterlagen entspreche. In dem beigefügten Entwurf dieser Anweisung heißt es: „Im Rahmen des Datenschutzes ist es

[129] § 22 Abs. 4 SGB II

zulässig, dass Kunden für die Entscheidung über die Leistung nichtrelevante Daten schwärzen (zum Beispiel Teile von Kontoauszügen, Teile des Mietvertrages). Die Anforderung ungeschwärzter Unterlagen ist lediglich bei konkretem Verdacht einer Manipulation zulasten des Jobcenters zulässig. In diesem Fall ist ein Aktenvermerk zu fertigen, in dem der Verdacht begründet wird."

Die generelle Anforderung von Unterlagen in Kopie ohne Möglichkeit für die Antragstellerinnen/Antragsteller, nicht leistungsrelevante Daten zu schwärzen, ist unzulässig. Die Sozialleistungsträger haben die Antragstellerinnen/Antragsteller auf die Möglichkeit von Schwärzungen hinzuweisen. Die Angaben zu Name, Anschrift und Bankverbindung der Vermieterin/des Vermieters sind nicht in jedem Fall erforderlich. Der Sozialleistungsträger hat die Notwendigkeit dieser Angaben im Einzelfall zu begründen.

7.2.4 Anfertigung von Personalausweiskopien im Jobcenter

Bei der Stellung von Sozialleistungsanträgen nach dem SGB II wird eine Vielzahl von Daten erhoben. Die Hilfesuchenden haben dazu den umfangreichen Vordruck der Bundesagentur für Arbeit (Antrag auf Leistungen nach dem SGB II) auszufüllen. Einige Jobcenter verlangen bei der Antragstellung vollständige Personalausweiskopien. Die Ablichtung wird der jeweiligen Leistungsakte beigefügt.

Begründet wird diese komplette Speicherung der Personalausweisdaten mit der Identifizierungsfunktion dieses Dokuments. Der Personalausweis sei bei allen öffentlichen Stellen vorzulegen und diene der zweifelsfreien Feststellung der Identität der Bürgerin oder des Bürgers. Durch die Organisationsstruktur der Jobcenter wechsle die Sachbearbeitung eines Falles innerhalb eines Leistungsteams unter Umständen bei jedem Besuch. Dadurch entfalle bei der Vorsprache der Hilfesuchenden zum Beispiel die Möglichkeit, eine dringende Barzahlung vorzunehmen, da die Identifizierung als anspruchsberechtigte Person nicht möglich ist. Durch die hinterlegte Kopie sei eine Sofortzahlung auch in den immer wieder vorkommenden Fällen des Ausweisverlustes möglich. Die Kopie ersetze letztendlich auch die Vorlage einer melderechtlichen Bescheinigung.

Die Speicherung der gesamten Personalausweisdaten ist allerdings unzulässig. Entsprechend dem Zweckbindungsgrundsatz nach § 67 c Abs. 1 SGB X dürfen Sozialdaten nur gespeichert werden, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden gesetzlichen Aufgaben nach den Sozialge-

setzbüchern erforderlich ist und für die Zwecke erfolgt, für die die Daten erhoben worden sind.

Mit diesem Grundsatz ist die Verfahrensweise der Jobcenter nicht zu vereinbaren. Ein Personalausweis enthält viele Angaben, die nicht zur Aufgabenerfüllung des Leistungsträgers benötigt werden. Beispielsweise ist die Kenntnis von der Augenfarbe einer Hilfe suchenden Person völlig unerheblich für die Leistungsgewährung.

Natürlich ist das Argument nicht von der Hand zu weisen, die Ausweiskopien dienen der Identifizierung der Personen, insbesondere im Falle eines Ausweisverlustes. Aber auch vor diesem Hintergrund ist die Anfertigung einer vollumfänglichen Ausweiskopie nicht zulässig. Die Identifizierung der Leistungsempfängerinnen und -empfänger ist bereits durch ihren Namen, ihr Geburtsdatum und ihr Lichtbild möglich. Darüber hinausgehende Angaben, beispielsweise zu Wohnort, Augenfarbe, Größe, Tag und Ort der Ausstellung des Ausweises sind nicht erforderlich. Für eine Ablichtung der Rückseite des Dokuments besteht deshalb keine gesetzliche Grundlage. Lediglich die Speicherung von Name, Geburtsdatum und Lichtbild ist zu Identifikationszwecken durch Anfertigung einer Kopie von der Vorderseite des Ausweises zulässig. Da auch die Vorderseite des Ausweises nicht zur Aufgabenerfüllung erforderliche Daten beinhaltet (Personalausweisnummer), besteht für die Antrag stellende Person das Recht zur Unkenntlichmachung dieser Angaben. Es bietet sich hier die Möglichkeit des Schwärzens an. Darauf sollten die Jobcenter hinweisen.

Die Anfertigung einer vollständigen Personalausweiskopie im Rahmen der Beantragung von Sozialleistungen in den Jobcentern ist unzulässig. Erforderlich ist nur die Speicherung der Angaben zu Name, Geburtsdatum und Lichtbild der Antragstellerin bzw. des Antragstellers.

7.2.5 Angaben zu Dritten bei Anträgen auf Sozialleistungen

Immer wieder erreichen uns Anfragen von Bürgerinnen und Bürgern, die bei der Beantragung von Sozialleistungen aufgefordert werden, Angaben zu Dritten (Ehepartner, Lebensgefährten, Mitbewohner, Vermieter etc.) zu machen. Diese Angaben können für die Leistungsgewährung erforderlich sein. Insbesondere beim Zusammenleben der oder des Hilfebedürftigen mit Personen in einer Bedarfsgemeinschaft sind die Angaben zu den Einkommens- und Vermögensverhältnissen dieser Personen für die Leistungsberechnung relevant.

7.2

Der Gesetzgeber hat mit den Regelungen zur Bedarfsgemeinschaft nicht nur die Leistungsberechtigten, sondern auch deren Familien in die Regelungen des SGB II einbezogen. Dies soll die Eigenverantwortung der erwerbsfähigen Hilfebedürftigen und der Personen, die mit ihnen in einer Bedarfsgemeinschaft leben, stärken und dazu beitragen, dass sie ihren Lebensunterhalt selbst bestreiten können.

Die benötigten Daten sind gemäß § 67 a Abs. 2 Satz 1 SGB X grundsätzlich zunächst bei den Betroffenen selbst zu erheben. Nur diejenige Person, die ihre Sozialdaten selbst zur Verfügung stellt, kann auch kontrollieren, welche Sozialdaten sie in welchem Umfang preisgibt. Voraussetzung für eine bewusste Mitwirkung der Betroffenen ist die Aufklärung über den Zweck der Datenerhebung. Wenn die betroffene Person weiß, wofür der Sozialleistungsträger ihre Daten benötigt, kann sie die Offenlegung auch tatsächlich kontrollieren. Diesem Grundsatz entsprechend sind die Angaben von weiteren, mit der Antragstellerin oder dem Antragsteller in einer Bedarfsgemeinschaft lebenden Personen, grundsätzlich auch bei diesen selbst zu erheben.

Die Praxis zeigt, dass die Formulierungen in vielen Vordrucken der Sozialleistungsträger auf die Weitergabe von Daten Dritter durch die Antrag stellende Person gerichtet sind. Dies entspricht nicht dem beschriebenen datenschutzrechtlichen Grundsatz, wonach Sozialdaten in erster Linie zunächst bei Betroffenen zu erheben sind. Werden Daten von Dritten auf einem gemeinsamen Formular erfragt, so ist zumindest die Kenntnis dieser Dritten von der Datenerhebung sicherzustellen. Hier besteht die Möglichkeit der Unterschriftsabgabe durch die Dritten.

Bei besonders sensitiven Daten sollte den Dritten jedoch die Möglichkeit der gesonderten Abgabe ihrer Sozialdaten eingeräumt werden. Auskünfte zu Gesundheit können beispielsweise in gesonderter Form erteilt werden. Dies gilt auch für Informationen zu Wohnung oder Unterkunft im Falle eines Untermietverhältnisses.

Jeder Mensch entscheidet grundsätzlich selbst über die Preisgabe seiner Daten. Werden Daten von Personen benötigt, die keine Sozialleistungen beantragt haben, so müssen die Angaben unmittelbar von ihnen selbst erfragt werden. Aus praktischen Gründen ist die Abgabe auf einem Formular gemeinsam mit der Antrag stellenden Person möglich. Durch die Unterschrift stellen Dritte sicher, dass sie Kenntnis von der Weitergabe der Daten an den Sozialleistungsträger haben. Entsprechend sollten die Vordrucke zur Beantragung von Leistungen gestaltet sein.

7.2.6 E-Mail-Kommunikation zwischen Heimen und öffentlicher Verwaltung

Eine Trägerorganisation von Einrichtungen der Alten-, Behinderten- und Jugendhilfe, die ausdrücklich nicht gegenüber den Behörden genannt werden wollte, weil sie dann wirtschaftliche Nachteile befürchtete, teilte uns mit, dass sie von Behören aufgefordert wurde, sensitive personenbezogene Daten per E-Mail bzw. als E-Mail-Anlagen zu übersenden. Die Möglichkeit der verschlüsselten Übermittlung wurde dabei nicht angeboten. Zu den genannten öffentlichen Stellen gehört die Heimaufsicht im Landesamt für Gesundheit und Soziales, die tabellarischen Übersichten der Mitarbeiterinnen und Mitarbeiter der Einrichtungen erhält, die Senatsverwaltung für Integration, Arbeit und Soziales, die „Qualitätsbögen zur Struktur und Leistung" mit Mitarbeiterdaten fordert, und die Sozialämter der Bezirke, die Entwicklungsberichte von Behinderteneinrichtungen mit intimen Daten aus dem Leben behinderter Menschen anfordern.

Wir machten die genannten Behörden darauf aufmerksam, dass die Heimträger gegen datenschutzrechtliche Bestimmungen verstoßen, wenn sie solchen Aufforderungen oder Erwartungen entsprechen. Öffentlich-rechtliche Heimträger, z. B. Stiftungen öffentlichen Rechts, müssen mit förmlichen Beanstandungen rechnen. Private Heimträger, dazu gehören auch Stiftungen bürgerlichen Rechts, müssen damit rechnen, dass bei schwerwiegenden Mängeln bezüglich der technisch-organisatorischen Anforderungen von § 9 Bundesdatenschutzgesetz (BDSG) die zuständige Aufsichtsbehörde für den Datenschutz die Beseitigung der Mängel unter Androhung von Zwangsgeld verlangt und ggf. die Verwendung des E-Mail-Dienstes untersagt.

Die unverschlüsselte Übersendung sensitiver personenbezogener Daten stellt unbestreitbar einen solchen schweren Mangel der Weitergabekontrolle nach Nr. 4 der Anlage zu § 9 Satz 1 BDSG dar. Die Daten übermittelnden Stellen haben zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Bei der Übertragung von Daten per E-Mail kann dies nur mit der Verschlüsselung der Daten sichergestellt werden.

Wir baten darum, die Behörden und deren Dienstkräfte darauf aufmerksam zu machen, dass die Heimträger nicht um die elektronische Übermittlung personenbezogener Daten per unverschlüsselte E-Mail zu bitten sind, zumal sie aus wirtschaftlichen Erwägungen geneigt sein dürften, Wünschen der Aufsicht führenden Behörden entgegenzukommen, auch wenn dies zu rechtswidrigem Handeln führt.

7.2

Soweit weiterhin der elektronische Weg für die Datenanlieferung der Heimträger bevorzugt werde, habe dies verschlüsselt zu erfolgen.

Die Senatsverwaltung für Integration, Arbeit und Soziales verwies darauf, dass sich ihre Zuständigkeit auf Teile der Behindertenhilfe, die Wohnungslosenhilfe und die Altenhilfe beschränkt, wobei im Bereich der Altenhilfe keine personenbezogenen Daten von der Senatsverwaltung erhoben würden. Bei der Übermittlung der personenbezogenen Daten für die übrigen Bereiche in der Zuständigkeit der Senatsverwaltung seien 2006 letztmalig Excel-Tabellen unverschlüsselt per E-Mail übersandt worden. Seitdem würden die Daten im Rahmen eines E-Government-Verfahrens mit einer in Entwicklung befindlichen Webanwendung übertragen, die den Datenschutz nach aktuellen Standards sicherstellen würde. Bisher sind wir jedoch weder über das neue Verfahren noch über die dazugehörige Sicherheitskonzeption unterrichtet worden.

Die Heimaufsicht im Landesamt für Gesundheit und Soziales räumte ein, dass sie auf Anforderung Formulare per E-Mail versandt, jedoch keine Rücksendung der ausgefüllten Formulare verlangt hat. Dies sei auch nur in den wenigsten Fällen geschehen, normalerweise erfolge die Rücksendung per Post. Die Heimaufsicht bedauerte, gegen die gelegentlichen E-Mail-Rücksendungen nicht eingeschritten zu haben. Nunmehr würden die Beschäftigten der Träger über die Rechtswidrigkeit eines solchen Vorgehens informiert und der Vordruck würde um einen entsprechenden Hinweis ergänzt.

Die bezirklichen Sozialämter teilten einhellig mit, dass sie keine Datenübermittlungen per E-Mail verlangen würden, gleichwohl nicht immer ausgeschlossen sei, dass es abweichende Absprachen gäbe, um die Abläufe zu beschleunigen. Die meisten Sozialämter kündigten an, ihre Bediensteten noch einmal darüber belehren zu wollen, dass sie keine Übersendungen per E-Mail anfordern sollen, da dies die Leistungserbringer zu rechtswidrigem Handeln verleiten würde. Einige Bezirksämter waren gegenüber der Empfehlung, künftig den verschlüsselten E-Mail-Versand zu verwenden, durchaus aufgeschlossen.

Der unverschlüsselte Versand sensitiver personenbezogener Daten per E-Mail ist stets unzulässig, weil im Internet die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten nicht sichergestellt werden kann. In den meisten angeschriebenen Behörden gibt es Dienstanweisungen, die dies unterstreichen. In diesem Falle ging es jedoch nicht um die Behörden, die E-Mails versenden wollten, sondern um Außenstehende, die aus Gründen der Bequemlichkeit und vordergründigen Effizienz dazu „angeregt“ wurden, selbst gegen den obigen Grundsatz zu verstoßen. Dies muss unterbleiben!

7.3 Gesundheit

7.3.1 Wir kennen Sie doch! – Aufbewahrungsfristen für die zahnärztliche Behandlungsdokumentation

Bei dem Besuch einer Zahnarztpraxis musste eine Patientin eine überraschende Feststellung machen: Ihre Behandlungsdaten waren noch in dem EDV-System der Praxis gespeichert, obwohl ihre letzte Behandlung durch den betreffenden Zahnarzt rund 15 Jahre zurücklag. Sie bat uns um datenschutzrechtliche Bewertung.

Eine unbegrenzte Speicherung von Patientendaten steht im Widerspruch zu den Vorgaben des Bundesdatenschutzgesetzes. § 35 Abs. 2 BDSG bestimmt, dass personenbezogene Daten zu löschen sind, wenn ihre Speicherung unzulässig ist oder sobald ihre Kenntnis für die Aufgabenerfüllung der Ärztin oder des Arztes nicht mehr erforderlich ist. Die Speicherdauer hat sich also grundsätzlich danach zu richten, wie lange die ärztlichen Daten für Behandlungs- oder Abrechnungszwecke benötigt werden. Eine feste Frist besteht insoweit nicht.

Eine über die Dauer der Behandlung hinausgehende Aufbewahrung ist geboten, wenn sie spezialgesetzlich angeordnet ist. Solche Aufbewahrungspflichten ergeben sich für Kassenzahnärztinnen und -ärzte aus dem Bundesmantelvertrag-Zahnärzte (BMV-Z). Nach § 5 Abs. 2 BMV-Z sind die zahnärztlichen Aufzeichnungen (Befunde und Behandlungsmaßnahmen) sowie die diagnostischen Unterlagen bei kieferorthopädischen Behandlungen mindestens drei Jahre nach Abschluss der Behandlung aufzubewahren. Eine längere Aufbewahrungsfrist kann sich im Einzelfall zudem aus besonderen medizinischen Erfordernissen ergeben. Eine generelle zehnjährige Aufbewahrungsfrist für zahnärztliche Aufzeichnungen, wie sie sich etwa aus der Berufsordnung für Ärzte ergibt, besteht für Zahnärztinnen und Zahnärzte im Übrigen nicht.

Eine längere Aufbewahrungsfrist kann schließlich aus den Verjährungsvorschriften des Bürgerlichen Gesetzbuchs folgen. Ansprüche der Patientin oder des Patienten aus der Zahnarzthaftung können auch deutlich nach Ablauf der dreijährigen Dokumentationspflicht verjähren. Voraussetzung für eine an den Verjährungsvorschriften orientierte Aufbewahrungsfrist ist jedoch, dass mit der Geltendmachung zivilrechtlicher Ansprüche tatsächlich – und nicht nur typischerweise – noch zu rechnen ist. Eine bloß abstrakte Gefährdung reicht insoweit nicht aus. Zudem muss den jeweiligen Patientenunterlagen eine Beweisfunktion zukommen. Eine Notwendigkeit zur Beweissicherung fehlt schon dann, wenn die Patientin oder der Patient die Löschung der Daten vorher selbst verlangt hat. Sich in einem

solchen Fall in einem Prozess auf eine Beweispflicht der Ärztin oder des Arztes zu berufen, wäre treuwidrig und ist daher unzulässig.

Der bisherige Umgang mit Patientendaten in der betreffenden Zahnarztpraxis wurde diesen Anforderungen nicht gerecht. Die bloße technische Möglichkeit zu einer beliebig langen Speicherung begründet nicht deren datenschutzrechtliche Zulässigkeit. Die Praxisorganisation musste daher entsprechend unseren Vorgaben umgestaltet und die unzulässig gespeicherten Daten gelöscht werden.

7.3.2 Anforderung von vollständigen Patientenakten durch Krankenkassen im Regressfall

Die Kassenärztliche Vereinigung Brandenburg wies uns auf Folgendes hin: Eine im Land Brandenburg tätige Vertragsärztin erhielt ein Schreiben der AOK Berlin, mit dem sie in einem konkreten Behandlungsfall zur Übersendung von Kopien der vollständigen Patientendokumentation aufgefordert wurde. Die Krankenkasse begründete die Anforderung der Unterlagen mit der Notwendigkeit, das Vorliegen eines Behandlungs- oder Pflegefehlers zu prüfen, um ggf. Ersatzansprüche gegenüber dem Schadensverursacher geltend zu machen. In dem konkreten Fall waren der Krankenkasse durch die Versorgung mehrerer Dekubitalgeschwüre der betroffenen Versicherten erhebliche Kosten entstanden.

Die Krankenkasse stützte ihr Vorgehen auf § 294 a Sozialgesetzbuch – Fünftes Buch (SGB V). Liegen Hinweise auf durch Dritte verursachte Gesundheitsschäden vor, sieht diese Vorschrift für Vertragsärzte und Krankenhäuser in der Tat eine Pflicht zur Mitteilung der erforderlichen Daten, einschließlich der Angaben über Ursachen und den möglichen Verursacher, gegenüber den Krankenkassen vor. Mit der 2004 in das SGB V eingefügten Vorschrift sollte die Position der Krankenkassen bei der Ermittlung anderer Kostenträger und der Substanziierung und Geltendmachung von Schadensersatzansprüchen gestärkt werden.

Die Vorschrift des § 294 a SGB V verpflichtet die Leistungserbringer aber nur dann zur Übermittlung von Patientenunterlagen, wenn der Aufforderung der Krankenkasse ein konkret zu bezeichnender Verdacht auf eine Drittschädigung zugrunde liegt und die angeforderten Daten für die Klärung von Ersatz- oder Erstattungsansprüchen auch tatsächlich erforderlich sind. Die pauschale Anforderung einer vollständigen Krankenakte ist daher grundsätzlich nicht von der Vorschrift gedeckt.

Die Krankenkasse ist bezüglich des Vorliegens von Verdachtsmomenten und hinsichtlich der Erforderlichkeit darlegungspflichtig, um den Leistungserbringer in die Lage zu versetzen, aus medizinisch-fachlicher Sicht eine eigenverantwortliche Entscheidung über die zu übermittelnden Daten zu treffen. Dieser Darlegungspflicht genügte das fragliche Schreiben der AOK an die Vertragsärztin nicht, da lediglich darauf hingewiesen wurde, dass durch die Versorgung mehrerer Dekubitusfälle erhebliche Kosten entstanden seien. Inwieweit der Krankheitsverlauf Anhaltspunkte für das Vorliegen eines drittverursachten Gesundheitsschadens bietet, wurde nicht ausreichend begründet. Die Berufung auf die bloße statistische Wahrscheinlichkeit eines Behandlungsfehlers reicht jedenfalls nicht aus.

Das Auskunftsbegehren hätte zudem auf die für notwendig erachteten Unterlagen beschränkt werden müssen. Der Umfang kann je nach Behandlungsfehlervorwurf, Behandlungsverlauf, Behandlungsdauer, Art der Erkrankung oder zu berücksichtigenden Grund- oder Begleiterkrankungen unterschiedlich sein. Soweit wie möglich sollten die erbetenen Daten unter Nutzung der bei der Krankenkasse bereits vorhandenen Informationen konkret bezeichnet werden. Hier bietet sich eine Bezugnahme auf die Datenkataloge des § 295 SGB V (Abrechnung ärztlicher Leistungen) an.

Die AOK Berlin hat diese Vorgaben zur Anwendung des § 294 a SGB V akzeptiert und zugesagt, ihre Vorgehensweise künftig entsprechend anzupassen. Sie hat aber auch darauf verwiesen, dass in besonders gelagerten Einzelfällen die gesamte Dokumentation des Behandlungsverlaufs für einen bestimmten Zeitraum angefordert werden müsse. Dies könne insbesondere in Dekubitusfällen angezeigt sein, da hier eine Bewertung der Risikoeinschätzung, des Prophylaxeplanes, der Durchführung der Prophylaxe und der Anpassung der Behandlung und der Medikation an den jeweils aktuellen Gesundheitszustand der geschädigten Person notwendig sei. Dagegen haben wir keine Einwände erhoben.

Vor dem Hintergrund der ärztlichen Schweigepflicht ist eine restriktive Auslegung des § 294 a SGB V geboten. Ärztinnen und Ärzte sind nur dann verpflichtet, Patientenunterlagen direkt an die Krankenkasse zu übermitteln, soweit diese Daten für die Erkennung und Ermittlung von Ersatz- oder Erstattungsforderungen der Krankenkasse im Einzelfall erforderlich sind und die Krankenkasse diese Erforderlichkeit begründet hat. Ermittlungen „ins Blaue“ hinein im Sinne einer Verdachtsschöpfung sind von der Vorschrift nicht gedeckt.

Die Auslegungs- und Anwendungsprobleme im Zusammenhang mit § 294 a SGB V werden künftig möglicherweise noch größer. Die Bundesregierung plant eine Erweiterung der Mitteilungspflichten für die Ärzteschaft und damit eine zu-

sätzliche Einschränkung des Patientengeheimnisses. Der neue Absatz 2 der Vorschrift soll folgendermaßen lauten:

„Liegen Anhaltspunkte dafür vor, dass Versicherte sich eine Krankheit vorsätzlich oder bei einem von ihnen begangenen Verbrechen oder vorsätzlichen Vergehen oder durch eine medizinisch nicht indizierte ästhetische Operation, eine Tätowierung oder ein Piercing zugezogen haben (§ 52), sind die an der vertragsärztlichen Versorgung teilnehmenden Ärzte und Einrichtungen sowie die Krankenhäuser nach § 108 verpflichtet, den Krankenkassen die erforderlichen Daten mitzuteilen. Die Versicherten sind über den Grund der Meldung nach Satz 1 und die gemeldeten Daten zu informieren." [130]

7.3.3 Der Dauerbrenner! – *Outsourcing* im Krankenhaus

Bereits vor zwei Jahren hatten wir darüber berichtet, dass Krankenhäuser – vornehmlich aus Kostengründen – zunehmend dazu übergehen, die nicht zum unmittelbaren medizinischen Kernbereich zählenden Dienstleistungen aus dem Krankenhausbetrieb auszugliedern und die Aufgaben an Drittunternehmen abzugeben [131]*. Dieser Trend ist ungebrochen. Die damit verbundenen datenschutzrechtlichen Fragestellungen sind nach wie vor aktuell.*

Auch das größte Universitätsklinikum Europas, die Charité – Universitätsmedizin Berlin –, macht vor dieser Entwicklung nicht Halt. Bereits zum 1. Januar 2006 hat sie einzelne Leistungen im Bereich des kaufmännischen, technischen und infrastrukturellen Facility Managements umstrukturiert und diese Aufgaben im Rahmen von Leistungsverträgen auf die Charité CFM Facility Management GmbH, also ein privatrechtlich organisiertes Unternehmen, übertragen. Wir unterziehen das erfolgte Outsourcing derzeit einer datenschutzrechtlichen Kontrolle. Dabei steht die Übertragung der folgenden Dienstleistungen im Mittelpunkt unseres Interesses:

- Interne Postdienste,
- Betreiben der Informations-, Kommunikations- und Sicherheitstechnik,
- Telefonzentrale,

[130] Gesetzentwurf der Bundesregierung, BR-Drs. 718/07: Entwurf eines Gesetzes zur strukturellen Weiterentwicklung der Pflegeversicherung (Pflege-Weiterentwicklungsgesetz)

[131] JB 2005, 4.5.1

- Archivdienste,
- Reinigungs-, Stations- und Desinfektionsdienste,
- Betreiben der Medizintechnik,
- Liegenschafts-, Haus- und Raumverwaltung,
- Patienten- und Mitarbeiterverpflegung.

Im Zuge ihrer Aufgabenerfüllung nehmen Mitarbeiterinnen und Mitarbeiter der CFM GmbH nach derzeitiger Organisationsstruktur zwangsläufig auch Patientendaten zur Kenntnis, die der ärztlichen Schweigepflicht[132] unterliegen. Eine solche Offenbarung von schützenswerten Geheimnissen ist ohne Einwilligung der betroffenen Personen und ohne besondere gesetzliche Befugnis nur gegenüber den sog. „berufsmäßig tätigen Gehilfen" im Sinne von § 203 Abs. 3 Satz 1 StGB möglich. Diese werden den der Verschwiegenheitsverpflichtung primär unterliegenden Personen gleichgestellt.

Um ein solches Berufsgehilfen-Verhältnis zu begründen, genügt es allerdings nicht, die Mitarbeiterinnen und Mitarbeiter des Auftragnehmers auf das Patientengeheimnis zu verpflichten. Wer zu dem Kreis der Schweigepflichtigen zu zählen ist, bestimmt sich ganz danach, ob die Hilfsperson in den organisatorischen und weisungsgebundenen internen Bereich der vertrauensbegründenden Sonderbeziehung einbezogen ist. Berufsmäßig tätiges Hilfepersonal sind daher nur die Personen, die innerhalb des beruflichen Wirkungskreises der Schweigepflichtigen eine auf deren berufliche Tätigkeit bezogene unterstützende Tätigkeit ausüben, die die Kenntniserlangung von fremden Geheimnissen mit sich bringt. Diese Voraussetzungen erfüllen die Mitarbeiterinnen und Mitarbeiter der CFM GmbH in aller Regel nicht. Bei den übertragenen Aufgabenbereichen fehlt es bereits am unmittelbaren inneren Zusammenhang mit dem eigentlichen medizinischen Behandlungsgeschehen. Es geht vielmehr um Verrichtungen, die nur die äußeren Bedingungen für die ärztliche Tätigkeit schaffen oder betreffen.

Unabhängig davon scheitert die Annahme der Gehilfeneigenschaft schon daran, dass die Belegschaft der CFM GmbH nicht in ausreichender Weise in die Organisation des jeweiligen Krankenhauses eingebunden ist. Eine solche Einbindung muss tatsächlich bestehen. Sie kann nicht formalvertraglich, etwa durch abstrakte Einräumung von Weisungsbefugnissen, begründet werden. Kein Hilfspersonal sind daher externe Dienstleistungsunternehmen, die rechtlich eigenständig und selbstverantwortlich Aufträge durchführen. Dies folgt zwar nicht zwingend aus dem Begriff des Gehilfen, wohl aber aus dem Grundgedanken der Vorschrift. Schützt diese auch das allgemeine Vertrauen in die Verschwiegenheit der Angehörigen

[132] § 203 Strafgesetzbuch (StGB), § 9 Berufsordnung der Ärztekammer Berlin

bestimmter Berufe, so können Gehilfen nur solche Personen sein, die an diesem Vertrauen teilhaben, was über den inneren Zusammenhang mit der ärztlichen Tätigkeit hinaus auch eine gewisse organisatorische Zugehörigkeit voraussetzt. Demnach kommen als Gehilfen in aller Regel nur Bedienstete des Krankenhauses selbst in Betracht. Die CFM GmbH handelt als rechtlich selbständiges Unternehmen außerhalb des Krankenhauses und zählt nicht zu dessen organisatorischen Bestandteilen.

Eine gesetzliche Befugnis, die die Offenbarung von Patientendaten an die CFM GmbH rechtfertigen würde, ist ebenfalls nicht ersichtlich. Gemäß § 27 Abs. 3 Berliner Landeskrankenhausgesetz (LKHG) dürfen zwar in eng begrenzten Fällen Patientendaten an Stellen außerhalb des Krankenhauses offenbart werden, unter anderem dann, wenn es zur Durchführung des Behandlungsvertrags erforderlich ist. Diese Voraussetzungen sind für hier in Frage stehende Dienstleistungen aber nicht gegeben.

Fehlt eine gesetzliche Offenbarungsbefugnis und kommt eine Einwilligung der Patientin oder des Patienten nicht in Betracht, kann ein Verstoß gegen die ärztliche Schweigepflicht nur vermieden werden, wenn die Patientendaten vor dem Verlassen der ärztlichen Sphäre anonymisiert, pseudonymisiert oder verschlüsselt werden.

Die aufgrund der ärztlichen Schweigepflicht engen rechtlichen Grenzen für OutsourcingVorhaben im Gesundheitsbereich haben wir dem Vorstand der Charité in Bezug auf die einzelnen ausgelagerten Dienstleistungen dargelegt. Dieser hat uns zugesagt, alle notwendigen technischen und organisatorischen Maßnahmen zu ergreifen, um den Datenschutzanforderungen gerecht zu werden. So sollen etwa alle Dienstleistungen, für deren Erfüllung die Kenntnisnahme von Patientendaten erforderlich ist (z. B. Archiv- und Postdienste), künftig wieder unter der uneingeschränkten Kontrolle und Weisung der Charité-Belegschaft durchgeführt werden. Die Patienten- und Mitarbeiterverpflegung soll unter Pseudonym erfolgen.

Das in den Berliner Krankenhäusern verbreitete Outsourcing von bestimmten Dienstleistungen trifft einerseits auf enge Grenzen, die mit der Beachtung der ärztlichen Schweigepflicht verbunden sind, ist aber zumindest zum Teil unvermeidbar, z. B. bei der Wartung hoch komplexer Diagnosesysteme, die unter anderem auch informationstechnische Systeme sind, die sensitive medizinische und personenbezogene Daten verarbeiten[133]. Die Krankenhäuser stehen dabei vor einem Dilemma,

[133] dies ist ein Konvergenz-Phänomen, vgl. 1.1

das nicht leicht zu lösen ist. Die Kontrolle bei der Charité soll auch dazu dienen, gemeinsam mit ihren Experten hier Lösungen näherzukommen.

7.3.4 Patientengeheimnis auch nach dem Tod: Ausgabe von Leichenschauscheinen durch beauftragtes Privatunternehmen

Durch ein Bestattungsunternehmen wurden wir darauf aufmerksam gemacht, dass ein Berliner Krankenhaus den Transport von Verstorbenen in die klinikeigene Pathologie sowie die Ausgabe der Leichenschauscheine an die Angehörigen bzw. Bestattungsunternehmen durch eine private Firma durchführen lässt.

Wir haben das Krankenhaus darauf hingewiesen, dass die damit verbundene mögliche Kenntnisnahme des Inhalts der Leichenschauscheine durch Beschäftigte des beauftragten Fuhrunternehmens einen Bruch der ärztlichen Schweigepflicht bedeuten kann. Dies kommt jedenfalls in Betracht, soweit Angaben über die Todesursache, eine möglicherweise bestehende Seuchengefahr oder die medizinischen Angaben im vertraulichen Teil des Leichenschauscheins (§ 2 Abs. 2 DVO-Bestattungsgesetz) betroffen sind.

Das in § 203 StGB normierte ärztliche Schweigegebot bezieht sich auch auf Feststellungen, die am Körper der Toten getroffen werden. Dies folgt zum einen aus dem Schutzzweck der Norm. Schutzgut des § 203 StGB ist nicht nur das Persönlichkeitsrecht des Einzelnen, sondern auch das allgemeine Vertrauen in die Verschwiegenheit der Angehörigen bestimmter Berufe als Voraussetzung dafür, dass diese ihre im Interesse der Allgemeinheit liegenden Aufgaben erfüllen. Zum anderen stellt Absatz 4 der Vorschrift ausdrücklich klar, dass die ärztliche Pflicht zur Verschwiegenheit nicht durch den Tod der Patientin oder des Patienten aufgehoben wird.

Sowohl das Offenbaren als auch das Verwerten eines Patientengeheimnisses ist allerdings nur dann rechtswidrig und ggf. strafbar, wenn die ärztliche Leitung des Krankenhauses „unbefugt“ handelt. Eine Offenbarungsbefugnis für die hier in Frage stehende Konstellation war jedoch nicht ersichtlich. Die Regelungen zur Auftragsdatenverarbeitung in § 11 BDSG führen lediglich dazu, dass der Datenfluss zwischen Krankenhaus als Auftraggeber und Fuhrunternehmen als Auftragnehmer rechtlich nicht als Datenübermittlung angesehen wird. Das ändert jedoch nichts daran, dass mit der Datenweitergabe eine Offenbarung im Sinne von § 203 StGB stattfindet, die einer besonderen Befugnis bedarf. Die allgemeinen Regeln zur Auftragsdatenverarbeitung stellen keine entsprechenden Befugnisnormen dar,

weil darin der besondere Schutz des Patientengeheimnisses keine ausreichende Berücksichtigung findet. So unterliegen die Auftragnehmer in der Regel nicht einer beruflichen Schweigepflicht, soweit sie nicht als „berufsmäßig tätige Gehilfen“ der Ärztin oder des Arztes angesehen werden können. Letzteres ist für externe Dienstleister, die rechtlich eigenständig und selbstverantwortlich Aufträge durchführen, zu verneinen[134]. Auch die in § 27 Abs. 3 LKHG vorgesehenen gesetzlichen Offenbarungsbefugnisse gelten hier nicht. Die Ausgabe der Leichenschauscheine ist nicht mehr Teil der Durchführung des Behandlungsvertrags.

Fehlt eine gesetzliche Offenbarungsbefugnis und kommt eine Einwilligung der Patientin bzw. des Patienten nicht oder nicht mehr in Betracht, kann ein Verstoß gegen die ärztliche Schweigepflicht und damit eine mögliche Strafbarkeit nur vermieden werden, wenn eine Kenntnisnahme der Daten durch das beauftragte Unternehmen von vornherein ausgeschlossen ist. Wir haben dem Krankenhaus daher vorgeschlagen, eine entsprechende Verfahrensweise – etwa die Weitergabe der Leichenschauscheine in einem geschlossenen Umschlag oder die Pseudonymisierung der Namen der Verstorbenen – vorzusehen.

Das Krankenhaus hat sich allerdings dafür entschieden, auf die Einschaltung des privaten Fuhrunternehmens zu verzichten und das Sterbefallmanagement wieder intern zu regeln. Die Ausgabe der Leichenschauscheine erfolgt durch Angestellte der Klinik. Damit wird sowohl den Vorgaben des DVO-Bestattungsgesetzes als auch den Anforderungen an den Datenschutz und die ärztliche Schweigepflicht Rechnung getragen.

7.3.5 Auf Nummer sicher! Pflegeheim stellt vorsorglich Antrag auf Sozialhilfe für eine Bewohnerin

Die Bewohnerin eines Pflegeheimes beschwerte sich bei uns darüber, dass die Pflegeheimleitung für sie als Selbstzahlerin einen Antrag auf Sozialhilfe gestellt hat. Hintergrund war ein Streit um die Rechtmäßigkeit der Anpassung des monatlichen Heimentgelts nach Erhöhung der Pflegestufe. Die Bewohnerin zahlte lediglich den alten Betrag weiter, woraufhin das Pflegeheim Klage auf Zahlung des Differenzbetrags beim Landgericht erhoben hat. Die Leitung des Pflegeheims wollte aber den Ausgang des gerichtlichen Verfahrens nicht abwarten und hat den ihrer Meinung nach bestehenden ungedeckten existenzsichernden Bedarf der Bewohnerin dem Sozialhilfeträger gegenüber angezeigt und in diesem Zusammenhang per-

[134] vgl. dazu bereits die Ausführungen unter 7.3.3

sonenbezogene Daten (u. a. Name, Geburtsdatum, Pflegestufe) übermittelt.

Zwar bestehen keine Zweifel an der grundsätzlichen Rechtmäßigkeit der Anzeige eines Sozialhilfebedarfs durch eine Pflegeeinrichtung. Aus § 18 Abs. 1 Sozialgesetzbuch – Zwölftes Buch (SGB XII) ergibt sich, dass jedermann befugt ist, Mitteilungen über das mögliche Vorliegen eines Hilfebedarfs gegenüber dem zuständigen Träger der Sozialhilfe zu machen. Es handelt sich bei dieser Vorschrift aber nicht um eine Datenverarbeitungsbefugnis. Die mit einer entsprechenden Anzeige zusammenhängende Übermittlung personenbezogener Daten der potenziell Hilfebedürftigen an den Sozialhilfeträger muss sich – zumindest in Fällen, in denen nicht-öffentliche Stellen tätig werden – an § 28 Abs. 1 Satz 1 Nr. 2 BDSG messen lassen. Danach ist das Übermitteln personenbezogener Daten nur dann zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Diese Voraussetzungen waren in diesem Fall nicht erfüllt, da zum Zeitpunkt der Antragstellung bei dem zuständigen Sozialamt keine konkreten Anhaltspunkte für einen Hilfebedarf der Bewohnerin vorlagen. Ein bloßes Nichtwissen um die wirtschaftliche Lage einer Heimbewohnerin reicht jedenfalls nicht aus, um die in § 28 Abs. 1 Satz 1 Nr. 2 BDSG vorgesehene Interessenabwägung zugunsten des Heimes ausfallen zu lassen. Andernfalls müssten die Pflegeheime in einer Vielzahl von Fällen sozusagen vorsorglich Mitteilungen an die Sozialämter tätigen. Grund für die Nichtzahlung eines Teilbetrags des Heimentgelts war vorliegend allein die gerichtlich zu klärende Frage der Rechtmäßigkeit des Erhöhungsverlangens. Die zivilrechtlichen Auseinandersetzungen ändern aber nichts an der finanziellen Leistungsfähigkeit der Bewohnerin. Eine Datenübermittlung an den Sozialleistungsträger war damit unzulässig.

Ein Antrag auf Kostenübernahme beim Sozialamt ist nur zulässig, wenn gesicherte Erkenntnisse über den bestehenden Hilfebedarf vorliegen.

7.3.6 Mysteriöser Aktenfund

Mitte August 2007 informierte uns die Presse darüber, dass sich auf dem Gelände des ehemaligen Leichenschauhauses in der Nähe des Berliner Hauptbahnhofes Gesundheitsakten zusammen mit Bauschutt befinden sollen. Umgehend prüften wir die Angelegenheit vor Ort. Ein Vertreter der

Senatsverwaltung für Gesundheit, Umwelt und Verbraucherschutz war bereits dort und hatte die noch vorhandenen Unterlagen sichergestellt. Das Gelände war vor einiger Zeit an einen Lebensmitteldiscounter verkauft worden. Nunmehr erfolgten die Abrissarbeiten.

Wir verlangten von der Senatsverwaltung für Gesundheit, Umwelt und Verbraucherschutz und dem ihr nachgeordneten Landesinstitut für gerichtliche und soziale Medizin Aufklärung. Die Senatsverwaltung erklärte, nach der Räumung der Liegenschaft „Leichenschauhaus“ im Februar 2006 habe eine gemeinsame Begehung des Landesinstituts, des Polizeiverwaltungsamtes als Eigentümer und des Bezirksamtes Mitte stattgefunden. Auch bei einer ein Jahr später erfolgten weiteren Begehung hätten sich keinerlei medizinische Akten oder Dokumente mehr auf dem Gelände befunden.

Nach den Recherchen der Senatsverwaltung und des Landesinstituts stellte sich heraus, dass der größte Teil der Unterlagen ordnungsgemäß archiviert worden war. Dementsprechend hätten die Originalunterlagen bereits vernichtet sein müssen. Anders verhält es sich mit Röntgenbildern, insbesondere CT-Aufnahmen. Diese werden nicht elektronisch archiviert, sondern im Original weiter aufbewahrt. Gleichwohl konnte die Angelegenheit nicht abschließend aufgeklärt werden, sodass die Senatsverwaltung für Gesundheit, Umwelt und Verbraucherschutz Strafanzeige gegen Unbekannt stellte. Das Ermittlungsverfahren ist zwischenzeitlich ergebnislos eingestellt worden.

Werden Grundstücke oder Gebäude für Abrissarbeiten, für Verkäufe oder anderweitige Bauarbeiten vorbereitet, so ist größte Sorgfalt darauf zu legen, dass sich keine personenbezogenen Daten oder andere Unterlagen in diesen Gebäuden mehr befinden. Um einen ordnungsgemäßen Nachweis zu führen, sollten entsprechende Ortsbegehungen schriftlich protokolliert werden.

7.3.7 Elektronische Fallakte (eFA)

Ein Konsortium führender deutscher Krankenhausunternehmen, der Deutschen Krankenhaus Gesellschaft und dem Fraunhofer Institut für Software- und Systemtechnik (ISST) befasst sich mit der Entwicklung und Einführung der sog. elektronischen Fallakte (eFA)[135]. Nach der ersten Unterrichtung durch das Berliner ISST (Standorte Berlin und Dortmund) wurde vereinbart, dass der Berliner Beauftragte für Datenschutz und In-

[135] www.fallakte.de

formationsfreiheit die Koordination der bundesweiten Abstimmung der datenschutzrechtlichen und technisch-organisatorischen Fragen mit den Datenschutzbeauftragten des Bundes und der Länder und der Aufsichtsbehörden für den Datenschutz in der Privatwirtschaft übernehmen wird, weil in Berlin mit dem ISST, der Deutschen Krankenhausgesellschaft, der Charité, der Vivantes GmbH und den Helios Kliniken GmbH große und wesentliche Konsortialmitglieder ihren Sitz haben.

Zur Koordination wurden alle deutschen Datenschutzbehörden eingeladen, sich an der datenschutzrechtlichen Begleitung des Projekts eFA zu beteiligen. Die Arbeit der Arbeitsgruppe, die sowohl eine Stellungnahme zum Projekt zum Zwecke der Abstimmung als auch Kontrollansätze für konkrete Fallaktenprojekte zum Ergebnis haben soll, ist wegen der Komplexität des Projekts noch nicht abgeschlossen.

Bei der Entwicklung der eFA handelt es sich nicht um ein konkretes Anwendungsprojekt zur allgemeinen Verbesserung der Kommunikation zwischen Leistungserbringern des Gesundheitswesens im einzelnen Behandlungsfall, sondern um die Ausarbeitung einer Spezifikation, auf der konkrete und in der Regel noch lokal begrenzte Anwendungsprojekte aufgebaut werden können. Es geht also nicht um eine neue bundesweite Infrastruktur im Gesundheitswesen, sondern um einen Standard, der zur Vereinheitlichung der technischen Grundlagen für diverse begrenzte und meist auch auf einzelne medizinische Fachgebiete bezogene Einzelprojekte zum Austausch von fallbezogenen Informationen zwischen Leistungserbringern führen soll.

Für die Mitglieder des Konsortiums zur Entwicklung der Fallakte gilt, dass zur Sicherstellung einheitlicher Kommunikationsstrukturen zwischen großen und kleinen Kooperationspartnern die Spezifikation eFA verbindlich als Grundlage von Projekten (als „Leitkultur“) zu verwenden ist.

Anders als die elektronische Krankenakte ist die eFA keine medizinische Primärdokumentation, die zum Nachvollzug ärztlichen Handelns herangezogen werden kann. Eine der wichtigsten zu klärenden Fragen ist, ob es sich bei der eFA um ein Dokumentationssystem handelt und ob sie nicht vielmehr eine reine Kommunikationsplattform zum Austausch von Dokumenten zwischen den Erbringern medizinischer Leistungen darstellt. Die Antwort auf diese Frage würde die datenschutzrechtliche Verantwortung nach § 3 Abs. 7 BDSG klären. Außerdem hängt von der Antwort ab, wer für die Dokumentation der Abfragen der Leistungserbringer verantwortlich ist.

Weitere datenschutzrechtliche Fragen betreffen die Rechtsgrundlage für die Fallakte. Konsens ist, dass dies nur die informierte schriftliche Einwilligung der Patientin oder des Patienten sein kann. Der Umfang der Einwilligung ist allerdings strittig. Nach Auffassung der Projektvertreter benötigen alle in den Fall involvierten Ärztinnen und Ärzte den vollständigen Zugriff auf die eFA. Eine differenzierte Einwilligung auf einzelne Teile der eFA würde daher keinen Sinn machen. Aber es sollen jeweils gesonderte Einwilligungen eingeholt werden, wenn zusätzliche Ärztinnen und Ärzte in die Behandlung eingebunden werden und den Zugang auf eine eFA erhalten sollen. Die Patientinnen und Patienten sollen ihre Einwilligung jederzeit zurückziehen können. Klar ist, dass die Art und Weise, wie die Einwilligungen und ihr eventueller Widerruf von einer Einwilligung erfolgen und organisiert werden, eine wesentliche Herausforderung für die auf der eFA-Spezifikation aufbauenden Projekte sein wird.

Weitere datenschutzrechtliche Fragen betreffen den Personenbezug der zur Organisation der eFA erforderlichen Metadaten, den Umfang der Zugriffsberechtigungen und die Klärung der datenschutzrechtlichen Verantwortung. Nicht zuletzt wird zu prüfen sein, wie die sehr hohen Anforderungen an die Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und vor allem auch der Authentizität der medizinischen Daten in dem Projekt erfüllt werden.

Die eFA wird als freiwillige Mehrwertanwendung der elektronischen Gesundheitskarte (eGK) angesehen, die insbesondere bei der Sicherstellung der Einwilligung, der Kontrolle des Zugriffs und der Sicherstellung von IT-Sicherheitszielen eine Rolle spielen soll. So lange die eGK noch nicht verfügbar ist, wird auch die eFA nicht im vollen Umfang in die praktische Anwendung gehen, auch wenn bereits heute Pilotprojekte auf der eFA-Spezifikation durchgeführt werden, bei denen die eGK-Funktionen durch andere Maßnahmen ersetzt werden.

7.4 Personalwesen

7.4.1 Zugang zu Mitarbeiterdaten

Vom Personalrat eines Berliner Finanzamtes hatten wir den Hinweis erhalten, dass alle Sachgebietsleitungen über das Intranet an jedem Werktag Personaldaten der Beschäftigten zu Krankheit, Urlaub, Mutterschutz, Kur und „Hamburger Modell“ erhalten, selbst wenn sie für diese Beschäftigten in keiner Weise zuständig sind.

Bei den genannten Daten handelt es sich um Personalaktendaten i. S. d. § 56 ff. Landesbeamtengesetz (LBG), das insoweit auf alle Beschäftigtengruppen im öffentlichen Dienst des Landes Berlin analog anzuwenden ist. Nach § 56 LBG sind Personalaktendaten vertraulich zu behandeln und vor unbefugter Einsicht zu schützen. Daher dürfen Zugang zur Personalakte bzw. zu Personalaktendaten nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist. Die Sachgebietsleitungen, selbst wenn sie für die betroffenen Dienstkräfte zuständig sind, müssen nicht stets Kenntnis über den Grund der Abwesenheit erlangen. Dabei steht außer Frage, dass eine Sachgebietsleitung Informationen über Abwesenheitszeiten von Beschäftigten in ihrem Arbeitsgebiet erhalten muss, um Vertretungen regeln zu können. Für diese Aufgabenerfüllung dürfte es jedoch unerheblich sein, ob die Betroffenen wegen Krankheit, Heilbehandlung oder aus einem anderen Grund abwesend sind. Entscheidend ist lediglich der Tatbestand sowie die voraussichtliche Dauer der Abwesenheit.

Wir baten daher, die Abwesenheitsliste, die nach Hauptsachgebieten zu trennen war, nur den in diesen Hauptsachgebieten eingesetzten Sachgebietsleitungen zuzusenden.

7.4.2 Umgang mit Personaldaten von Lehrkräften an einer Berliner Schule

Ein Berliner Schulleiter hatte über einen Zeitraum von mehr als 20 Jahren Notizen und Vermerke zu einer Lehrkraft an seiner Schule u. a. in Terminkalendern, Ordnern etc. aufbewahrt. Anlässlich eines an die damalige Senatsverwaltung für Bildung, Jugend und Sport gerichteten Schreibens vom Oktober 2005 griff er auf diese Datensammlung zurück, um ein möglichst negatives Bild von der betroffenen Lehrkraft zu zeichnen. Die Sammlung zeigte dabei eine Lücke zwischen den Jahren 1985 und 2002 auf. Der betroffene Lehrer wandte sich mit der Bitte um Prüfung an unsere Behörde. Er beklagte zudem eine willkürlich lange Speicherung bzw. Aufbewahrung von Krankheits- und Fehlzeiten an der Schule durch den Schulleiter.

Bezüglich des Umgangs mit Krankheits- und Fehlzeiten teilte der Schulleiter mit, dass nicht grundsätzlich Daten über alle Fehlzeiten von Lehrkräften aufbewahrt würden. Dies sei nur dann der Fall, wenn diese überproportional oft fehlten. Zunächst würden alle Atteste in einem Ordner abgelegt und später in die entsprechende Personalakte aufgenommen.

Nach Gesundung der Beschäftigten würden die Atteste an die Personalstelle weitergeleitet. Dies träfe auch auf Einzelfehltage zu. Nur in bestimmten Fällen würden Atteste kopiert, um bei wiederholt kurzfristigen Erkrankungen Gespräche mit der jeweiligen Lehrkraft führen zu können.

Nach § 2 Abs. 2 BlnDSG i. V. m. § 28 Abs. 1 Nr. 1 BDSG ist die Datenerhebung und –speicherung für eigene Geschäftszwecke zulässig, wenn es der Zweckbestimmung eines Dienstverhältnisses dient. Die Aufzeichnung von Verhaltens- und Leistungsdaten dient der Sicherung eines ordnungsgemäßen, reibungslosen und funktionsfähigen Ablaufs eines Arbeitsverhältnisses. Zu diesem Zweck ist es daher grundsätzlich zulässig, Notizen und andere Aufzeichnungen über Beschäftigte anzufertigen und aufzubewahren. Sie sind vertraulich zu behandeln und vor dem Zugriff Dritter zu schützen. Ein Terminkalender, der in der Regel offen auf dem Schreibtisch liegt, ist zur Aufbewahrung von Personaldaten daher ungeeignet, da andere Lehrkräfte, zumindest aber die Leitungsvertretung oder sogar Reinigungskräfte Notizen im Kalender zur Kenntnis nehmen können.

Personenbezogene Daten sind gemäß den Vorgaben des Berliner Datenschutzgesetzes dann zu löschen, wenn ihre Kenntnis zur Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.

Im vorliegenden Fall waren die Notizen und Aufzeichnungen des Schulleiters zur Abklärung möglicher dienstrechtlicher Maßnahmen zwar zunächst als erforderlich zu betrachten. Eine Aufbewahrungsdauer von maximal drei Jahren wäre also zulässig gewesen. Spätestens nach Ablauf dieser Zeit hätte jedoch geklärt sein müssen, ob die Personalstelle einzuschalten oder die Angelegenheit erledigt ist. Insbesondere lag auch keine "Kette" von personalrechtlich relevanten Auffälligkeiten vor, da ca. 17 Jahre lang offensichtlich kein Anlass für weitere Aufzeichnungen zu der Person des Petenten bestand.

Die Aufbewahrung der personenbezogenen Daten aus den 80er Jahren durch die Schulleitung war daher unzulässig. Selbst für den Fall, dass aufgrund der Aufzeichnungen des Schulleiters dienstrechtliche Maßnahmen gegen den Petenten eingeleitet worden wären, hätten die Unterlagen nach Aufnahme in dessen Personalakte in der Schule vernichtet werden müssen.

Notizen für spätere dienstliche Beurteilungen sind grundsätzlich ebenso geboten und daher ebenfalls zulässig. Sie sind nach Abgabe bzw. Abschluss der Beurteilung jedoch zu vernichten. Dies wird regelmäßig nach spätestens fünf Jahren (regelmäßiger Beurteilungszeitraum) der Fall sein.

Angaben zu Krankheits- und Fehltagen dürfen gemäß § 28 Abs. 1 Nr. 1 und § 2 Abs. 2 BlnDSG aufbewahrt werden, sofern es für das Dienstverhältnis erforderlich ist. Ist die Anzahl von Fehltagen zur Einleitung eines „Betrieblichen Eingliederungsmanagements“ (BEM)[136] oder zur Durchführung eines vertraulichen Personalgesprächs zwischen Schulleitung und Betroffenen relevant, so sind diese bis zur Abklärung der Angelegenheit in der Schule vorzuhalten oder zur weiteren Veranlassung an die Schulaufsicht zu übermitteln. Anderenfalls müssen diese Daten spätestens nach Ablauf von 13 Monaten gelöscht werden.

Die Aufbewahrung der Unterlagen verstieß gegen § 2 Abs. 2 BlnDSG in Verbindung mit § 35 Abs. 2 Nr. 3 BDSG. Wir haben aufgrund der oben genannten Datenschutzverstöße einen Mangel festgestellt und den Schulleiter gebeten, künftig die gesetzlichen Bestimmungen einzuhalten.

7.4.3 Aufnahme eines Gesprächsvermerks in die Personalakte

Ein Beamtenanwärter stand im Verdacht, an mehreren Tagen unentschuldigt und grundlos gefehlt und somit möglicherweise ein Dienstvergehen nach § 40 Landesbeamtengesetz (LBG) begangen zu haben. Zu diesem Vorwurf erfolgte eine mündliche Anhörung. In dem Gespräch konnte der Anwärter den Vorwurf des Dienstvergehens ausräumen, indem er seine – zunächst unentschuldigten – Fehlzeiten nachträglich glaubhaft mit kurzfristigen Erkrankungen erklärte und für einen Tag ein Attest nachreichte. Der Gesprächsvermerk wurde von der Personalstelle in eine als „Sonderheft“ bezeichnete Teilakte der Personalakte aufgenommen und der Anwärter hierüber am selben Tag unterrichtet. Dieser Vermerk verblieb zweieinhalb Jahre in der Personalakte, weshalb sich der Beamtenanwärter mit der Bitte um datenschutzrechtliche Prüfung an unsere Behörde wandte. Die verantwortliche Stelle lehnte zunächst eine Entfernung des Vermerks aus der Personalakte mit dem Hinweis ab, der Vermerk enthielte wichtige Hinweise zur persönlichen Eignung des Anwärters im Rahmen der nach § 12 LBG vorzunehmenden Bestenauslese. Folglich müsse der Vermerk auch nicht nach § 56 e Abs. 1 LBG nach einem Jahr vernichtet werden, da es sich um einen Vorgang über krankheitsbedingte Fehlzeiten des Anwärters handele.

Wir haben der Behörde dazu Folgendes mitgeteilt:

[136] vgl. dazu 7.4.4

7.4

Nach § 56 Abs. 1 Satz 2 LBG gehören zur Personalakte alle Unterlagen einschließlich der in Dateien gespeicherten, die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten). Dies sind neben Personalpapieren und dienstlichen Beurteilungen Unterlagen, die den Inhalt des Dienstverhältnisses insgesamt oder einzelne aus ihm fließende Rechte und Pflichten verändern oder bestimmen oder die Art und Weise erhellen, in der die jeweilige Entscheidung vorbereitet wurde. Zu den Personalaktendaten gehören dabei selbstverständlich auch Fehlzeiten der Beschäftigten.

Im vorliegenden Fall handelte es sich jedoch nicht nur um die übliche Dokumentation von Fehlzeiten, sondern um einen Gesprächsvermerk zur Abklärung von zunächst unentschuldigten Fehlzeiten. Wie die Verwaltung selbst ausführte, konnte der Petent in diesem Gespräch den Vorwurf eines möglichen Dienstvergehens ausräumen. Damit war der Verdacht eines dienstlichen Fehlverhaltens des Petenten nach § 40 LBG endgültig ausgeräumt. Seine Fehlzeiten waren daher nicht mehr klärungsbedürftig oder gar unentschuldigt und hätten als „normale Fehlzeiten“ Eingang in die Personalakte finden müssen. Der Gesprächsvermerk diente auch nicht zur Begründung einer Personalentscheidung oder sonstigen personalrechtlichen Maßname, sondern lediglich zur Aufklärung eines zunächst unklaren Sachverhalts.

Da sich die Behörde im vorliegenden Fall jedoch entschieden hatte, den Sachverhalt personalaktenkundig zu machen, wurde er nach § 56 Abs. 1 LBG Bestandteil der Personalakte, unterlag aber damit der Tilgungsfrist nach § 56 e Abs. 1 Nr. 2 LBG, wonach Unterlagen über Beschwerden, Behauptungen und Bewertungen auf Antrag des Beamten nach einem Jahr zu entfernen und zu vernichten sind, falls sie für den Beamten ungünstig sind oder ihm nachteilig werden können.

Etwas anderes hätte gegolten, wenn die Dienststelle ein erhebliches Dienstvergehen festgestellt und ein Disziplinarverfahren gegen den Betroffenen eingeleitet hätte. In diesem Fall hätten sich die Tilgungsfristen nach den Vorschriften des Disziplinarrechts gerichtet.

Die anhaltende Aufbewahrung des Vermerks in der Personalakte war rechtswidrig. Aufgrund unserer Intervention wurde der Gesprächsvermerk aus der Personalakte entfernt.

7.4.4 Betriebliches Eingliederungsmanagement (BEM)

In unserem letzten Jahresbericht hatten wir ausführlich über das BEM in § 84 Abs. 2 Sozialgesetzbuch – Neuntes Buch (SGB IX) berichtet und darauf hingewiesen, dass eine entsprechende Rahmendienstvereinbarung zwischen der Senatsverwaltung für Inneres und Sport und dem Hauptpersonalrat noch aussteht. Dies führte in der Folgezeit dazu, dass immer mehr öffentliche Stellen des Landes Berlin eigene Leitfäden und Handlungshilfen für die Durchführung des BEM erstellten.

> *Der Leitfaden eines Bezirksamtes sah vor, dass der Innere Dienst (ID) die jeweilige Leitung des Leistungs- und Verantwortungsbereichs bzw. der Serviceeinheit (LuV/SE) über das Vorliegen der Voraussetzungen für die Einleitung eines BEM im konkreten Einzelfall informiert und die notwendigen Daten (Name der betroffenen Beschäftigten, Hinweis auf geplantes BEM) an die Beschäftigtenvertretungen (Personalrat, ggf. Frauenvertretung, ggf. Schwerbehindertenvertretung) weitergibt. Die LuV-/SE-Leitung sollte dann ggf. in Abstimmung mit den genannten Beschäftigtenvertretungen über die Einleitung des BEM entscheiden. Der Leitfaden sah vor, dass der ID lediglich die erforderlichen Einleitungsschritte organisiert und koordiniert.*
>
> *Zur Begründung wurde ausgeführt, dass es sich beim BEM um Aufgabe der LuV-/SE-Leitung handele, die diese lediglich aus praktischen Gründen an den ID delegiere, weil dieser in enger Anbindung an die LuV-/SE-Leitung arbeite. Die LuV-/SE-Leitung trage die Ergebnisverantwortung und müsse daher die Richtigkeit der Arbeit seines ID überprüfen können. In diesem Zusammenhang sei es unabdingbar notwendig, die Daten der LuV-/SE-Leitung zu übermitteln.*

Wir haben dem Bezirksamt Folgendes mitgeteilt:

Bei Fehlzeiten der Beschäftigten, insbesondere wenn diese krankheitsbedingt sind, handelt es sich um Personalaktendaten i. S. d. § 56 Abs. 1 LBG, der analog auf alle Beschäftigungsgruppen im öffentlichen Dienst Anwendung findet. Diese Daten unterliegen aufgrund ihrer hohen Sensibilität einer gesteigerten Geheimhaltungspflicht durch den Arbeitgeber bzw. Dienstherrn.

Nach § 56 Abs. 3 LBG dürfen daher nur Beschäftigte Zugang zur Personalakte bzw. zu Personalaktendaten haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist. Folglich obliegt es nur der Personalakten führenden Stelle sowie ggf. den Perso-

nalverwaltungen innerhalb der Beschäftigungsstelle der Betroffenen (z. B. Büroleitungen, interne Dienste etc.), Fehlzeiten von Beschäftigten zu dokumentieren. Eine Rechtsgrundlage für die Übermittlung dieser Personalaktendaten von den internen Diensten an die LuV-/SE-Leitungen ist nicht ersichtlich.

Eine Einschaltung von LuV-/SE-Leitungen in der ersten Phase des BEM begegnet aber auch aus anderen Gründen erheblichen Bedenken:

Der Gesetzgeber hat mit 84 Abs. 2 SGB IX eine Norm zur Vorbeugung und Überwindung von Arbeitsunfähigkeit der Beschäftigten und damit zur Erhaltung ihrer Arbeitsplätze geschaffen. Wie in dem Leitfaden zutreffend ausgeführt wird, können Bedingungen und Belastungen am Arbeitsplatz zur Entstehung der Krankheit bei den Betroffenen beitragen und diese fördern. Insoweit wäre es wenig sinnvoll und eher kontraproduktiv, wenn diejenige Person oder Stelle, die möglicherweise „das Problem“ darstellt, ohne Kenntnis oder gar Einwilligung der Betroffenen über das Vorliegen der Voraussetzung des BEM informiert wird und aktiv werden soll. Bereits ihr Anschreiben an die Betroffenen könnte zu deren weiterer Verunsicherung führen und damit eine erfolgreiche Durchführung des BEM verhindern.

Der betroffenen Person muss im Hinblick auf ihr informationelles Selbstbestimmungsrecht die Möglichkeit gegeben werden, ohne Kenntnis ihrer LuV-/SE-Leitung das BEM durchzuführen, abzulehnen und bestimmte Personen bei der Durchführung des BEM auszuschließen. Dies kann nicht gewährleistet werden, wenn die LuV-/SE-Leitungen selbst den Erstkontakt mit den Betroffenen aufnehmen und die Betroffenen einem vermeintlichen Zwang ausgesetzt werden, sich zu einem „freundlichen Gesprächsangebot“ ihrer LuV-/SE-Leitung zu äußern. Dass eine solche mögliche (kommentarlose) Ablehnung oder der Ausschluss bestimmter Personen (eventuell der LuV-/SE-Leitung selbst) für das Betriebsklima nicht sonderlich förderlich ist, versteht sich von selbst. Dies wiederum stünde in eklatantem Widerspruch zu den gesetzgeberischen Intentionen. Selbstverständlich kann es sinnvoll sein, wenn die LuV-/SE-Leitung an dem BEM mitwirkt. Die Entscheidung darüber muss jedoch den Betroffenen selbst überlassen sein.

Wie die Datenschutzbeauftragten des Bundes und der Länder daher festgestellt haben, handelt es sich bei der Einleitung und Durchführung des BEM um eine originäre Aufgabe der Personalverwaltung und nicht der Fachvorgesetzten, die sie erst nach Zustimmung der Betroffenen an das Integrationsteam überträgt.

Die eingangs genannte Rahmendienstvereinbarung ist am 12. November 2007 endlich in Kraft getreten.

Nur die Personalakten führende Stelle oder die Personalverwaltung „vor Ort“ darf krankheitsbedingte Fehlzeiten der Beschäftigten erheben und über die Einleitung eines BEM entscheiden sowie ggf. den Erstkontakt mit den Betroffenen herstellen.

7.4.5 Unverschlüsselte Bewerberdaten im Internet

Arbeitsuchende nehmen häufig die Hilfe von professionellen Arbeitsvermittlungen in Anspruch. In der Hoffnung und Erwartung, dadurch zeitnah und ohne großen Aufwand an die entsprechenden Arbeitgeber vermittelt zu werden, überlassen sie den Arbeitsvermittlungen Bewerbungsunterlagen mit einer Vielzahl von sehr privaten und damit sensiblen Daten zu ihrem beruflichen Werdegang und Lebenslauf. Nicht selten übermitteln die privaten Arbeitsvermittlungen diese Daten dann auch für sog. Initiativ-Bewerbungen an potenzielle Arbeitgeber. Dafür bedienen sie sich zunehmend des Internets, da der E-Mail-Verkehr kostengünstig und schnell ist, und versenden die Bewerbungsunterlagen unverschlüsselt.

> *Ein Unternehmen legte den Arbeitsuchenden dafür vorformulierte Einwilligungserklärungen vor, in denen sich die Betroffenen mit der unverschlüsselten Übertragung einverstanden erklären sollten. Das Unternehmen trug dazu vor, eine hohe Empfangsquote der Bewerbungen könne nur durch unverschlüsselten Versand erreicht werden, da verschlüsselte E-Mails durch SPAM-Filter aussortiert würden und zudem die Verbreitung und Nutzung von Verschlüsselungssoftware zu gering und der Zeitaufwand für die Übermittlung zu groß wären. Im Übrigen sei nur ein Prozent der E-Mail-Adressen oder der potenziellen Arbeitgeber technisch auf den Empfang verschlüsselter E-Mails vorbereitet, indem sie beispielsweise einen öffentlichen Schlüssel bereitstellen und E-Mail-Clients verwenden, die E-Mails entschlüsseln könnten.*

Diesen Einwand konnten wir nicht akzeptieren. Wir haben die Arbeitsvermittlung auf folgende Rechtslage hingewiesen:

Bei Bewerberdaten handelt es sich um besonders sensible Daten der Betroffenen. Ein unsachgemäßer Umgang mit diesen Daten stellt einen schweren Eingriff in das Persönlichkeitsrecht der Betroffenen dar.

Gemäß § 9 Satz 1 BDSG haben nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in seiner Anlage ge-

nannten Anforderungen, zu gewährleisten. Nach Nr. 4 dieser Anlage hat die verantwortliche Stelle zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Die Umsetzung von § 9 BDSG ist kein Recht der Betroffenen, sondern eine gesetzliche Pflicht der verantwortlichen Stelle. Ein freiwilliger Verzicht nach § 4 a Abs. 1 BDSG auf technisch-organisatorische Maßnahmen ist schon deshalb nicht möglich, weil die Folgen bzw. die Tragweite eines solchen Verzichtes für die Beteiligten nicht überschaubar wären. Im Übrigen handelt es sich bei § 9 BDSG um eine ordnungsrechtliche Vorschrift, die nicht durch eine materiell-rechtliche Regelung[137] aufgehoben werden kann.

Eine vorformulierte Einwilligungserklärung würde auch gegen § 307 Abs. 1 und 2 Nr. 1 Bürgerliches Gesetzbuch (BGB) verstoßen. Danach sind Bestimmungen in allgemeinen Geschäftsbedingungen unwirksam, wenn sie den Vertragspartner des Verwenders entgegen den Geboten von Treu und Glauben unangemessen benachteiligen. Eine unangemessene Benachteiligung ist nach § 307 Abs. 2 BGB im Zweifel dann anzunehmen, wenn eine Bestimmung mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinbaren ist. Da die den Betroffenen abverlangten Erklärungen als allgemeine Geschäftsbedingungen i. S. d. genannten Vorschrift zu betrachten sind, wäre die Einwilligungserklärung zur unverschlüsselten Übermittlung der Bewerberdaten unzulässig.

Auch der Zeitaufwand für die verschlüsselte Übermittlung ist entgegen der Behauptung der Arbeitsvermittlung zumutbar. Tatsächlich ist es nämlich durch einfache Korrekturen an der Einstellung der SPAM-Filter leicht möglich, verschlüsselten E-Mails eine positivere Bewertung durch die Filterprogramme zu verschaffen. Es ist davon auszugehen, dass Arbeitgeber, die auf elektronischem Weg erreichbar sind, in der Regel mit Einstellungen ihrer SPAM-Filter arbeiten, die ihnen eine tatsächliche Erreichbarkeit auch mittels verschlüsselter E-Mails erlauben. Selbst wenn es zu einer Aussortierung der E-Mail kommt, bieten moderne Systeme zur SPAM-Filterung die Möglichkeit, die E-Mail in einem zweiten Versuch zuzustellen.

Ob nur ein Prozent der E-Mail-Adressen der potenziellen Arbeitgeber – wie ebenfalls von der Arbeitsvermittlung behauptet – technisch auf den Empfang ver-

[137] § 4 a BDSG

schlüsselter E-Mails vorbereitet ist (indem sie beispielsweise einen öffentlichen Schlüssel bereitstellen und E-Mail-Clients verwenden, die E-Mails entschlüsseln können), ist ebenso wenig bekannt wie eine verlässliche Studie über die Verbreitung von Software zur Ver- und Entschlüsselung von E-Mails. Die PGP Corporation gibt dazu an, dass ihre Software „weltweit von über 30.000 Unternehmen und öffentlichen Verwaltungen eingesetzt" wird[138]. Der Aufwand für das Verschlüsseln einer E-Mail ist gegenüber dem unverschlüsselten Versand zwar erhöht, aus unserer Sicht ist der Zeitaufwand aber nach kurzer Einarbeitungszeit auf 10 bis 15 Sekunden pro Mail, zuzüglich des einmaligen Aufwandes für das Suchen und Importieren des Schlüssels, zu senken. Angesichts der Sensitivität der verwendeten personenbezogenen Daten steht der Aufwand damit in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck.

Denkbar wäre allenfalls die Bereitstellung einer Online-Plattform zum Zweck des Eigenversandes durch die Arbeitsuchenden. Dazu müssten die Arbeitsvermittlungen Listen potenzieller Arbeitgeber (Branchenlisten) und eine technische Infrastruktur bereitstellen. Bei der Bereitstellung einer solchen Online-Plattform sind die Vorgaben des Telemediengesetzes (TMG) zu beachten. Dies bedeutet, dass die Arbeitsvermittlung insoweit als Anbieterin eines Telemediendienstes anzusehen ist und damit sicherzustellen hat, dass die Nutzerin oder der Nutzer das Online-Angebot gegen die Kenntnisnahme Dritter geschützt in Anspruch nehmen kann. Diese Plattform ermöglicht über das Protokoll HTTPS eine verschlüsselte Datenkommunikation, ohne dass die Bewerberinnen und Bewerber dafür besondere Vorkehrungen treffen müssten.

Da zwischen der Arbeitsvermittlung und potenziellen Arbeitgebern in der Regel jedoch keine Geschäftsbeziehungen bestehen und die Arbeitgeber meistens vorher auch nicht bekannt sind, ist die Verschlüsselung auf dem Weg zwischen der Vermittlungsplattform und potenziellen Arbeitgebern nur in den seltenen Ausnahmefällen möglich, in denen die Arbeitgeber einen verschlüsselten E-Mail-Empfang anbieten. Davon kann man im Regelfall nicht ausgehen. Sofern die Arbeitsuchenden unverschlüsselte E-Mails selbst versenden, tun sie dies eigenverantwortlich.

Die Bereitstellung der Online-Plattform durch die Arbeitsvermittlung begründet jedoch auch eine besondere Verantwortung gegenüber den Arbeitsuchenden. Diese macht es zwingend erforderlich, dass die Vermittlung auf ihrer Website die Betroffenen ausdrücklich darauf hinweist, dass der Übertragungsweg zwischen dem Server bei der Arbeitsvermittlung und dem potenziellen Arbeitgeber nicht unerhebliche Risiken aufweist, die dazu führen können, dass die E-Mails von Unbefugten

[138] http://www.pgp.com/de/news/2005/growthcapital.html

zur Kenntnis genommen, manipulativ verändert oder ganz unterdrückt werden können. Der Warnhinweis dient also der Klärung des Umstandes, dass die Arbeitsuchenden das Geschäftsmodell der Vermittlung insoweit auf eigene Gefahr nutzen. Diese Hinweispflicht besteht auch dann, wenn die Interessenten die Infrastruktur von Schnittstellen aus nutzen, die sich in den Geschäftsräumen der Vermittlung befinden.

Die unverschlüsselte Übermittlung von sensitiven Bewerberdaten via Internet durch die Arbeitsvermittlung verstieß gegen § 9 BDSG und war rechtswidrig.

7.5 Wohnen und Umwelt

7.5.1 Baustellen im Nachbarstreit

Die Bauherrn und Eigentümer eines Grundstücks, die nach einem Baugenehmigungsverfahren ihre Baumaßnahmen eingeleitet hatten, staunten nicht schlecht, als die Eigentümer des Nachbargrundstücks sich darüber beschwerten, die Baumaßnahmen würden vom Bauantrag abweichen und eine ursprünglich geplante Mauer würde nicht so gebaut, wie es im Antrag angegeben worden sei. Die Bauherren ersuchten uns, den Vorgang aufzuklären und weitere Einblicke der Nachbarn in ihr Baugenehmigungsverfahren zu unterbinden. Sie vermuteten nämlich – weil sie über ihre Baumaßnahmen niemand anderem als dem Bauordnungsamt Auskunft gegeben hatten –, dass die Beschwerde auf Kenntnissen beruhe, die nur durch Einsicht in die Bauakten gewonnen worden sein konnten. Das Bezirksamt Tempelhof-Schöneberg von Berlin – Amt für Planen, Genehmigen und Denkmalschutz – informierte uns darüber, dass die Nachbarn des Baugrundstückes tatsächlich Akteneinsicht in das Bauvorhaben genommen hätten. Die Akteneinsicht sei nach dem Berliner Informationsfreiheitsgesetz (IFG) gewährt worden.

Im Ergebnis durfte die Akteineinsicht gewährt werden, obwohl das IFG nicht einschlägig war. Die Auskunft aus oder Einsicht in die Bauunterlagen ließ sich jedoch auf § 59 Abs. 3 Bauordnung von Berlin (BauO) in Verbindung mit § 13 Abs. 1 und 2 Verwaltungsverfahrensgesetz (VwVfG) stützen. Das Bezirksamt war zwar zunächst der Auffassung, dass eine relevante Beeinträchtigung der Nachbarn durch die Baumaßnahmen nicht hätte entstehen können und § 59 Abs. 3 BauO nicht einschlägig sei. Eine Baugenehmigung ist jedoch ein Verwaltungsakt mit Drittwirkung. Die Drittwirkung richtet sich gegen die Person, der das Nachbarschaftsgrundstück gehört, weil Beeinträchtigungen über Grundstücksgrenzen hin-

weg bei Baumaßnahmen grundsätzlich nicht auszuschließen sind. Ob eine Beeinträchtigung tatsächlich vorliegt, kann als Ergebnis, nicht jedoch als Voraussetzung des Einsichtsrechts festgestellt werden. Die Betroffenheit der Nachbarn als Drittwirkung des Verwaltungsakts folgt nicht aus vermuteten oder tatsächlichen Gefährdungen. Sie ist vielmehr eine abstrakte Rechtsposition, die sich unmittelbar aus dem Nachbarschaftsverhältnis ergibt. Jedoch stehen die Informationsrechte des § 59 Abs. 3 nur der Eigentümerin oder dem Eigentümer eines Nachbargrundstückes zu, nur sie sind im Sinne dieser Vorschrift „Beteiligte". Benachbarte Mieterinnen oder Mieter sind das nicht. Während sich diese Rechte aus § 59 Abs. 3 Satz 1 BauO ergeben, folgen Rechte nicht beteiligter Personen nur aus § 59 Abs. 3 Satz 2 BauO, insbesondere aus den Ziffern 1 bis 3. Nach unserer Beratung hat sich das Bezirksamt unserer Rechtsauffassung schließlich angeschlossen.

Der Rückgriff auf das Informationsfreiheitsgesetz war verfehlt. Dem Recht des Bürgers auf Akteneinsicht war dennoch zu entsprechen. Der Grundsatz der Gesetzesbindung verlangt von der Verwaltung, dass für Verwaltungsentscheidungen auch die richtigen Rechtsgrundlagen herangezogen und genannt werden.

7.5.2 Großer Streit im Kleingartenverein

Mitglieder eines Kleingartenvereins schilderten uns folgendes Problem: Ihr Vorstand verweigere ihnen „aus datenschutzrechtlichen Gründen" die Einsicht in die Mitgliederliste, obwohl die Mitglieder die Einberufung einer außerordentlichen Mitgliederversammlung anstrebten. Die Kleingartenkolonie werde in der Rechtsform des eingetragenen Vereins von den Mitgliedern und dem Vereinsvorstand verwaltet. Der Vorsitzende des Vorstandes habe gegen Regelungen der Satzung verstoßen. Zur Einberufung einer außerordentlichen Mitgliederversammlung könnten ohne Einsicht in die Mitgliederliste nicht genügend Personen aktiviert werden, da ein großer Teil der Nutzenden, wie üblich zum Ende des Sommers, „den Laden dichtgemacht hätte" und persönlich auf den Parzellen nicht mehr anzutreffen sei.

Grundsätzlich steht das Datenschutzrecht der Einsichtnahme von Mitgliedern in die Mitgliederliste des Vereins nicht entgegen, wenn sie ernsthaft die Einberufung einer Mitgliedervollversammlung verlangen. Das gilt auch dann, wenn detaillierte Verfahrensvorschriften in der Satzung fehlen. Dies folgt aus der Natur und dem Wesen des Vereinsrechts, das dem einzelnen Mitglied Mitwirkungsrechte einräumt, wenn es um elementare Angelegenheiten des Vereins und um die Funktionsfähigkeit seiner Organe geht.

Als personenbezogene Daten unterliegen die Mitgliederlisten gleichwohl dem Bundesdatenschutzgesetz. Die Weitergabe von Daten durch den Vereinsvorstand ist gemäß § 4 BDSG rechtmäßig, wenn sie durch die Einwilligung der betroffenen Mitglieder oder durch eine Rechtsvorschrift gedeckt ist. So kann es dem Vereinszweck „dienlich“ sein, dass Mitglieder die Anschriften der übrigen Vereinsmitglieder erfahren, um die Mindestzahl von anderen Vereinsmitgliedern zu bewerben, die nach § 37 Bürgerliches Gesetzbuch (BGB) bzw. nach entsprechenden Regelungen der Vereinssatzung für die Einberufung einer außerordentlichen Mitgliederversammlung erforderlich wäre. Dann (und auch nur dann) besteht ein Anspruch des einfachen Mitglieds auf Einsichtnahme in die Mitgliederlisten. Die mit der Einsichtnahme verbundene Datenweitergabe findet auf der gesetzlichen Grundlage des § 28 Abs. 1 Nr. 1 BDSG statt, der eine Datenweitergabe gestattet, wenn dies der „Zweckbestimmung“ eines „vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen“ dient. Der vereinsrechtliche Anspruch auf die Einsicht in die Adressenliste „dient“ datenschutzrechtlich der Erreichung des Vereinszweckes.

Im Sinne der Verhältnismäßigkeit muss die Einsicht in die Mitgliederdaten allerdings auf Informationen beschränkt werden, die zur Kontaktaufnahme tatsächlich erforderlich sind. In der Regel genügt hierzu die Mitteilung von Namen und Adressen, eventuell auch der Telefonnummern. Wer personenbezogene Daten empfängt, darf sie grundsätzlich nur zu dem Zweck verwenden, zu dem er sie erhalten hat.

Die Zulässigkeit der Verarbeitung personenbezogener Daten im Vereinsleben ist wesentlich vom Vereinszweck geprägt, dem die Verarbeitung dienlich sein muss. Satzungsmäßige Regelungen können auch in datenschutzrechtlicher Hinsicht Zweifel ausräumen und die Grenzen der Datenverarbeitung definieren. Sie haben sich aber an der Zweckdienlichkeit i. S. d. § 28 Abs. 1 Nr. 1 BDSG auszurichten.

7.5.3 Ein wachsamer Siedlungsvorstand

Der Vorstand einer Siedlungsgemeinschaft, die sich in der Gestalt eines eingetragenen Vereins verwaltet, beschwerte sich darüber, Mitarbeiter des Bezirksamtes Pankow hätten, ohne die Betroffenen zu informieren oder deren Genehmigung einzuholen, persönliche Daten unzulässig veröffentlicht. Im Zusammenhang mit einem Gutachten zur Ermittlung der Nutzungsentgelte für Pachtgrundstücke wären nämlich personenbezogene Daten, die dem Gutachten beigefügt waren, veröffentlicht worden, ohne die Nutzenden zu informieren und ohne eine Genehmigung von diesen einzuholen, und zwar Namen, Anschriften, Fotografien und Grundrisse von

Grundstücken. Das Bezirksamt habe den Vorstand rechtsverbindlich aufgefordert, dieses Gutachten nebst Grundbuchauszügen und den o. g. personenbezogenen Daten im Vereinshaus der Siedlung auszulegen.

Bei unserer datenschutzrechtlichen Überprüfung bezog sich das Bezirksamt Pankow auf einen Beschluss des Bezirksamts, wonach die Nutzungsentgelte für die zu Erholungszwecken dienenden Parzellen auf das ortsübliche Entgelt (wie in dem Sachverständigengutachten empfohlen) zu erhöhen seien. Die Erhöhung beruhe auf § 20 Abs. 1 Schuldrechtsanpassungsgesetz i. V. m. der Nutzungsentgeltverordnung (NutzEV). Die Nutzungsentgeltverordnung schreibe in § 6 Abs. 1 NutzEV vor, dass die Erklärung über die Entgelterhöhung zu begründen sei. Zur Begründung könne nach dieser Vorschrift auf ein Gutachten über die ortsüblichen Nutzungsentgelte für vergleichbare Grundstücke Bezug genommen werden[139]. Die Nutzenden seien deshalb darauf hingewiesen worden, dass das Gutachten mit Anlagen im Vereinshaus zur Einsichtnahme vor Ort ausliege und auch beim Immobilienservice des Bezirksamtes eingesehen werden könne. Dem Gutachten seien grundsätzlich Grundbuchauszüge und Fotos beizufügen.

Da eine Einwilligung der Betroffenen zu dieser öffentlichen Auslegung der wertermittelnden Anlagen zum Gutachten nicht vorlag, bedurfte es einer Rechtsgrundlage, um die o. g. personenbezogenen Daten auszulegen. Weder das Schuldrechtsanpassungsgesetz noch die Nutzungsentgeltverordnung enthalten eine solche Grundlage. Also war zwar die Einsicht in den nicht personenbezogenen Teil des Gutachtens ohne Weiteres zulässig und notwendig, nicht aber die Einsicht in dessen personenbezogene Anlagen. Die personenbezogenen Daten des Gutachtens, die lediglich zur Meinungsbildung und zur Bewertung verarbeitet oder offenbart werden, durften nicht ausgelegt werden. Der datenschutzrechtliche Erforderlichkeitsgrundsatz hätte zur Folge, dass im Streitfall der vollständige Inhalt des Gutachtens mit den personenbezogenen Anlagen den Prozessbeteiligten zugänglich zu machen wäre, nicht jedoch beliebigen Personen oder auch nur solchen Personen, die am Vertragsverhältnis oder an einer späteren prozessualen Auseinandersetzung nicht beteiligt sind. Das Bezirksamt hätte als speichernde Stelle die Angemessenheit der Datenübermittlung und Datennutzung begrenzen und auf die Zweckbindung und den Verwendungszusammenhang der personenbezogenen Daten achten müssen.

Das Auslegen des Gutachtens ließ sich auch nicht mit § 6 Abs. 2 Satz 1 Nr. 1 d IFG rechtfertigen. Denn nach dieser Bestimmung dürfen nur bestimmte personenbezogene Daten zugänglich gemacht werden. Dazu gehören zwar Tatsachen, „dass die Betroffenen Eigentümer, Pächter, Mieter oder Inhaber eines vergleichbaren

[139] § 6 Abs. 1 Ziff. 2 NutzEV

Rechts sind“, sowie deren Namen, Titel, akademischen Grade, Geburtsdaten, Berufsbranchen- oder Geschäftsbezeichnung, innerbetriebliche Funktionsbezeichnung, Anschriften und Telefonnummern. Weitere personenbezogene Daten, wie Grundbuchauszüge, Fotos etc., durften nach dem eindeutigen Wortlaut des IFG jedoch nicht zugänglich gemacht werden.

Nach eingehender Beratung hat sich das Bezirksamt unserer Rechtsauffassung angeschlossen. Dem Vorstand des Siedlungsvereins, der sich weigerte, das Gutachten zu veröffentlichen, gebührte das Verdienst, dass es zu keiner erheblichen Beeinträchtigung grundrechtlich geschützter Interessen kam.

Das datenschutzrechtliche Erforderlichkeitsprinzip verlangt bei der Datenübermittlung und Nutzung, sich auf die geringstmögliche Beeinträchtigung grundrechtlich geschützter Interessen zu beschränken. Da es für die Wertbemessung nur auf die abstrakten Aussagen des Gutachtens ankam, war die Veröffentlichung der personenbezogenen Bewertungsgrundlagen nicht erforderlich.

8 Wissen und Bildung

8.1 Wissenschaft und Forschung

Forschung im Dunkelfeld – das Berliner Leaking-Projekt

Wissenschaftlerinnen und Wissenschaftler der Freien Universität Berlin haben Mitte des Jahres 2006 ein Projekt gestartet, bei dem es um die Prävention von schwerer zielgerichteter Gewalt gegen Schülerinnen und Schüler, Lehrkräfte und Schulpersonal geht. Als im April 2002 ein ehemaliger Schüler ein Massaker am Erfurter Gutenberg-Gymnasium anrichtete, war ganz Deutschland in Aufruhr. Dieses Verbrechen hatte sich durch verschiedene Informationen und Verhaltensauffälligkeiten des Betroffenen angekündigt. Die Hinweise wurden jedoch nicht ernst genommen bzw. konnten aufgrund fehlender Informationen kaum ernst genommen werden. Bei derartigen Vorfällen sickern fast regelmäßig im Vorfeld Tatfantasien oder Pläne potenzieller Täter durch (Leaking). Auch an Berliner Schulen kommt es hin und wieder zu Ankündigungen schwerer und zielgerichteter Gewalt durch Schülerinnen und Schüler gegenüber anderen Schülerinnen und Schülern, Lehrkräften und dem Schulpersonal.

Das Forschungsprojekt soll klären, welche Anzeichen insbesondere die Lehrkräfte und das Schulpersonal ernst nehmen sollten, um sie von „normalen" und nicht ernst gemeinten verbalen Drohungen zu unterscheiden. Das Berliner Leaking-Projekt ist datenschutzrechtlich in keiner Weise unproblematisch. Dabei werden zum Teil Informationen ohne Einwilligung der Betroffenen in pseudonymisierter Form aufbereitet, zum anderen wird versucht, mit Schülerinnen und Schülern sowie Eltern, die mit einer solchen Ankündigung oder Tat konfrontiert sind, unmittelbar in Kontakt zu treten.

Die Forscherinnen und Forscher haben sich deshalb frühzeitig an uns gewandt und wir haben das Forschungsprojekt begleitet. Mehrfach haben wir die einzelnen Schritte der Datenerfassung und -sammlung sowie der Sicherung der Daten geprüft. Das Brisante dieses Projekts besteht darin, dass selbst wenn eine Schülerin oder ein Schüler derartige gewalttätige Absichten hegt oder sogar schon umgesetzt hat, es nicht zu einer Stigmatisierung kommen darf. Gleichzeitig ist es erforderlich, so viele Informationen wie möglich über die (potenzielle) Täterin oder den (potenziellen) Täter sowie das Umfeld, die Stellung in der Schule, die psychische Konstitution zu erheben. Es konnten Verfahren gefunden werden, mit denen in den Unter-

lagen der Forscherinnen und Forscher die betroffenen Schülerinnen und Schüler, aber auch deren Eltern und die Schulen weitestgehend anonymisiert bleiben.

Das Projekt wird sicherlich über einen längeren Zeitraum fortgeführt werden müssen, um zu entsprechenden Ergebnissen zu gelangen. Ziel ist es, für die Pädagogik Hinweise zu erarbeiten, um derartige Ankündigungen schwerer und zielgerichteter Gewalt zu erkennen und entsprechende Maßnahmen einzuleiten, damit es nicht zur Umsetzung dieser Gewaltankündigungen kommt.

Auch komplizierte und vielschichtige Verfahren der wissenschaftlichen Forschung sind bei einer konsequenten Pseudonymisierung datenschutzgerecht umsetzbar.

8.2 Statistik

8.2.1 Volkszählung 2011 – Entscheidung für einen registergestützten Zensus

Bereits bei der Verabschiedung des Volkszählungsgesetzes 1986 für die Volkszählung 1987 im alten Bundesgebiet hatte der Deutsche Bundestag entsprechend den Auflagen des Bundesverfassungsgerichtes deutlich gemacht, dass von der Bundesregierung die Erforschung und Prüfung alternativer Methoden zur herkömmlichen Volkszählung erwartet wird. In den 90er Jahren hat in diesem Zusammenhang eine längere Diskussion in Fachkreisen stattgefunden. So war es durch den unzureichenden Vorbereitungsstand in Deutschland nicht möglich, sich am weltweiten Zählungszyklus um das Jahr 2000 zu beteiligen, sodass die Bundesrepublik nur durch die Lieferung hochgerechneter Bevölkerungsangaben den Verpflichtungen gegenüber der EU nachkam.

Im Jahr 2001 wurde ein Zensustest vorgenommen, über den wir in den Jahresberichten 2001 und 2002 berichteten. Dieser Test zeigte jedoch, dass allein die Zusammenführung von Daten aus verschiedenen Registern (Melderegister, Datenbestände der Bundesagentur für Arbeit und Dateien zur Beamten- und Richterschaft) den Anforderungen einer Volkszählung nicht genügen kann. Die amtliche Statistik kam zu dem Schluss, dass eine registergestützte Volkszählung durch eine Wohnungs- und Gebäudezählung sowie eine größere Bevölkerungsstichprobe ergänzt werden muss. Dafür sind intensive und aufwändige Vorbereitungen erforderlich. Wichtigste Komponente für den gesamten Zensus ist die Schaffung eines Registers der bewohnten Adressen. Hierzu sollen nicht nur die Adressen aus den 14.000 Melderegistern zusammengeführt, sondern auch andere Quellen genutzt werden. Die Datenschutzbeauftragten machten deutlich, dass allein die Vorberei-

tung eines entsprechenden Zensus und die Schaffung eines solchen Adressregisters einer gesetzlichen Grundlage bedarf.

Anfang des Jahres 2007 brachte die Bundesregierung den Entwurf eines Zensusvorbereitungsgesetzes in den Bundestag ein. Der Bundesrat kritisierte, dass damit zwar im abgeschotteten Raum der Statistik ein Register der potenziell bewohnten Adressen geschaffen wird, dieses jedoch nicht adressscharf durch die Meldebehörden überprüft werden kann. Sowohl die Bundesregierung als auch die Datenschutzbeauftragten machten deutlich, dass eine Rückübermittlung dieser zusammengeführten Daten an die Meldebehörden zur adressscharfen Klärung von Unplausibilitäten rechtlich nicht zulässig ist. Genau solche Rückübermittlungen waren Kern der Kritik des Bundesverfassungsgerichtes am Volkszählungsgesetz 1983. Es wurde deshalb mit dem Grundgesetz als unvereinbar verworfen. Eine Klärung von Unplausibilitäten der Melderegister durch eine Rückübermittlung von personenbezogenen oder adressscharfen Daten aus der Statistik in den Verwaltungsvollzug ist unzulässig. In der Folge wurde dies als Grundsatz der „Trennung von Statistik und Verwaltungsvollzug“ für die amtliche Statistik anerkannt und konsequent durchgesetzt.

Der Aufbau des Adressregisters war noch in einem weiteren Punkt zu kritisieren. So soll adressscharf eine Georeferenzierung, also eine Zuordnung von Adressen zu Koordinaten der Kartografie und Geodäsie erfolgen. Durch die vielfältigen Nutzungsmöglichkeiten von veröffentlichten statistischen Ergebnissen bieten sich dadurch unabsehbar viele Varianten, verschiedene Ergebnisse und Analysen für bestimmte geografische Bezugspunkte zu kombinieren. Bei einer Georeferenzierung kann man sie faktisch wie Folien übereinanderlegen und somit ein hohes Risiko der Reidentifizierung zunächst anonymer statistischer Ergebnisse bewirken.

Im September 2007 erfolgte eine Anhörung zum Entwurf des Zensusvorbereitungsgesetzes im Innenausschuss des Deutschen Bundestages. Mehrere Datenschutzbeauftragte machten bei dieser Anhörung deutlich, dass datenschutzrechtlich keine Rückübermittlung von adressscharfen Daten bzw. unklaren Adressen an die Meldebehörden erfolgen darf. Der Gesetzentwurf spricht daher von der Klärung in sog. „Anschriftenbereichen“. Genau diesen Aspekt versuchte der Bundesrat nachfolgend im Gesetzgebungsverfahren zu verändern. Im November wurden jedoch die zunächst vom Bundesrat einstimmig erhobenen Einsprüche mit der Zweidrittelmehrheit des Bundestages zurückgewiesen und das Zensusvorbereitungsgesetz[140] beschlossen.

[140] BGBl. I 2007, 2808

8.2

Die Datenschutzbeauftragten von Bund und Ländern werden in den nächsten Monaten genau beobachten, wie das Verfahren der Erstellung des Adressregisters verläuft, um sicherzustellen, dass keine Einzeldaten aus dem abgeschotteten Bereich der Statistik zurück in den Verwaltungsvollzug übermittelt werden.

8.2.2 Berlin – Hauptstadt der Migrantinnen und Migranten

Das Statistische Jahrbuch für Berlin weist zum 31. Dezember 2005 460.555 Ausländerinnen und Ausländer, die in Berlin wohnen, aus. Diese Zahl ist jedoch weder für die Planung im Bildungsbereich, in der Gesundheits- und Altersversorgung noch für die gezielte Beschäftigungsförderung und andere Bereiche geeignet. Sie trifft keine Aussage darüber, wie viele der in Berlin wohnenden Personen einen Migrationshintergrund und damit einen besonderen Förderungs- und Integrationsbedarf haben, obwohl sie die deutsche Staatsbürgerschaft besitzen. Seit mehreren Jahren überlegte daher die Berliner Statistik, anhand welcher Daten des Melderegisters tief regionalisierte Angaben zu den Ausländerinnen und Ausländern sowie den Deutschen mit Migrationshintergrund gewonnen werden können.

Aufgrund des Mikrozensusgesetzes 2005-2014 wurden im Jahre 2005 bei der bundesweiten kleinen Volkszählung (1%-Stichprobe) erstmals Fragen auch zur Herkunft der Ehepartner und der Eltern der Betroffenen sowie deren Kinder gestellt. Parallel dazu wurde nach ehemaligen Staatsbürgerschaften gefragt. Im Ergebnis stellte sich heraus, dass für Berlin etwa 793.900 Personen, d. h. 23,2 % der Bevölkerung, entweder eine ausländische Staatsbürgerschaft besitzen oder einen Migrationshintergrund haben. Die Daten der 1%-Stichprobe des Mikrozensus sind jedoch nicht tiefer regionalisierbar. Damit ist auch keine Datenbasis für eine räumlich bezogene Planung von Maßnahmen zur Förderung und Integration möglich. Aufgrund von § 8 Landesstatistikgesetz wurden dem Statistischen Landesamt zur Klärung dieser wissenschaftlich-methodischen Fragestellung 1.000 Datensätze aus dem Melderegister übermittelt. Aus datenschutzrechtlicher Sicht ist festzustellen, dass diese Vorschrift in Zukunft neu gefasst werden sollte, um eine eindeutige Rechtsklarheit zu schaffen.

Neben anderen Merkmalen, die zulässigerweise aus den Melderegistern für statistische Zwecke genutzt werden dürfen, wurden die Merkmale „zweite Staatsangehörigkeit, Geburtsort, Geburtsland, Name und Geburtsdatum der Ehegatten, Kinder bzw. Eltern“ übermittelt. Durch die Kombination der Merkmale „zweite Staatsangehörigkeit, Geburtsort, Geburtsland und die Verweise zwischen Kindern

und Eltern“ konnten knapp 92 % der Migranten identifiziert werden. Aufgrund dieses positiven Ergebnisses wurde angeregt, die Meldedaten-Übermittlungsverordnung um Datenflüsse aus dem Melderegister an das Amt für Statistik Berlin-Brandenburg zu ergänzen. Wenn auch nicht alle unsere Anregungen aufgegriffen wurden, so erfolgte eine Ergänzung der Übermittlungsverordnung um die Merkmale „Einbürgerungskennzeichen, Geburtsland, für Personen unter 18 Jahren folgende Merkmale der gesetzlichen Vertreter (sofern Vater/Mutter): Staatsangehörigkeiten, Einbürgerungskennzeichen und Geburtsland“. Die Übermittlung erfolgt halbjährlich.

Die Regelung im Landesstatistikgesetz zur Erhebung für besondere Zwecke, die bislang auf 1.000 Befragte begrenzt ist, sollte den Veränderungen in der amtlichen Statistik, insbesondere bei der Nutzung von Registerdaten, angepasst werden, um hier eine hinreichende Rechtssicherheit zu schaffen.

8.3 Schule

8.3.1 Erweiterung der vorschulischen Sprachförderung – Sprachstandsfeststellung

Mit dem Entwurf eines Gesetzes zur vorschulischen Sprachförderung[141] *soll in Berlin für alle Kinder eine Pflicht zur Teilnahme an vorschulischen Sprachstandsfeststellungen und bei Bedarf an Sprachfördermaßnahmen geschaffen werden. Bereits im Mai 2008 sollen die Erstklässler des Sommers 2009 im Alter von vier (statt bisher fünf) Jahren getestet werden. Bei Bedarf erhalten die Vorschulkinder eine Sprachförderung, die von bisher sechs Monaten auf dann ein Jahr verlängert wird. Die Umsetzung dieser Maßnahmen wird mit zahlreichen Datenflüssen verbunden sein.*

Zur Einführung der Maßnahmen sieht das Gesetz zur vorschulischen Sprachförderung Änderungen und Ergänzungen im Schulgesetz, Kindertagesförderungsgesetz und in der Kindertagesförderungsverordnung vor. Zur Umsetzung der gesetzlichen Zielvorgaben werden der Schule, der Schulaufsicht und den Trägern der Jugendhilfe umfangreiche Tätigkeiten zur Mithilfe zugewiesen. Auch wenn den neuen Regelungen in der Gesamtschau zu entnehmen ist, dass es sich bei der Ausweitung der vorschulischen Sprachförderung um eine schulbezogene Aufgabe handelt, lässt der Entwurf im Einzelnen eine konkrete und normenklare Aufgaben-

[141] Abghs.-Drs. 16/0794

zuweisung vermissen. Unsere Empfehlung, eine gesetzliche Regelung zu schaffen, in der die Aufgaben und die Verantwortlichkeiten den jeweiligen Stellen eindeutig zugewiesen werden, wurde nur eingeschränkt umgesetzt.

Für die Kinder, die zum Zeitpunkt der Sprachstandsfeststellung eine Tageseinrichtung der Jugendhilfe besuchen, wird die Sprachstandsfeststellung in dieser Einrichtung durchgeführt. Bei allen anderen Kindern erfolgt die Sprachstandsfeststellung in einer zuvor von der Schulaufsichtsbehörde festgelegten Einrichtung der Jugendhilfe. Die Ermittlung des betroffenen Personenkreises (alle Kinder eines bestimmten Jahrganges in Abgrenzung zu den sich bereits in einer Tageseinrichtung der Jugendhilfe befindlichen Kindern) soll in der Praxis durch einen Datenabgleich zwischen dem Melderegister und dem Datenbestand zur Kita-Verwaltung erfolgen. Das Ergebnis dieses Abgleichs soll der Schulverwaltung mitgeteilt werden.

In Gesprächen mit der Senatsverwaltung für Bildung, Wissenschaft und Forschung konnte Einigkeit darüber erzielt werden, dass für die Übermittlung von personenbezogenen Daten aus der Jugend- an die Schulverwaltung im Schulgesetz eine ausreichende Rechtsgrundlage geschaffen wird.

Entsprechend unseren Empfehlungen sollen der Umfang der zu übermittelnden Daten durch einen abschließenden Datenkatalog gesetzlich begrenzt und das Schulgesetz durch eine Rechtsverordnung ergänzt werden, die das Nähere über Art, Umfang, Zweck und weitere Fragen der Datenverarbeitung regeln wird.

8.3.2 Überprüfung von Meldedaten durch Schulämter bei Anmeldung zur Einschulung

Verschiedenen Pressemeldungen[142] war zu entnehmen, dass die Schulämter die Angaben der Eltern, die ihre Kinder für das nächste Schuljahr zur Einschulung an einer Grundschule anmelden, verstärkt kontrollieren würden. Zum Nachweis des tatsächlichen Lebensmittelpunktes würde von den Betroffenen u. a. die Vorlage von z. B. Mietverträgen, Strom- und Telefonrechnungen, GEZ-Anmeldungen usw. verlangt werden.

Nach § 55 Abs. 1 Schulgesetz (SchulG) sind schulpflichtige Kinder von ihren Erziehungsberechtigten nach öffentlicher Bekanntmachung grundsätzlich an der für sie zuständigen Grundschule anzumelden. Die zuständige Grundschule ist nach

[142] z. B. Berliner Morgenpost v. 27. Oktober 2007, Tagesspiegel v. 29. Oktober 2007

§ 55 Abs. 1 Satz 2 SchulG die Schule, in deren Einzugsbereich die Schülerin oder der Schüler wohnt. Wohnung im Sinne dieses Gesetzes ist nach § 41 Abs. 5 SchulG die Wohnung einer Person nach den §§ 16, 17 Meldegesetz (MeldeG). Bei Kindern mit mehreren Wohnorten ist die Hauptwohnung maßgebend. Als Hauptwohnung ist die Wohnung anzusehen, in der das Kind den Schwerpunkt seiner Lebensbeziehungen hat.

Die Entscheidung über die Aufnahme an einer Grundschule trifft nach § 41 Abs. 4 Satz 2 SchulG die zuständige Schulbehörde. Diese darf nach § 64 Abs. 1 SchulG die personenbezogenen Daten von Schülerinnen und Schülern und deren Erziehungsberechtigten erheben, die für diese schulbezogene Aufgabe erforderlich sind. Unstreitig ist es für die Zuweisung an die zuständige Grundschule erforderlich, dass die Schulbehörde Daten über den (Haupt-) Wohnsitz des Kindes erhebt.

Entgegen der Auffassung einer Kammer des Verwaltungsgerichts Berlin[143] ist die Schulverwaltung dabei an die im Melderegister erfassten Daten gebunden[144]. Die Schulbehörde hat zwar den Sachverhalt – wie das Gericht zutreffend feststellt – nach § 24 Abs. 1 Verwaltungsverfahrensgesetz (VwVfG) von Amts wegen unter Bestimmung von Art und Umfang der Ermittlungen festzustellen. Diese Verpflichtung zur umfassenden Sachverhaltsaufklärung hat jedoch dort ihre Grenze, wo die Schulbehörde an die Entscheidung einer anderen Behörde (hier: die Meldebehörde) gebunden ist.

Nach § 1 Abs. 1 Nr. 1 a) MeldeG obliegt es der Meldebehörde, die Einwohner und deren Wohnungen zu registrieren, um die für die rechtmäßige Erfüllung der Aufgaben öffentlicher Stellen erforderlichen Grunddaten feststellen und nachweisen zu können. Zu diesen Grunddaten gehören nach § 2 Abs. 1 Nr. 11 MeldeG auch die Angaben über die gegenwärtige und frühere Haupt- und Nebenwohnung[145] eines Einwohners. Nach dem Willen des Bundesgesetzgebers sollte durch den in § 12 Abs. 2 Melderechtsrahmengesetz (MRRG) festgeschriebenen (und vom Berliner Landesgesetzgeber in § 17 Abs. 2 MeldeG übernommenen) „objektivierten Hauptwohnungsbegriff“ die Wahlfreiheit bei der Bestimmung der Hauptwohnung nach dem alten Melderecht der Länder beseitigt werden. Die Unterscheidung zwischen Haupt- und Nebenwohnung sollte nach einheitlichen Kriterien vorgenommen werden, „weil viele Behördenzuständigkeiten oder Rechte und

[143] Beschluss v. 16. Juli 2007 – VG 9 A 162.07
[144] JB 2005, 4.6.3
[145] i. S. d. §§ 16, 17 MeldeG

Pflichten des Einwohners, die an seine Wohnung anknüpfen, eindeutig festgelegt sein müssen“[146].

Hinsichtlich der Festlegung des Hauptwohnsitzes einer Person haben die Angaben im Melderegister danach nicht nur Indiz-, sondern auch Tatbestandswirkung. Der Schulbehörde ist es verwehrt, eine vom Melderecht abweichende Festlegung der Hauptwohnung vorzunehmen. Die Tatsachenermittlungspflicht der Schulbehörde beschränkt sich vielmehr auf die Erhebung der Melderegistereintragung zur Person des Kindes[147].

Ergeben sich für die Schulbehörde aus den besonderen Umständen des Einzelfalls offensichtliche Anhaltspunkte dafür, dass die Meldedaten der Meldebehörde nicht den tatsächlichen Wohnverhältnissen entsprechen, kann sie die Meldebehörde unter Angabe der Anhaltspunkte um Überprüfung bitten. Die Meldebehörde hat dann die erforderlichen Ermittlungen in eigener Zuständigkeit zu führen. Die Meldepflichtigen haben der Meldebehörde nach § 14 MeldeG die erforderlichen Auskünfte zu geben und die zum Nachweis der Angaben erforderlichen Unterlagen vorzulegen. Nach § 9 Abs. 1 Satz 1 MeldeG hat die Meldebehörde unrichtige Daten im Melderegister von Amts wegen zu berichtigen.

Es bleibt festzustellen, dass weitere Ermittlungen der Schulbehörde zur Feststellung des tatsächlichen Lebensmittelpunktes eines Kindes nach Vorlage einer gültigen Meldebescheinigung[148] mit Angaben zur Hauptwohnung des Kindes unzulässig sind.

Nur dann, wenn die Schulpflicht des Kindes nicht durch die melderechtliche Festlegung der Hauptwohnung, sondern durch die Bestimmung des „gewöhnlichen Aufenthalts“[149] begründet wird (z. B. bei Kindern von berufsbedingt zwischen verschiedenen Wohnungen pendelnden Eltern), ist die Schulbehörde nach § 24 Abs. 1 VwVfG i. V. m. § 64 Abs. 1 SchulG berechtigt, weitere personenbezogene Daten zum tatsächlichen und zugleich überwiegenden Aufenthaltsort des Kindes von den Erziehungsberechtigten zu erheben. Diese sind dann nach § 64 Abs. 1 Satz 2 SchulG zur Erteilung der erforderlichen Auskunft verpflichtet. Der Verhältnismäßigkeitsgrundssatz ist hier zu beachten. Unverhältnismäßig wäre hier z. B. die Vorlage vollständiger Mietvertragsunterlagen mit Angaben zu Miethöhe, Mitbe-

146 vgl. die Begründung zum Entwurf des MRRG, BT-Drs. 8/3825, S. 20 und S. 30 f. zu § 12

147 vgl. dazu das Urteil des OVG Schleswig-Holstein v. 25. Juni 1991 – 2 L 58/91 – und den Beschluss des OVG Schleswig-Holstein v. 12. Dezember 2005 – 2 LB 31/05

148 § 2 Nr. 1 DVO-MeldeG

149 vgl. § 41 Abs. 1 Satz 1, 2. Alternative SchulG

wohnern usw. Die Betroffenen sind berechtigt, derartige nicht erforderliche Angaben unkenntlich zu machen (zu schwärzen). Ausreichend ist in jedem Fall, dass die verlangten Nachweise nur vorgelegt werden. Die Vorlage ist in den Einschulungsunterlagen zu vermerken. Eine Speicherung des Originals bzw. einer Kopie des Nachweises in den Einschulungsunterlagen ist unzulässig.

Wir haben dies den bezirklichen Schulämtern mitgeteilt.

Bei Anmeldung zur Einschulung haben die Schulbehörden regelmäßig die im Melderegister erfassten Daten ihrer Entscheidung über die Aufnahme eines Schulkindes zugrunde zu legen. Soweit ausnahmsweise weitere Daten erhoben werden müssen, ist der Verhältnismäßigkeitsgrundsatz strikt zu wahren.

8.3.3 Der alte Schülerausweis hat ausgedient

Die Senatsverwaltung für Bildung, Wissenschaft und Forschung informierte uns darüber, dass die bisherigen Schülerausweise in Berlin mittelfristig durch eine landesweit einheitliche SchülerCard *ersetzt werden sollen. Zur Vorbereitung dieses Vorhabens sei mit der BVG ein Pilotprojekt, an dem sich ca. 60 Schulen beteiligen, vereinbart worden. Die SchülerCard, auf der neben der (Schüler-)Ausweisfunktion auch noch eine Fahrberechtigung für den Bereich des Verkehrsverbundes Berlin-Brandenburg dokumentiert werden kann, wird von der BVG im Auftrag der Senatsverwaltung hergestellt. Die dazu erforderlichen personenbezogenen Daten der Betroffenen werden von der BVG ebenfalls im Auftrag der Senatsverwaltung verarbeitet.*

Auftraggeber einer Datenverarbeitung kann nur eine Daten verarbeitende Stelle i. S. d. § 4 Abs. 3 Nr. 1 Berliner Datenschutzgesetz (BlnDSG) sein. Daten verarbeitende Stellen sind hier zweifelsfrei die jeweiligen Schulen, die der BVG die Daten zur Herstellung von Schülerausweisen (SchülerCard) bereitstellen. Nur diese Schulen – und nicht die Senatsverwaltung – können daher als Auftraggeber der Datenverarbeitung fungieren. Die Verträge zur Auftragsdatenverarbeitung können somit nur zwischen den einzelnen Schulen und der BVG geschlossen werden. Die Senatsverwaltung kann hier jedoch im Rahmen einer Vertretungsbefugnis für die einzelnen Schulen tätig werden, wenn diese der Senatsverwaltung zuvor eine entsprechende Vollmacht zur Vereinbarung einer Auftragsdatenverarbeitung mit der BVG erteilt haben. Eine solche Vertretungsbefugnis ist zwar gesetzlich nicht ausdrücklich vorgesehen; soweit sie ausschließlich im Interesse der Betroffenen ausgeübt wird, ist sie gleichwohl datenschutzrechtlich nicht zu kritisieren.

8.3

Nach § 64 Abs. 1 SchulG dürfen die Schulen nur die personenbezogenen Daten der Schülerinnen und Schüler und deren Erziehungsberechtigten verarbeiten, die für die Erfüllung von schulbezogenen Aufgaben erforderlich sind. Dies gilt auch für den Fall, dass die Daten Dritten im Rahmen einer Auftragsdatenverarbeitung nach § 3 BlnDSG bereitgestellt werden sollen.

Die Herstellung und Ausgabe von Fahrberechtigungen für die BVG zählt in keinem Fall zu den schulbezogenen Aufgaben. Daher darf die Schule zu diesem Zweck auch keine personenbezogenen Daten von den Betroffenen (auch nicht mit deren Einwilligung) erheben. Anders verhält es sich mit der Erhebung von personenbezogenen Daten zur Bereitstellung von Schülerausweisen. Diese dienen nach Nr. 2 Abs. 1 der Ausführungsvorschriften über Schülerausweise dem Nachweis der Schülereigenschaft. Die Erhebung der für den Schülerausweis erforderlichen personenbezogenen Daten, einschließlich Lichtbild, dient somit der Erfüllung von schulbezogenen Aufgaben. Die Schule kann diese Daten – gestützt auf die Einwilligung der Antrag stellenden Personen (bzw. deren Erziehungsberechtigten) – nach § 64 Abs. 1 SchulG erheben und im Rahmen der Auftragsdatenverarbeitung an Dritte weitergeben.

In Berlin besteht keine Schülerausweispflicht. Daher ist die Erhebung der Daten zur Erstellung der SchülerCard nur mit Einwilligung der Betroffenen zulässig. Vor Abgabe der Einwilligung sind die Betroffenen über den Zweck und den Umfang der Datenverarbeitung aufzuklären. Vor diesem Hintergrund ist darauf zu achten, dass die Daten, die an den Auftragnehmer weitergeleitet werden, und die Daten (z. B. Name, Vorname usw.), die auf dem Datenträger (Schulausweis) gespeichert werden, in der Vereinbarung mit dem Auftragnehmer abschließend aufgezählt werden.

Nach Herstellung und Übergabe der SchülerCard an die Betroffenen ist eine weitere Speicherung ihrer personenbezogenen Daten zur Berücksichtigung von möglichen schutzwürdigen Belangen der Betroffenen (z. B. durch Fehldrucke, Namensverwechslungen usw.) von drei Monaten ausreichend. Danach sind die personenbezogenen Daten der Antrag stellenden Personen sowie deren Erziehungsberechtigten in der Schule und bei der BVG zu löschen.

Die Senatsverwaltung für Bildung, Wissenschaft und Forschung hat unsere datenschutzrechtlichen Empfehlungen bei der Vertragsvereinbarung mit der BVG zur Einführung der SchülerCard im Wesentlichen berücksichtigt.

8.3.4 Der Schüler als Fernsehstar – Eine (nachträgliche) Erfolgsgeschichte für den Datenschutz!

Im vergangenen Jahr[150] berichteten wir über die datenschutzrechtlichen Probleme bei der Herstellung und Ausstrahlung der Fernsehreportage „S.O.S. Schule – Hilferuf aus dem Klassenzimmer". Damals mussten wir feststellen, dass die betroffene Schule es im Vorfeld der Fernsehaufnahmen versäumt hatte, von den betroffenen Schülerinnen, Schülern und Lehrkräften die erforderlichen schriftlichen Einwilligungen in die Übermittlung ihrer Daten an die Fernsehproduktionsfirma einzuholen.

In seiner Stellungnahme zum Jahresbericht 2006[151] hat der Senat dazu ausgeführt, dass die Beanstandung des Berliner Beauftragten für Datenschutz und Informationsfreiheit in der Angelegenheit zu Recht erfolgt sei. Der Vorfall sei zum Anlass genommen worden, um die Schulen auf die datenschutzrechtlichen Bestimmungen und den Umstand, dass sie im Hinblick auf die Erteilung der Drehgenehmigung und die schriftliche Einwilligungserklärung der Betroffenen im Vorfeld der Aufnahmen selbst handeln müssen, hinzuweisen.

Von der Senatsverwaltung für Bildung, Wissenschaft und Forschung wurde zu diesem Zweck ein „Merkblatt zur Übermittlung personenbezogener Daten an Dritte im Rahmen von Interviews, TV- und Filmaufnahmen an der Berliner Schule" nebst Mustern für die einzuholenden schriftlichen Einwilligungen gefertigt und an die Schulen verteilt. Damit hat die Senatsverwaltung einen wichtigen Beitrag zur Wahrung der Persönlichkeitsrechte und der Einhaltung der Datenschutzrechte bei Film- und Fernsehaufnahmen in den Berliner Schulen geleistet.

8.3.5 Schülerstatistik online ab Herbst 2008

Auch im vergangenen Jahr wurde zwischen Bildungspolitik, Bildungsforschung und Datenschutzbeauftragten heftig über eine bundesweite Schüler- bzw. Bildungsdatenbank mit einem eindeutigen Personenkennzeichen gestritten, der sog. Schüler-ID. Die Fronten wurden bei einer Tagung im Februar 2007 in Berlin im Roten Rathaus deutlich.

Auch wenn die Bildungspolitik und die Bildungsforschung von einer Einwegverschlüsselung der Schülerdaten über eine sog. Hash-Funktion ausgingen, stellen

[150] JB 2006, 6.3.3

[151] Abghs.-Drs. 16/0772, S. 133

die Datenschutzbeauftragten die Erforderlichkeit einer solchen Datenbank in Frage. Bislang ist nicht der Nachweis geführt worden, dass entsprechende Erkenntnisse nicht auch über eine Stichprobe gewonnen werden können. Aufseiten der Bildungspolitik und -forschung scheint jedoch Bewegung in die Diskussion gekommen zu sein. Im November 2007 machten die Bundesbildungsministerin und Berlins Senator für Bildung, Wissenschaft und Forschung als Vorsitzender der Kultusministerkonferenz erstmals das Bestreben öffentlich, ein bildungswegübergreifendes Bildungspanel zu schaffen. Wie dieses im Einzelnen konzipiert werden soll, muss datenschutzrechtlich eingehend geprüft werden.

Unabhängig davon sind in Berlin zwischenzeitlich die Voraussetzungen geschaffen worden, ab Herbst 2008 die bisherige klassenbezogene Bildungsstatistik auf eine Schülerindividualstatistik mit Online-Datenerhebung umzustellen. Die Schulen übermitteln dann die Statistikdaten nicht mehr klassenweise in Papierform, sondern je Schüler elektronisch, verschlüsselt mit einem nur der Schule bekannten Pseudonym, an die Statistikstelle der Senatsschulverwaltung. Eine Rechtsgrundlage dafür besteht schon seit 1994. Ein Datensicherheitskonzept liegt vor und wurde von uns nicht grundsätzlich bemängelt. Ab Februar 2008 beginnen die Einweisungen und Schulungen für die Berliner Schulen. In den nächsten Monaten wird der Berliner Beauftragte für Datenschutz und Informationsfreiheit insbesondere die Abschottung der Statistikstelle in der Senatsverwaltung für Bildung, Wissenschaft und Forschung überprüfen, damit es nicht zu einer unzulässigen Vermengung von Verwaltungsvollzug und Statistik kommen kann.

Nach den vorliegenden Unterlagen ist die Schülerindividualstatistik als Onlinestatistik datenschutzrechtlich hinreichend vorbereitet. Die Datensicherheit und die Abschottung der Statistikstelle in der Senatsverwaltung sind noch zu prüfen.

9 Wirtschaft

9.1 Novellierung des Wertpapierhandelsgesetzes

Das Gesetz zur Umsetzung der Richtlinie über Märkte für Finanzinstrumente und der Durchführungsrichtlinie der Kommission (Finanzmarktrichtlinie-Umsetzungsgesetz)[152] soll die Rechte der Bankkundinnen und -kunden stärken und die Transparenzpflichten der Banken erhöhen. Neu geregelt wurde auch die Pflicht der Finanzdienstleister zur Abfrage von Kundendaten vor einer Anlageberatung, einer Finanzportefeuilleverwaltung oder der Entgegennahme von Kundenaufträgen. Zu der Umsetzung der Neuregelung, die am 1. November 2007 in Kraft trat, liegen erste Erfahrungen vor. Festgestellt werden kann jedenfalls, dass die Banken nach dem Motto „Lieber ein Datum zu viel als zu wenig" verfahren. So sollen zwar nach § 31 Abs. 4 und 5 Wertpapierhandelsgesetz Informationen über Kenntnisse und Erfahrungen der Kundinnen und Kunden in Bezug auf geplante Geschäfte abgefragt werden, nicht jedoch der Bildungsstand, wie dies eine Berliner Bank machte. Auch die Frage des Güterstandes dürfte für die Wertpapierberatung wenig zielführend sein. Das Hauptproblem bei der Datenerhebung der Kundinnen und Kunden ist aber, dass die Banken in der Regel für die gesamte Kundschaft einen einheitlichen Fragebogen verwenden. Hierbei wird übersehen, dass bei einer Kundin oder einem Kunden, die bzw. der eine sog. AAA-Anleihe im Euro-Raum kaufen will, keine Informationen über Erfahrungen mit Optionsgeschäften benötigt werden. Bei der Anlageberatung oder Finanzportefeuilleverwaltung sind auch nur die Fragen erforderlich, die Finanzinstrumente betreffen, die die Kundschaft nicht vorab ausgeschlossen hat.

Die Abfrage von Anlegerdaten durch Finanzdienstleister hat sich am Erforderlichkeitsprinzip zu orientieren.

9.2 Verkauf der Landesbank Berlin

Im Jahr 2007 wurde die Landesbank Berlin an den Deutschen Sparkassen- und Giroverband verkauft. In dem Bieterverfahren hatten die Interessierten Gelegenheit, sich über die finanzielle Situation des potenziellen Kaufobjekts zu informieren (due-dilligence-Verfahren). Während dieses Verfahrens wurden die für die Interessierten entscheidungserheblichen Unterlagen in einen sog. „grünen Raum" gebracht. In diesem Raum be-

[152] BGBl. I 2007, 1330 ff.

fanden sich keine Akten, sämtliche Unterlagen waren eingescannt. Die Bietenden hatten insbesondere Zugriff auf ausgewählte Kreditakten und andere Portefeuille-Angaben des Unternehmens.

Während des Bieterverfahrens ist sicherzustellen, dass die Bietenden keine personenbezogenen Informationen über die Bankkundinnen und -kunden, die auch durch das Bankgeheimnis geschützt sind, über andere Geschäftspartner der Bank und über Beschäftigte erhalten. Gerade zu diesem Zweck wird der „grüne Raum" eingerichtet, in den nur anonymisierte Unterlagen gelangen dürfen. Wie beim Verkauf der Berliner Bank[153] haben wir in der Bank eine Kontrolle durchgeführt, um zu überprüfen, ob das Anonymisierungsgebot im Bieterverfahren eingehalten wurde. Hierzu haben wir aus unter 3.200 Dokumenten Stichproben gemacht.

Die größten Mängel wurden bei den Immobilienmietverträgen festgestellt. Hier hatte die Landesbank Berlin überhaupt keine Schwärzungen durchgeführt. Die Dokumente enthielten somit den Vor- und Nachnamen der Mieterinnen und Mieter, die Anschrift, teils zusätzlich die Privatanschrift, die Miethöhe und sogar das Geburtsdatum. Demgegenüber waren die Kreditakten meist sorgfältig anonymisiert, aber auch hier gab es Ausnahmen. In einer Risikokreditakte waren auf einem Fax der Name und die Faxnummer des Kreditnehmers sichtbar. Auf dem Fax legte der Kreditnehmer seine Solvenz anhand von kopierten Kontoauszügen dar. Teils wurde versäumt, die Unterschrift des Kreditnehmers zu schwärzen. Die Kreditakte enthielt viele Einzelheiten über verschiedene Mitglieder des Familienbetriebes. Eine Ermittlung dieser Personen wäre ohne Schwärzung unproblematisch möglich gewesen. Ein Dokument enthielt die Auflage des Erblassers, dass die Erben die Grabstätten einer namentlich benannten Familie für einen bestimmten Zeitraum pflegen müssen. Eine Ermittlung der Erben (und Kreditnehmer) erscheint möglich.

Auch die Namen der Beschäftigten der Landesbank Berlin waren in vielen Fällen nicht ausreichend anonymisiert. Nicht geschwärzt waren auch Namen von Notaren und Steuerberatern, Insolvenzverwaltern, Urkundsbeamten, Dienstkräften des Finanzamtes, Reno-Gehilfen etc. Der Bank wurde aufgegeben, vor Beginn des Bieterverfahrens die Mängel zu beseitigen. Dies wurde von uns in einer Stichprobe überprüft.

Beim Verkauf landeseigener Unternehmen (z. B. Banken, Wohnungsbaugesellschaften) ist sicherzustellen, dass personenbezogene Daten insbesondere von Kundschaft und Beschäftigten vor Beginn des Bieterverfahrens ausgesondert und nur diejenigen Unternehmensunterlagen offenbart werden, die die Kaufinteressier-

[153] JB 2006, 7.2.1

ten zur Einschätzung der finanziellen Situation des potenziellen Kaufobjekts benötigt. Eine entsprechende Beschlussempfehlung hat zwischenzeitlich auch der Unterausschuss Datenschutz und Informationsfreiheit des Innenausschusses des Abgeordnetenhauses gegeben.

9.3 Datenübermittlung des Versicherungsvermittlers an die Versicherung

Gewerbliche Versicherungsvermittler sind nach dem Versicherungsvertragsgesetz[154] verpflichtet, die Kundinnen und den Kunden umfassend zu beraten und diese Beratung zu dokumentieren. Dazu werden sie die Vermögensverhältnisse (einschließlich der familiären und steuerlichen Situation) der künftigen Versicherten erfragen und sie darauf aufbauend beraten. Dies führt dazu, dass die hierbei erhobenen Daten bei komplizierten und teuren Versicherungen umfangreich und detailliert sein können. Für die Versicherer stellen diese Daten einen großen Wert dar, da sie z. B. ihre Werbemaßnahmen gezielt an die persönlichen Verhältnisse der Versicherten anpassen können. Eine Versicherung forderte von seinen Versicherungsvermittlern die Zusendung der Protokolle.

Gewerbsmäßige Versicherungsvermittler können sowohl Versicherungsvertreter sein, die auf Versichererseite tätig sind, als auch Versicherungsmakler, die nicht von einem Versicherer beauftragt sind.

Dem Versicherungsmakler dienen die Beratungsprotokolle als Hilfsmittel zur Erfüllung seiner gesetzlichen Beratungspflicht und zusätzlich zum Zwecke der Verteidigung gegen Schadensersatzansprüche des Versicherungsnehmers aus § 63 VVG. Für das Versicherungsverhältnis zwischen Versicherer und Versicherungsnehmer sind die Beratungsprotokolle ohne Bedeutung, eine nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) erforderliche Rechtsvorschrift für die Übermittlung des Beratungsprotokolls an die Versicherung ist nicht ersichtlich. So haftet die Versicherung nach § 6 Abs. 6 VVG auch nicht für Beratungsfehler des Versicherungsmaklers. Demgegenüber erfüllt der Versicherungsvertreter mit seiner Beratung und Dokumentation zusätzlich auch die neu eingeführte Beratungspflicht des Versicherers aus § 6 VVG. Eine Übermittlung des Beratungsprotokolls bei Versicherungsvertretern ist danach nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG rechtmäßig.

[154] §§ 61, 62 VVG

9.4

Falls das Beratungsprotokoll sensitive Daten im Sinne von § 3 Abs. 9 BDSG enthält (z. B. Gesundheitsdaten), darf das Beratungsprotokoll insoweit nicht übermittelt werden. Sensitive Daten sind entweder zu schwärzen oder der Versicherungsvertreter muss sich vor der Übermittlung sensitiver Daten eine Einwilligung nach §§ 4, 4 a Abs. 1 und 3 BDSG geben lassen.

Versicherungsmakler dürfen ohne Einwilligungserklärung des Betroffenen das Beratungsprotokoll nicht an die Versicherung übermitteln, wohl aber – in bestimmten Grenzen – die Versicherungsvertreter.

9.4 Vorsicht bei Hilfsangeboten

Es kommt in letzter Zeit häufiger vor, dass Bürgerinnen und Bürger ein überraschendes Hilfsangebot erhalten. So wird Schuldnerinnen oder Schuldnern, die in das Schuldnerverzeichnis eingetragen wurden, eine Schuldnerberatung oder Schuldenregulierung angeboten. Fondsbesitzer, deren Fonds in den Konkurs zu drohen gehen, erhalten Hilfsangebote von angeblichen Selbsthilfeorganisationen oder „Verbraucherschützern". Ziel des Hilfsangebotes ist es in der Regel, für Anwaltskanzleien Mandate zu akquirieren und Vermittlungsgebühren zu erhalten.

Die angeblichen Helfer handeln auch datenschutzrechtlich unzulässig. Schuldnerverzeichnisdaten dürfen nur zu den in § 915 Abs. 3 Zivilprozessordnung (ZPO) genannten Zwecken verwendet werden, insbesondere um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldnerinnen und Schuldner ihren Zahlungsverpflichtungen nicht nachkommen. Die Verwendung von Schuldnerverzeichnisdaten für Werbezwecke ist demgegenüber in § 915 Abs. 3 ZPO nicht vorgesehen und damit rechtswidrig.

Die personenbezogenen Daten von Fondszeichnern beschaffen sich die Vereine häufig aus dem Handelsregister. Zur Durchführung der Mailingaktion werden die Handelsregisterdaten mit Adressdaten aus öffentlich-zugänglichen Quellen ergänzt. Nach § 9 Abs. 1 Handelsgesetzbuch (HGB) ist die Einsicht des Handelsregisters jedem zu Informationszwecken gestattet. Nach § 9 Abs. 2 Satz 1 HGB kann von den Eintragungen eine Abschrift gefordert werden. Die im HGB erwähnten Informationszwecke beziehen sich insbesondere auf die Publizität des Handelsregisters[155]. Von der Intention des § 9 HGB ist jedenfalls nicht jede Datenabfrage, insbesondere nicht die zur Kundenakquise, erfasst.

[155] vgl. § 15 HGB

Auch wenn die Einsicht des Handelsregisters jedem zu Informationszwecken gestattet ist, bedeutet dies nicht, dass die Speicherung, Veränderung, Übermittlung und Nutzung dieser personenbezogenen Daten unbegrenzt möglich sind. Dies ergibt sich aus § 28 Abs. 1 Satz 1 Nr. 3 BDSG. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt. Selbst wenn § 9 Abs. 1 HGB die Datenerhebung der Handelsregisterdaten gestatten würde, würde dies nicht bedeuten, dass auch die Speicherung der personenbezogenen Daten in der verantwortlichen Stelle, die Anreicherung dieser Daten durch die Adressdaten und die Nutzung dieser Daten für die Mailingaktion durch § 9 Abs. 1 HGB abgedeckt sind. Bei der nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG vorzunehmenden Abwägung ist gerade auch zu berücksichtigen, dass das Handelsgesetzbuch bewusst darauf verzichtet hat, die genaue Adresse als einzutragendes Datum in das Handelsregister aufzunehmen.

Überraschende Hilfsangebote von Schuldnerberatungen und vermeintlichen Verbraucherschutzorganisationen verstoßen in der Regel gegen datenschutzrechtliche Vorgaben. Auch im Übrigen ist Vorsicht geboten.

9.5 Bonitätsprüfung eines Vereinsvorsitzenden

Der Vorsitzende eines Vereins verhandelte mit einem Immobilienunternehmen über die Anmietung eines größeren Objektes. Der potenzielle Vermieter holte bei einer Wirtschaftsauskunftei eine umfassende Auskunft über den Petenten persönlich ein. Aufgrund dieser Auskunft brach das Immobilienunternehmen die Verhandlungen mit dem Verein ab.

Es ist höchstrichterlich anerkannt, dass im Zusammenhang mit einer Auskunft über eine juristische Person auch die Speicherung und Weitergabe persönlicher Daten über die Vertretung der juristischen Person zulässig sind, wenn diese im Rahmen der Gesamtbeurteilung der Kreditwürdigkeit nicht ohne Gewicht sind[156]. Danach wäre es rechtlich nicht zu beanstanden, wenn in einer Auskunft über den Verein Schuldnerverzeichnisinformationen über den Vereinsvorsitzenden enthalten sind. So ist es vertretbar, der Auskunft über einen Verein den Hinweis hinzuzufügen, dass der Vereinsvorsitzende Geschäftsführer einer GmbH war, bei deren

[156] BGH, NJW 2003, 2904; NJW 1986, 2505

Vermögen die Eröffnung eines Insolvenzverfahrens mangels Masse abgelehnt worden ist, weil dies Aufschlüsse über die Fähigkeit des Vereinsvorsitzenden, den Überblick über die wirtschaftlichen Verhältnisse der von ihm geleiteten Körperschaft zu behalten, geben könnte. Diese Informationen dürften an Gläubiger übermittelt werden, die gegenüber dem Verein ein wirtschaftliches Risiko eingehen.

Davon ist jedoch der Fall zu unterscheiden, dass dem potenziellen Vertragspartner eines eingetragenen Vereins eine Vollauskunft über die persönlichen Verhältnisse eines Vorstandsmitgliedes eines Vereins übermittelt wird. Hier ist zu berücksichtigen, dass der geplante Vertrag das Vorstandsmitglied nicht selbst verpflichtet; eine persönliche Haftung kommt nur in extremen Ausnahmefällen wie einer Insolvenzverschleppung in Betracht[157]. Es besteht also kein Grund, warum der potenzielle Vertragspartner des Vereins eine vollständige Bonitätsauskunft über das Vorstandsmitglied erhalten sollte. Die Übermittlung dieser Daten ist nach § 29 Abs. 2 Nr. 2 BDSG rechtswidrig, da bei diesem umfangreichen Bonitätsdatensatz die schutzwürdigen Interessen des Betroffenen höher zu gewichten sind als die eher zweifelhaften Interessen des potenziellen Vertragspartners.

Die Bonitätsprüfung eines Vereins rechtfertigt nicht die Übermittlung sämtlicher verfügbarer Bonitätsinformationen über den Vereinsvorsitzenden.

9.6 Spendenaufruf per Telefon

Ein gemeinnütziger Verein, der seine Vereinstätigkeit zu einem wesentlichen Teil aus privaten Spenden finanziert, wollte die öffentlich zugänglichen Telefonnummern seiner Spenderinnen und Spender (Telefonbuch, Telefon-CD) ermitteln und telefonisch um weitere Spenden bitten. Dies sei möglich, da NGOs (Nichtregierungsorganisationen) nicht unter das Gesetz gegen den unlauteren Wettbewerb (UWG) fielen. Der Verein bat uns um Auskunft, wie wir die geplante Telemarketingmaßnahme datenschutzrechtlich bewerten.

Ob NGOs unter das UWG fallen oder nicht, ist bisher noch nicht höchstrichterlich entschieden worden. Für die datenschutzrechtliche Bewertung kann die Frage aber offen bleiben, da das von dem Verein beabsichtigte Telemarketing wegen fehlender Rechtsvorschrift nach § 4 Abs. 1 BDSG rechtswidrig ist.

[157] § 42 Abs. 2 Satz 2 Bürgerliches Gesetzbuch (BGB)

§ 28 Abs. 1 Satz 1 Nr. 1 BDSG kommt als Rechtsvorschrift nicht in Betracht, da es hier um eine Werbung für eine neue Spende, nicht jedoch um die Abwicklung der erfolgten Spende geht.

§ 28 Abs. 3 Satz 1 Nr. 3 BDSG begründet das sog. Werbeprivileg. Die listenmäßige Verarbeitung der unter a) bis g) aufgezählten Daten wird durch den Gesetzgeber – um Werbung zu erleichtern – privilegiert. Der Gesetzgeber hat bei dem Werbeprivileg zwar die Anschrift der Betroffenen aufgenommen, um postalische Werbung zu ermöglichen; er hat jedoch bewusst darauf verzichtet, Telefonnummer und E-Mail-Adresse zu privilegieren. Danach kommt § 28 Abs. 3 Satz 1 Nr. 3 BDSG nicht als eine das Telemarketing rechtfertigende Rechtsvorschrift in Betracht.

Als Rechtsvorschriften können auch § 28 Abs. 1 Satz 1 Nr. 2 oder 3 BDSG nicht herangezogen werden. Nach diesen Rechtsvorschriften müssen die Interessen der verantwortlichen Stelle mit den schutzwürdigen Interessen der Betroffenen abgewogen werden. Auch wenn der Name und die Telefonnummer dem Telefonbuch entnommen werden können, ist Nr. 3 nicht einschlägig, da für die Werbeaktion auch die öffentlich nicht zugängliche Information benötigt wird, dass die Angerufenen schon einmal gespendet haben. Bei der Anwendung des § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist es schon zweifelhaft, ob der Verein berechtigte Interessen an dem Telemarketing geltend machen kann, zumal er auch die Möglichkeit hätte, postalische Werbung zu betreiben. In jedem Fall liegen aber überwiegende schutzwürdige Interessen der Betroffenen vor. Diese müssen nicht damit rechnen, dass ihre nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG verarbeiteten Daten um Telefondaten erweitert werden, um sie anschließend im Rahmen von „Cold Calls“ (unerbetene Telefonanrufe) zu neuen Spenden zu bewegen.

Auch Spendenorganisationen sind ohne Einwilligung der Betroffenen nicht zu telefonischer Werbung berechtigt.

9.7 Unverzügliche Beachtung des Werbewiderspruchs

Ein Unternehmen, das postalische Werbung versandte, informierte Betroffene, die Werbewiderspruch eingelegt haben, darüber, dass sie in den nächsten drei Monaten noch mit Werbung des Unternehmens rechnen müssten. Derartige Werbung sei nach hergebrachter Auffassung des Bundesgerichtshofs trotz Widerspruch zu dulden, denn es stünde außer Verhältnis zum Grad der durch die Werbung eingetretenen Belästigung, wenn

bereits gedrucktes Werbematerial aus einer größeren Auflage wieder aussortiert werden müsste.

Das Unternehmen berief sich zur Begründung der Dreimonatsfrist auf ein Urteil des Bundesgerichtshofs aus dem Jahre 1973, dem ein Lebenssachverhalt aus dem Jahre 1970 zugrunde lag[158]. Dort hatte der Bundesgerichtshof entschieden, dass die Beachtung des Widerspruchs nicht geboten sei, wenn dies wegen Art und Anlage der Werbeaktion für das werbende Unternehmen mit einem Arbeits- und Kostenaufwand verbunden sei, der in keinem angemessenen Verhältnis zu der mit der Werbung verbundenen Belästigung der Umworbenen stehe. Das werbende Unternehmen hatte übersehen, dass der Bundesgerichtshof für den Sachverhalt aus dem Jahre 1970 nur Normen des Bürgerlichen Gesetzbuches angewandt hat, da das Bundesdatenschutzgesetz noch nicht in Kraft getreten war. Eine Berufung auf dieses Urteil für Lebenssachverhalte aus dem Jahre 2007 ist somit nicht möglich. Die sofortige Beachtung des Werbewiderspruchs wird durch die moderne Computertechnik erleichtert. Analog § 3 a BDSG sind Werbeaktionen so zu organisieren, dass Werbewidersprüche unverzüglich (ohne schuldhaftes Zögern) umgesetzt werden können.

Werbewidersprüche sind unverzüglich zu beachten.

9.8 Sachgerechte Datensperrung

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. Allerdings tritt nach § 35 Abs. 3 Nr. 1 BDSG in diesen Fällen anstelle einer Löschung eine Sperrung, wenn der Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen. Insbesondere haben Wirtschaftsunternehmen Aufbewahrungsfristen nach dem Handelsgesetzbuch (Wirtschaftsprüfung) und der Abgabenordnung (Steuerprüfung) zu beachten.

Bei mehreren Prüfungen auch größerer Unternehmen mussten wir feststellen, dass die vom Gesetz geforderte Datensperrung nur selten sachgerecht durchgeführt wird. Die „gesperrten Daten“ werden zwar wie vom Gesetz gefordert[159] gekennzeichnet, verbleiben jedoch im operativen Geschäft. So kommt es vor, dass Bank-

[158] BGH, GRUR 1973, 552

[159] vgl. § 3 Abs. 4 Nr. 4 BDSG

kundinnen oder -kunden nach mehreren Jahren wieder zu ihrer alten Bank wechseln und sich darüber wundern, dass die für die Kontoeröffnung zuständige Sachbearbeiterin bereits über alle erforderlichen personenbezogenen Daten verfügt.

Die Kennzeichnung ist kein Selbstzweck, sondern soll gerade sicherstellen, dass die mit der Sperrung einhergehenden Verarbeitungs- und Nutzungseinschränkungen eingehalten werden und die Daten von der Ausnahme des § 35 Abs. 8 BDSG abgesehen nur zu dem Zweck genutzt oder verarbeitet werden, der die Sperrung der Daten anstelle der Löschung erforderlich machte.

Gesperrte Daten sind aus dem operativen Geschäft zu entfernen.

9.9 Sperrdatei für Teilnahme am Glücksspiel

Das Bundesverfassungsgericht hat in einem Urteil vom März 2006[160] dem Gesetzgeber aufgegeben, bei Beibehaltung des staatlichen Sportwettmonopols die Begrenzung der Wettleidenschaft und Bekämpfung der Wettsucht materiell und strukturell zu gewährleisten. Der zum 1. Januar 2008 in Kraft getretene Staatsvertrag zum Glücksspielwesen in Deutschland[161] soll die vom Bundesverfassungsgericht geforderten Anforderungen erfüllen. Zu diesem Zweck wurden durch den Staatsvertrag Spielbanken und andere Glücksspielveranstalter verpflichtet, ein übergreifendes Spielersperrsystem zu unterhalten[162].

Der Glücksspielstaatsvertrag benennt keine einzelne Stelle, die für den Datenbestand der Sperrdatei verantwortlich ist. Verantwortliche Stelle ist somit jede einmeldende Stelle für den eingemeldeten Datenbestand[163]. Dies führt dazu, dass jede einmeldende Stelle gleichzeitig Auskunftei ist und sich als solche bei den Aufsichtsbehörden nach § 4 d Abs. 1, 4 BDSG anzumelden hat. In die Sperrdatei einmelden können neben den Betroffenen (Selbstsperre) auch Mitarbeiterinnen und Mitarbeiter der Glücksspielveranstalter und Dritte (einseitige Sperren bzw. Fremdsperren). Die Sperrgründe „Spielsuchtgefährdet“, „Überschuldet“, „Spieleinsätze, die in keinem Verhältnis zum Einkommen und Vermögen stehen“ sind nachvollziehbar, nicht jedoch der Sperrgrund „Kommt seinen finanziellen Verpflichtungen

[160] BVerfG, NJW 2006, S. 1261 ff.
[161] GVBl. 2007, 604
[162] vgl. § 8 Abs. 1 GlüStV
[163] vgl. § 3 Abs. 5 AG GlüStV

nicht nach“. Eine Person, die bei bestimmten Rechnungen Zahlungsunwilligkeit zeigt, kann zwar in eine Bonitätswarndatei eingemeldet werden, allerdings kann sie über eine durchaus ausreichende Vermögensgrundlage verfügen, sodass eine Sperre für Glücksspiele nicht berechtigt wäre. Die Einschätzung des Personals aufgrund von Wahrnehmungen erscheint subjektiv, objektivierbare Kriterien werden in dem Staatsvertrag nicht genannt. Da auch Dritte die Möglichkeit haben, Meldungen abzugeben, besteht die Gefahr des denunziatorischen Missbrauchs, zumal unklar bleibt, welche Verifizierungsanforderungen an die Informationen der Dritten zu stellen sind.

Glücksspielveranstalter und Spielbanken benötigen nur die Information, dass eine bestimmte Spielerin oder ein bestimmter Spieler zu dem Zeitpunkt, zu dem sie bzw. er einen Spielvertrag abschließen wollte, gesperrt ist. Die in der Sperrdatei enthaltenen Informationen „Grund der Sperre“, „Dauer der Sperre“ und „Dokumente, die zur Sperrung geführt haben“ werden nicht benötigt, die im Staatsvertrag geregelte Übermittlung dieser Informationen an die Sperrdatei ist überflüssig und damit verfassungsrechtlich bedenklich. Nicht benötigt wird auch das Lichtbild der Spielerinnen oder des Spielers, da sie sich vor Abschluss des Spielvertrages sowieso ausweisen müssen.

Nicht verständlich ist auch, dass die Daten der Gesperrten nach Ablauf der Sperre noch sechs Jahre aufzubewahren sind. Zu welchem Zweck diese Aufbewahrung erfolgt, ergibt sich aus dem Staatsvertrag nicht.

Der Glücksspielstaatsvertrag sieht die Verarbeitung personenbezogener Daten in einer Sperrdatei vor, deren Umfang unverhältnismäßig in das Recht auf informationelle Selbstbestimmung der gesperrten Person eingreift.

10 Europäischer und internationaler Datenschutz

10.1 Europäische Union

Die Europäische Union ist am 1. Januar 2007 um Bulgarien und Rumänien erweitert worden. Datenübermittlungen in alle nunmehr 27 Mitgliedstaaten der Europäischen Union und in die übrigen Mitgliedstaaten des Europäischen Wirtschaftsraums (Island, Liechtenstein, Norwegen) sind nun unter vereinfachten Voraussetzungen möglich[164].

Seit dem 1. August gilt das *neue PNR-Abkommen* zwischen der Europäischen Union und den USA „über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records - PNR) und deren Übermittlung durch die Fluggesellschaften an das US-Department of Homeland Security (DHS) (*PNR-Abkommen von 2007*)“[165]. Damit wurden die Flugpassagierdatenübermittlungen an die US-Heimatschutzbehörde auf eine neue rechtliche Grundlage gestellt, die das Interimsabkommen zwischen der EU und den USA endgültig abgelöst hat. Dieses war als Konsequenz der Nichtigkeitsentscheidung des Europäischen Gerichtshofs im letzen Jahr ausgehandelt worden[166]. Schon an der äußeren Form des neuen Abkommens ist erkennbar, dass die US-Seite die Bedingungen maßgeblich diktiert hat: Der im Anhang befindliche Schriftwechsel zwischen den Vertragsparteien besteht aus einem vierseitigen Schreiben der USA an die EU und einem halbseitigen Antwortschreiben der EU. Das neue Abkommen entspricht aus europäischer Sicht nicht den datenschutzrechtlichen Standards. Die viel gelobte Reduzierung der Anzahl der Daten von 34 auf 19 kann sogar als „Etikettenschwindel“ bezeichnet werden, denn in Wahrheit ist der Datenumfang nicht geringer geworden. Tatsächlich wurden Datensätze nur zusammengefasst, z. B. Postadresse, E-Mail-Adresse und Telefonnummer unter einem neuen Punkt „Kontaktdaten“. Auch „sensitive“ Daten, die z. B. auf die Religionszugehörigkeit schließen lassen, müssen weiterhin an die US-Heimatschutzbehörde übermittelt werden.

Darüber hinaus enthält das neue Abkommen keine definitive Festlegung, welche US-Behörden für welche Zwecke auf diese Daten zugreifen können. Sie sollen zwar in erster Linie der Terrorismusbekämpfung dienen, ihre Verwendung zu beliebigen anderen Zwecken hat sich die US-Seite aber vorbehalten. Letzteres gilt auch nach dem Ende der neuen Speicherfrist, die den eigentlich skandalösen Aspekt des Abkommens darstellt. Sie wurde von 3,5 auf 15 Jahre verlängert, wobei

---

164 § 4 b Abs. 1, 2 Bundesdatenschutzgesetz (BDSG)

165 Beschluss des Rates der EU v. 23. Juli 2007; ABl. L 204, S. 16 ff.

166 ausführlich JB 2006, 8.1

die Daten in den letzten acht Jahren „ruhen“, d. h., sie werden nicht gelöscht und dürfen bei besonderem Verdacht verwendet werden.

Im Gegensatz zum früheren Abkommen erfolgt eine Evaluation des neuen Abkommens auf Wunsch der USA ohne Einbeziehung der Art. 29-Datenschutzgruppe. Diese hat sich mit den genannten und weiteren Details des Folgeabkommens kritisch auseinandergesetzt[167]. Bereits einige Monate vorher hat sie Musterinformationsblätter ausgearbeitet, die es den Reisebüros, Fluggesellschaften und sonstigen Organisationen erleichtern sollen, ihrer Informationspflicht gegenüber den Fluggästen einheitlich nachzukommen[168]. Abzuwarten bleibt nun, ob die endgültig zum 1. Januar 2008 ins Auge gefasste Umstellung des Übermittlungsverfahrens vom Pull- zum Push-System endlich realisiert wird. Dann wäre immerhin der direkte Zugriff der USA auf die PNR-Daten ausgeschlossen, weil die Fluggesellschaften von sich aus die verlangten Daten übermitteln.

Neuerdings zeigt sich auch die EU-Kommission von dieser „Antiterrormaßnahme“ überzeugt, denn sie will nun ihrerseits ein eigenes System zur Auswertung von Flugpassagierdaten errichten. Es soll „auf Vorrat“ alle Passagiere umfassen, die in die EU einreisen, und ist eng an das neue PNR-Abkommen mit den USA angelehnt. Dies hat die Art. 29-Datenschutzgruppe bereits scharf kritisiert. Bisher sei eine dringende Notwendigkeit für eine so weitreichende Maßnahme nicht dargelegt worden.

Das neue PNR-Abkommen mit den USA erfüllt nicht den europäischen Datenschutzstandard. Die Schaffung eines vergleichbaren Datenpools in Europa ist nicht zu rechtfertigen.

Mehrfach hat sich die Art. 29-Datenschutzgruppe mit Vertretern von *SWIFT (Society for Worldwide Interbank Financial Telecommunication)* getroffen, um ein datenschutzgerechtes Verfahren für internationale Finanztransaktionen zu entwickeln[169]. Im letzten Jahr hatten US-Medien aufgedeckt, dass der weltweit agierende Geldüberweisungsdienst zur Übermittlung von internationalen Zahlungsanweisungen den US-Behörden den Zugang zu den in den USA gespeicherten Daten ermöglichte.

---

[167] Stellungnahme 5/2007 v. 17. August 2007, WP 138, vgl. Dokumentenband 2007, S. 68

[168] Stellungnahme 2/2007 v. 15. Februar 2007 zur Information von Fluggästen über die Übermittlung von PNR-Daten an amerikanische Behörden, WP 132

[169] ausführlich JB 2006, 8.1

Zu den datenschutzrechtlichen Kernforderungen der Art. 29-Datenschutzgruppe zählt die Speicherung von Banküberweisungsdaten, die den innereuropäischen Zahlungsverkehr betreffen, allein in Europa oder in einem Drittstaat mit ausreichendem Datenschutzniveau. SWIFT will dem durch eine neue dezentrale Systemarchitektur Rechnung tragen, sodass Zugriffe von Drittstaaten auf diese Daten nicht mehr möglich sind. Künftig soll ein weiteres europäisches Datenverarbeitungszentrum in der Schweiz ansässig sein, auf dem alle Überweisungsdaten gespiegelt werden. Der vorhandene Server in den USA wird alle Überweisungsdaten der „Transatlantischen Zone" speichern, der bestehende Server in den Niederlanden dagegen alle Daten der „Europäischen Zone". Zu dieser Zone sollen alle Staaten des Europäischen Wirtschaftsraums und der Schweiz gehören. In allen übrigen Staaten können die entsprechenden nationalen Mitgliedsgruppen von SWIFT selbst wählen, zu welcher Zone sie gehören wollen.

Die zweite Kernforderung der Art. 29-Datenschutzgruppe ist eine entsprechende Information der Kundinnen und Kunden durch die Kreditinstitute. Die Gruppe hat hierzu einen Statusbericht erstellt, aus dem sich ergibt, dass alle Datenschutzaufsichtsbehörden in Europa in Kontakt mit den Banken und Finanzinstitutionen des jeweiligen Landes getreten sind. Wichtiger Bestandteil des Berichts ist ein Vorschlag, welche Elemente eine Information der Bank gegenüber den Bankkundinnen und -kunden beinhalten sollte. Eine einheitlich formulierte Kundeninformation ist dagegen nicht vorgesehen. Die Information der Bankkundinnen und -kunden erfolgt auch in Berlin bisher noch nicht in ausreichendem Maß[170].

SWIFT beabsichtigt, die neue dezentrale Systemarchitektur bis Ende 2009 einzuführen. Für die Übergangszeit ist gleichwohl eine gewisse Gewähr für den datenschutzgerechten Umgang mit europäischen Daten gegeben, denn SWIFT hat sich vorsorglich dem Safe-Harbor-Abkommen unterworfen. Die deutschen Aufsichtsbehörden haben allerdings betont, dass diese Maßnahme allein die strukturellen Datenschutz-Mängel bei SWIFT nicht beheben kann.

Dank des beharrlichen Einsatzes der Europäischen Datenschutzbehörden ist die Verarbeitung von innereuropäischen Finanztransaktionsdaten durch SWIFT auf einen datenschutzkonformen Weg gebracht.

[170] vgl. 2.5

10.2 Weitere Ergebnisse aus Brüssel

Die Art. 29-Datenschutzgruppe hat erneut zahlreiche Arbeitspapiere und Stellungnahmen verfasst. So hat sie sich mit der „Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)“ befasst und die Anforderungen definiert, die bei der Einrichtung solcher Systeme an den Datenschutz und die besonderen Schutzmechanismen dieser Systeme gestellt werden müssen[171]. Auch hat sie ein „Antragsformular für Genehmigungen von verbindlichen unternehmensinternen Datenschutzregelungen zur Übermittlung personenbezogener Daten“ verabschiedet, das ein einheitliches Vorgehen bei EU-weiter Anerkennung von Unternehmensregelungen gewährleistet[172]. Moderne Datenschutzthemen wie die RFID-Technik, die Online-Gesundheitsfürsorge (E-Health) und das Identitätsmanagement bei elektronischen Behördendiensten (E-Government) machten eine gründliche Auseinandersetzung und Analyse des Begriffs „personenbezogene Daten“ erforderlich[173]. Erstmals wurde in einer EU-weiten Befragungsaktion bei den privaten Krankenversicherungen ermittelt, inwieweit eine Koordinierung von Durchsetzungsaktivitäten der Datenschutzaufsichtsbehörden eine neue, wirksame Überwachungsstrategie sein kann[174]. Darüber hinaus hat sich die Art. 29-Datenschutzgruppe mit den Auswirkungen befasst, die das Binnenmarkt-Informationssystem (BIS, Internal Market Information System – IMI) mit sich bringt, das ein computergestütztes Hilfsmittel für den gesamten Informationsaustausch unter den Verwaltungen der EU-Mitgliedstaaten darstellt[175].

10.3 AG „Internationaler Datenverkehr“

Im Anschluss an die Diskussionen mit Vertreterinnen und Vertretern aus der Wirtschaft im letzten Jahr[176] hat die AG „Internationaler Datenverkehr“ des Düsseldorfer Kreises unter unserem Vorsitz ein „*Positionspapier*“ zu besonderen Fragestellungen beim internationalen Datenverkehr erarbeitet, das vom Düsseldorfer Kreis beschlossen wurde[177]. Daneben wurde eine „*Handreichung zur rechtli-*

---

171 Arbeitspapier v. 15. Februar 2007, WP 131

172 Empfehlung 1/2007 v. 10. Januar 2007, WP 133; vgl. JB 2006, 8.2

173 Stellungnahme 4/2007 v. 20. Juni 2007, WP 136

174 Bericht 1/2007 v. 20. Juni 2007 über die erste gemeinsame Durchsetzungsmaßnahme: Bewertung und zukünftige Schritte, WP 137

175 Stellungnahme 7/2007 v. 21. September 2007 zu Fragen des Datenschutzes im Zusammenhang mit dem Binnenmarkt-Informationssystem, WP 140; vgl. 2.6

176 vgl. JB 2006, 8.3

177 vgl. Dokumentenband 2007, S. 29

chen Bewertung von Fallgruppen zur internationalen Auftragsdatenverarbeitung“ verabschiedet[178]. Sie beinhaltet die häufigsten Fallkonstellationen und soll den Unternehmen die rechtliche Bewertung erleichtern.

Die AG „Internationaler Datenverkehr“ hat erstmals ungelöste Fragestellungen behandelt, die sich bei *Datenübermittlungen durch deutsche Unternehmen an US-Behörden einerseits und an US-Unternehmen im Vorfeld von Rechtsstreitigkeiten („Discovery“) andererseits* ergeben.

In der ersten Fallkonstellation geht es darum, dass deutsche Unternehmen durch Beschlagnahmeanordnungen des US-Justizministeriums direkt verpflichtet werden, personenbezogene Daten ihrer Mitarbeiterinnen und Mitarbeiter in den deutschen Niederlassungen an das Ministerium zu übermitteln. Hintergrund sind die u. a. vom Ministerium geführten Ermittlungen wegen Korruptionsverdachts bei verschiedenen weltweit tätigen Konzernen, die zudem der US-Börsenaufsicht unterliegen. In der zweiten Fallkonstellation geht es um die Herausgabe von Daten an private US-Unternehmen zur Prüfung der Erfolgschancen von zivilrechtlichen Klagen. Im Rahmen dieser „Pre-Trial Discovery of Documents“ können die Zivilprozessparteien nach amerikanischem Recht schon in einem frühen Stadium des Verfahrens umfänglich Einsicht in ihnen möglicherweise dienliche Unterlagen der Gegenseite nehmen. Bei dieser Beweisermittlung im Verfahrensstadium zwischen Klageerhebung und Hauptverhandlung können die gegnerische Partei oder Dritte zur Vorlage von Beweismitteln gezwungen werden, ohne dass die Klage auf ihre Schlüssigkeit hin überprüft wird. Das Gericht wird dabei nur im Rahmen der Anordnung von Schutz- oder Zwangsmaßnahmen eingeschaltet. Im Übrigen verantworten primär die Parteien und ihre Prozessvertreter dieses Verfahren. Die im US-Recht etablierte „Pre-Trial Discovery“, die sich auch auf elektronische Dokumente beziehen kann („E-Discovery“), entspricht in ihrer Wirkung häufig dem nach deutschem Prozessrecht unzulässigen Ausforschungsbeweis. Bereits im letzten Jahr wurde diese Fallkonstellation zur Beurteilung an uns herangetragen. Wir hatten ein zweistufiges Vorgehen befürwortet, das in einem ersten Schritt die Übermittlung pseudonymisierter Daten und erst in einem zweiten Schritt, nämlich im Bedarfsfalle, die Übermittlung personenbezogener Daten beinhaltete[179]. Offenbar hat der Prozessgegner in den USA die Unterscheidung gebilligt, was nicht sicher war und dann mit prozessualen Nachteilen für das Berliner Unternehmen hätte enden können.

Beiden Fallkonstellationen ist die Zwangslage gemeinsam, in der sich deutsche Unternehmen befinden: Sie müssen massive Nachteile finanzieller Art (Verlust des

[178] vgl. a. a. O., S. 31

[179] JB 2006, 8.1 (Fall Schering)

Börsenplatzes, des Prozesses) befürchten, wenn sie dem Herausgabeverlangen der US-Seite nicht folgen. Tun sie dies doch, verstoßen sie gegen die Übermittlungsbestimmungen des deutsches Datenschutzrechts[180], was mit einer Geldbuße bis zu 250.000 Euro geahndet werden kann[181]. Angesichts dieses Konflikts hat die AG „Internationaler Datenverkehr" beschlossen, die politische Ebene einzuschalten. Deshalb wurden diese Fragestellungen an das Bundesministerium der Justiz (BMJ) herangetragen mit dem Ziel, eine einheitliche Beratungspraxis der Aufsichtsbehörden gegenüber deutschen Unternehmen herbeizuführen. Das BMJ hat wie folgt geantwortet:

Bundesministerium der Justiz 31. Januar 2007
Lutz Diwell
Staatssekretär

Herrn
Dr. Alexander Dix
Berliner Beauftragter für
Datenschutz und Informationsfreiheit

Sehr geehrter Herr Dr. Dix,

mit Schreiben vom 5. Januar 2007 haben Sie die Bundesministerin der Justiz um Auskunft zu zwei Fragen des Datenschutzes im nichtöffentlichen Bereich gebeten.

Beide Fälle betreffen die Herausgabe von personenbezogenen Daten durch deutsche Unternehmen. Der erste Fall befasst sich mit der verpflichtenden Übermittlung dieser Daten aufgrund von Beschlagnahmeanordnungen an das US-Justizministerium zur Verwendung in dort geführten strafrechtlichen Ermittlungsverfahren. Der zweite Fall behandelt die Herausgabe von Daten an private US-Unternehmen zur Prüfung der Erfolgschancen von Zivilklagen.

In beiden Fällen bitten Sie um Prüfung, ob und in welchem Umfang Rechtshilfeabkommen einschlägige Regelungen für die Herausgabe von Daten vorsehen.

Hierzu darf ich Ihnen wie folgt antworten:

[180] § 28 BDSG
[181] § 43 Abs. 2 Nr. 1, Abs. 3 BDSG

Zu Frage 1:

Der strafrechtliche Rechtshilfeverkehr zwischen den USA und der Bundesrepublik Deutschland erfolgt derzeit auf vertragsloser Grundlage nach Maßgabe der Vorschriften des Gesetzes über die internationale Rechtshilfe in Strafsachen (IRG).

Verpflichtungen privater deutscher Unternehmen gegenüber ausländischen Stellen sind darin nicht enthalten. Das IRG richtet sich ausschließlich an deutsche Behörden. Diese können im Rahmen eines an sie gerichteten Rechtshilfeersuchens der zuständigen US-Behörden darum gebeten werden, nach den innerstaatlichen Vorschriften deutsche Unternehmen zur Herausgabe von Daten zu verpflichten. Die deutschen Behörden entscheiden anhand des Einzelfalls, ob dem Ersuchen nachzukommen ist.

Die direkte Übermittlung von Daten an die US-Behörden durch deutsche Unternehmen bleibt davon allerdings unberührt. Nach dem Recht der USA können in den USA ansässige deutsche Unternehmen einseitig dazu gezwungen werden, in Deutschland befindliche Beweismittel beizubringen. Der Einsatz dieser sog. exterritorial wirkenden Maßnahmen der US-Behörden, durch die deutsche Unternehmen zur Herausgabe von Daten verpflichtet werden, unterliegt derzeit keinerlei Beschränkungen.

Abhilfe kann von dem am 14. Oktober 2003 zwischen den USA und der Bundesrepublik Deutschland unterzeichneten Vertrag über die Rechtshilfe in Strafsachen erwartet werden, der voraussichtlich im Laufe dieses Jahres in Kraft treten wird.

Artikel 1 Abs. 5 des Vertrags sieht vor, dass eine Vertragspartei den anderen Staat vorrangig um Rechtshilfe nach Maßgabe der Bestimmungen des Vertrags ersuchen muss, wenn sie Beweismittel aus dem Ausland benötigt. Die Vorschrift bezieht sich nach Auffassung der Vertragsparteien auf die oben erwähnten exterritorial wirkenden Maßnahmen. Nach Artikel 1 Abs. 5 sind derartige Maßnahmen grundsätzlich nicht mehr zulässig. Vielmehr ist zunächst der Rechtshilfeweg zu beschreiten.

Demnach steht künftig der Rechtshilfevertrag nach seinem Inkrafttreten einer in Ihrer ersten Frage angesprochenen unmittelbaren Verpflichtung deutscher Unternehmen gegenüber dem US-Justizministerium zur Herausgabe von Daten ausdrücklich entgegen.

10.3

Zu Frage 2:

Die Fragestellung berührt den Anwendungsbereich des im Verhältnis zu den USA geltenden Haager Übereinkommens über die Beweisaufnahme im Ausland in Zivil- und Handelssachen vom 18. März 1970 (HBÜ). Eine Verpflichtung zur Übermittlung personenbezogener Daten im Verfahren der pre-trial discovery begründet das HBÜ jedoch nicht.

Nach Artikel 23 HBÜ kann jeder Vertragsstaat erklären, dass er Rechtshilfeersuchen nicht erledigt, die ein Verfahren zum Gegenstand haben, das in den Common-Law-Ländern unter der Bezeichnung „pre-trial discovery of documents“ bekannt ist.

Bei der „pre-trial discovery“ handelt es sich um ein dem deutschen Prozessrecht unbekanntes Beweismittelverfahren zwischen Klageerhebung und Hauptverhandlung, mit dessen Hilfe die gegnerische Partei oder Dritte zur Vorlage von Beweismitteln gezwungen werden können. Das Gericht wird in diesem Verfahrensstadium nur im Rahmen der Anordnung von Schutz- oder Zwangsmaßnahmen eingeschaltet. Im Übrigen unterliegt das Verfahren weitgehend der Verantwortung der Parteien und ihrer Anwälte. Aufgrund dieser Besonderheit kann „ersuchende Behörde“ i. S. d. HBÜ auch eine US-amerikanische Prozesspartei oder ihr Anwalt sein. Dies lässt § 2 Abs. 2 Satz 2 der Rechtshilfeordnung für Zivilsachen (ZRHO) innerhalb der Bundesrepublik Deutschland ausdrücklich zu.

Die Bundesrepublik Deutschland hat jedoch die Erklärung nach Artikel 23 HBÜ abgegeben.

Nach § 14 Abs. 1 des Gesetzes zur Ausführung des Haager Übereinkommens vom 18. März 1970 über die Beweisaufnahme im Ausland in Zivil- und Handelssachen werden dementsprechend Rechtshilfeersuchen nicht erledigt, die ein „pre-trial discovery of documents“ zum Gegenstand haben.

Das Haager Beweisaufnahmeübereinkommen regelt nur die Beweisaufnahme im Ausland. Weiter gehende multilaterale Übereinkommen oder bilaterale Abkommen, die auch die Beweisaufnahme im (US-amerikanischen) Inland abdecken, bestehen nicht.

Mit freundlichen Grüßen
Lutz Diwell

Für die erste Fallkonstellation bedeutet dies, dass nach Inkrafttreten des Vertrags über die Rechtshilfe in Strafsachen eine direkte Übermittlung von personenbezogenen Daten an das US-Justizministerium unzulässig ist. Bei solchen Herausgabeverlangen muss das Unternehmen zunächst den offiziellen Rechtshilfeweg beschreiten, d. h. an die Landesjustizverwaltung herantreten. Sie hat das Herausgabeverlangen auch unter Datenschutzaspekten zu prüfen. Betroffenen Unternehmen ist zu empfehlen, auch in der Übergangszeit bis zum Inkrafttreten des Vertrages die für die Rechtshilfe in Strafsachen zuständigen Behörden einzuschalten.

Für die zweite Fallkonstellation bedeutet die Antwort des BMJ, dass deutsche Unternehmen ein umfassendes Herausgabeverlangen von US-Unternehmen zurückweisen müssen. Hierbei können sie auf die Antwort des BMJ verweisen. Der Düsseldorfer Kreis vertritt hierzu folgende Auffassung: Pre-Trial Discovery - Ersuchen US-amerikanischer Unternehmen sind von § 4 c Abs. 1 Satz 1 Nr. 4 BDSG (der eine Datenübermittlung nur gestattet, wenn sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen *vor Gericht* erforderlich ist) i. V. m. dem „Erledigungsverbot“ nach HBÜ grundsätzlich nicht gedeckt. Das zweistufige Verfahren nach Pseudonymisierung kann dagegen weiterhin befürwortet werden.

Zwar scheint damit die Verfahrensweise aus deutscher Sicht vorerst geklärt. Unbefriedigend ist die Situation aber zumindest dann, wenn sich europaweit tätige Unternehmen (ggf. ein und desselben Konzerns) möglicherweise unterschiedlich verhalten. Deshalb hat die AG „Internationaler Datenverkehr“ eine Befassung der Art. 29-Datenschutzgruppe befürwortet und ihr die Fragestellungen unterbreitet. Bei der von uns eingeleiteten ersten Umfrageaktion unter ihren Mitgliedern hat sich herausgestellt, dass die rechtliche Beurteilung beider Fallkonstellationen sehr unterschiedlich erfolgt. Teilweise war man sich der Problematiken überhaupt nicht bewusst. Allseits war man sich allerdings einig, dass eine unterschiedliche Handhabung der US-Herausgabeersuchen in Europa möglichst vermieden werden soll. Die Art. 29-Datenschutzgruppe hat deshalb eine Unterarbeitsgruppe eingesetzt, die zunächst die Rechtslage in der EU näher beleuchten und eine Stellungnahme zu beiden Fallkonstellationen erarbeiten soll. Ziel ist dabei, die Problematiken einheitlich zu lösen, was u. U. dazu führen kann, dass die Auffassung des Düsseldorfer Kreises zur zweiten Fallkonstellation dort erneut diskutiert werden muss.

10.3

11 Organisation und Technik

11.1 RFID – Reisepass mit Fingerabdruckdaten

Seit dem 1. November 2007 gibt es nun bereits Reisepässe einer neuen Generation, die einen RFID-Chip enthalten, der die auf dem Pass gedruckten Daten und das Gesichtsbild speichert und per Funk aussenden kann („ePass“). RFID bedeutet „Radio Frequency Identification“ und meint, dass der Chip sich und damit die Person, die ihn besitzt, per Funk identifizieren kann. Auf den seit dem 1. November 2007 ausgegebenen Pässen wurde der Speicherumfang noch erweitert. Nun werden zusätzlich zu den bisherigen Daten zwei Fingerabdruckbilder auf dem Chip gespeichert.

Ein Ziel der Maßnahme ist eine sichere Überprüfung, ob ein bestimmter Pass auch zu einer bestimmten Person gehört. Dafür werden biometrische Verfahren[182] eingesetzt, die die vor Ort beispielsweise bei einer Polizeikontrolle erfassten Daten wie Fingerabdrücke oder Gesichtsbilder mit dem im Pass gespeicherten Daten vergleichen.

Die Hauptsorge von Datenschutzbeauftragten ist, dass diese Maßnahme zu einem Dammbruch führt: So soll demnächst auch der Personalausweis, den alle besitzen müssen, mit dem Funkchip ausgestattet sein und ebenfalls Fingerabdrücke und Gesichtsbilder speichern. Es werden folglich alle Bürgerinnen und Bürger „erkennungsdienstlich behandelt“.

Für die Sicherheitsbehörden wäre es natürlich ideal, wenn die biometrischen Daten der *gesamten Bevölkerung* zusätzlich in *zentralen Datenbanken* gespeichert würden. Sie glauben, dass dann viele Straftaten und Ordnungswidrigkeiten einfach am Computer durch eine Datenbankabfrage aufgeklärt werden könnten. Dabei achten doch in jedem Kriminalfilm die Täterinnen oder Täter darauf, ihre Fingerabdrücke zu entfernen – zukünftig könnten sie zudem Fingerabdrücke von Unbeteiligten am Tatort hinterlassen, beispielsweise an einem „geliehenen“ Feuerzeug, welches sie dort „vergessen“.

Bisher lehnt der Bundesgesetzgeber eine solche zentrale Speicherung ab. Dies wirkt sich aber nur im Inland aus. Setzt man den Reisepass ein, um andere Länder zu besuchen, werden einige dieser Länder, wie z. B. die USA, die biometrischen Daten bei der Grenzkontrolle auslesen und für unbestimmte Zeit in Datenbanken speichern.

---

[182] vgl. 2.4

11.1

Nach dem Ende des Berichtszeitraums ist eine Verfassungsbeschwerde gegen den ePass erhoben worden.

Sicherheit des ePasses

Außer wegen der unkontrollierten Verbreitung sensibler biometrischer Daten sorgen sich nicht nur Datenschutzbeauftragte um die Sicherheit der eingesetzten Technik. So können Betroffene prinzipiell nicht feststellen, wenn jemand versucht, die Daten aus dem Chip per Funk auszulesen. Es ist aber zu befürchten, dass mit einem handlichen Lesegerät die Pass- bzw. Personalausweisdaten einfach im Vorbeigehen ausgelesen werden können.

Da ein solches Szenario natürlich inakzeptabel ist, wurden in den Chip des Reisepasses Schutzmechanismen integriert, die ein unberechtigtes Auslesen verhindern sollen. Die erste „Schutzmaßnahme“ ist die Verwendung eines *passiven* RFID-Chips mit geringer Reichweite. Passiv bedeutet, dass der Chip nicht von allein senden kann, sondern nur Lesegeräten antworten kann, die maximal 10-15 cm entfernt sind. In der Praxis sind je nach Aufwand auch größere Entfernungen möglich. Insbesondere ist ein Abhören einer erlaubten Funk-Kommunikation zwischen Lesegerät und Pass (z. B. bei der Grenzkontrolle) nach einer Untersuchung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) noch aus mehreren Metern Entfernung möglich.

Basic Access Control

Da sich ein unbefugtes Mithören der Kommunikation nicht vermeiden lässt, wurden mit dem „Basic Access Control“ (BAC) und dem „Extended Access Control“ (EAC) zwei aufeinander aufbauende Schutzmechanismen eingeführt, die auf Techniken zur Verschlüsselung und digitalen Signatur beruhen.

Das Gesichtsbild und die Basisdaten des Reisepasses werden nur durch den ersten Schutzmechanismus BAC geschützt. Dieser funktioniert folgendermaßen: Ein Lesegerät muss, um mit einem Pass kommunizieren zu können, einen Verschlüsselungsschlüssel kennen. Ohne diesen Schlüssel kann es zwar senden, aber der Pass versteht die Anfrage nicht und die Antwort könnte wiederum das Lesegerät nicht entschlüsseln. Der Schlüssel ist quasi auf dem Pass selbst aufgedruckt: Das Lesegerät berechnet aus den zuvor optisch eingescannten Daten Passnummer, Geburts-

datum der Inhaberin oder des Inhabers und Ablaufdatum des Passes den Schlüssel. Dadurch soll sichergestellt werden, dass jeder Auslesevorgang durch Aufklappen und Übergeben des Passes legitimiert wird. Allerdings wurde gezeigt, dass BAC unsicher ist, da der berechnete Schlüssel einfach nicht zufällig genug ist. Spezialisten haben demonstriert[183], dass eine abgehörte Kommunikation zwischen Pass und Lesegerät unter bestimmten Annahmen schon heute innerhalb weniger Stunden entschlüsselt werden kann.

Die Pass-Daten sind auf dem Chip digital signiert gespeichert, d. h., die Passausstellerin oder der Passaussteller (die Bundesdruckerei bzw. das BSI) unterschreibt quasi das Dokument und jedes Lesegerät kann überprüfen, ob die Unterschrift echt ist. Daher ist es nicht möglich, einem Lesegerät einen gefälschten Pass unerkannt vorzulegen. Das Kopieren der Daten des Passes ist hingegen überhaupt kein Problem[184]: Ein gefälschter Pass mit einem handelsüblichen RFID-Chip mit den Daten einer ähnlich aussehenden Person würde von den Lesegeräten zunächst akzeptiert werden.

Extended Access Control

Den Fingerabdruck und weitere biometrische Daten, die ggf. in späteren Pass-Generationen gespeichert werden, gibt der Chip jedoch nur heraus, wenn zusätzlich der Schutzmechanismus EAC vom Lesegerät aktiviert wird. Dazu weist das Lesegerät gegenüber dem Pass mithilfe eines digitalen Zertifikats (praktisch eines vom BSI unterschriebenen Dokuments) nach, dass es berechtigt ist, die Fingerabdrücke auszulesen. Dadurch kann das BSI für jedes Land der Welt festlegen, ob es Fingerabdrücke aus deutschen Pässen auslesen darf. Zusätzlich weist der Pass ebenfalls mit einem digitalen Zertifikat seine Echtheit nach. Die Übertragung der Passdaten erfolgt mit EAC auch wesentlich stärker verschlüsselt, sodass ein Entschlüsseln durch Dritte momentan ausgeschlossen scheint. Auch ein wie oben beschrieben kopierter Pass würde beim Einsatz von EAC erkannt, da ein Teil der Daten von einem korrekt funktionierenden Pass nie ausgegeben wird.

Durch den Einsatz des erweiterten Schutzmechanismus EAC sind die Fingerabdruckdaten wesentlich besser geschützt als die anderen Daten (Name, Adresse, Foto etc.). Auch die Fälschungssicherheit ist erhöht, vorausgesetzt das Lesegerät

[183] http://www.heise.de/newsticker/meldung/69127
[184] http://www.golem.de/0608/46966.html

verwendet EAC. Jedoch bietet auch EAC Angriffspunkte, sodass die Sicherheit langfristig nicht garantiert werden kann – insbesondere wenn sich jemand durch Hacking-Methoden oder physische Analyse Zugriff auf einen Ausweis-Chip verschafft.

Sehr problematisch ist auch, dass die Zertifikate von (ausländischen) Lesegeräten allgemein bekannt werden könnten und damit der Schutz von EAC aufgehoben wäre. Dagegen versucht man sich zu schützen, indem man Gültigkeit der Zertifikate auf nur einige Monate beschränkt. Dies ist allerdings nahezu wirkungslos, da der Reisepass oder Personalausweis das aktuelle Datum nicht kennt und daher nicht überprüfen kann, ob das Zertifikat noch gültig ist.

Da jeder Pass jedoch auch einfachere bzw. nicht zum Auslesen der Fingerabdrücke berechtigte Lesegeräte unterstützen soll, sind alle anderen Daten des Passes nur durch den einfachen Schutzmechanismus BAC, also nicht ausreichend, geschützt. Wir empfehlen daher, den Pass in einer speziellen Hülle aufzubewahren, beispielsweise aus Aluminiumfolie, die die unkontrollierte Kommunikation des Chips unterbindet.

Mit dem elektronischen Reisepass wurde eine sehr riskante Entwicklung in Gang gesetzt, die u. U. zu zentralen Datenbanken der biometrischen Daten aller Bürgerinnen und Bürger führen könnte. Der Zugriff auf diese Daten lässt sich, wie vielfache Erfahrung zeigt, dauerhaft nicht wirksam einschränken. Die Sicherheit des Funkchips vor unberechtigtem Auslesen ist langfristig nicht zu garantieren – aber schon der einzelne Pass gilt 10 Jahre.

11.2 Behördliche Datenschutzbeauftragte

11.2.1 Gesprächskreis der bezirklichen Datenschutzbeauftragten

Die bezirklichen Datenschutzbeauftragten haben sich im Berichtsjahr erneut zu vier Gesprächsrunden getroffen, um sich über Datenschutzfragen auszutauschen. Der Themenkreis war wie immer breit gefächert und deshalb werden einige Themen (u. a. Ermittlung von Meldedaten durch die Schulbehörde; IT-Verfahren AUGUSTA – Erstellung von Ausnahmegenehmigungen für die Umweltzone) an anderer Stelle in diesem Bericht besprochen[185].

[185] vgl. 1.2

11.2.2 Workshop der Datenschutzbeauftragten der Gerichte

Mit den Datenschutzbeauftragten des Kammergerichts, des Landgerichts und der Amtsgerichte findet in der Regel dreimal im Jahr ein Gedankenaustausch statt, bei dem Datenschutzprobleme bei der ordentlichen Gerichtsbarkeit erörtert werden.

In der ersten Sitzung des Jahres stellte ein Teilnehmer zur Diskussion, ob es zulässig sei, den Geschäftsverteilungsplan (GVPl) eines Amtsgerichts im Internet zu veröffentlichen.

Maßgeblich für die Beurteilung der Frage ist § 21 e Abs. 9 Gerichtsverfassungsgesetz (GVG). Danach ist der Geschäftsverteilungsplan des Gerichts „in der von dem Präsidium oder aufsichtsführenden Richter bestimmten Geschäftsstelle zur Einsichtnahme aufzulegen; einer Veröffentlichung bedarf es nicht“. Der letzte Halbsatz ist jedoch nicht so auszulegen, dass eine Veröffentlichung verboten ist. Hiergegen spricht die Funktion der Auslegung des Geschäftsverteilungsplans. Er soll den Rechtsuchenden ermöglichen, die Zusammensetzung des Spruchkörpers in Erfahrung zu bringen und ihre – auch verfassungsrechtlich verbürgte – Ordnungsmäßigkeit zu überprüfen.

Nach einhelliger Auffassung sollen alle von dem Inhalt des Geschäftsverteilungsplans Kenntnis nehmen können. Ein Zweck oder ein Interesse braucht dabei nicht angegeben werden. Es bleibt somit festzuhalten, dass die Veröffentlichung des Geschäftsverteilungsplans, auch im Internet, keinen datenschutzrechtlichen Bedenken begegnet, soweit sich die Angaben zu den Richterinnen und Richtern auf das Erforderliche beschränken.

Einen breiten Raum in den Sitzungen nahm das Thema Videoüberwachung bei der ordentlichen Gerichtsbarkeit ein. Wir haben eine Stellungnahme erarbeitet, in der die Grundsätze für eine rechtliche Bewertung von Videoüberwachungen in der ordentlichen Gerichtsbarkeit dargestellt werden. Diese Grundsätze sollen als Hilfestellung für eine Vorabkontrolle nach § 19 a Abs. 1 Satz 2 Nr. 1 Berliner Datenschutzgesetz (BlnDSG) dienen.

Nach § 31 b Abs. 1 BlnDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit der Einsatz der Videoüberwachung zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

11.2

Als zulässiger Beobachtungszweck kommt hier eine Videoüberwachung zur Aufgabenerfüllung in Betracht. Gemeint ist damit nicht, dass die gesetzlichen Aufgaben unmittelbar durch die Videoüberwachung erfüllt werden müssen, es ist vielmehr ausreichend, dass sie ihre Erfüllung im weitesten Sinne unterstützen. Unter die Regelung fällt damit eine Videoüberwachung, mit der die Funktionsfähigkeit öffentlich zugänglicher Räume in den Gerichtsgebäuden gewährleistet werden kann, die für die Aufgabenerfüllung verwendet werden. Daneben kommt auch die Wahrnehmung des Hausrechts in Betracht, etwa wenn die Videoüberwachung Personen davon abhalten soll, Rechtsverstöße im Gerichtsgebäude zu begehen.

Die durch die Videoüberwachung verfolgten Zwecke sollten von der verantwortlichen Stelle schriftlich festgehalten werden. Dies ist erforderlich, da nur anhand der Zweckbestimmung eruiert werden kann, ob eine Videoüberwachung in Frage kommt, ob aufgezeichnet werden darf und wie lange die Aufzeichnungen gespeichert werden dürfen.

Eine Videoüberwachung ist allerdings nur zulässig, soweit sie zu den in § 31 b Abs. 1 BlnDSG genannten Zwecken auch erforderlich ist. Erste Voraussetzung dafür ist, dass die Videoüberwachung geeignet ist, den angestrebten Überwachungszweck zu erreichen. Dies ist etwa zweifelhaft, wenn die Videoüberwachung präventiv dem Schutz der Bediensteten dienen soll, die Videoaufnahmen aber nicht durchgehend vom Wachpersonal beobachtet werden und diese im Falle eines Zwischenfalls auch nicht in der Lage wären, rechtzeitig für Hilfe zu sorgen. Erfolgt die Videoüberwachung ausschließlich aus präventiven Gründen (Schutz der Bediensteten), dürfte in der Regel eine Aufzeichnung nicht erforderlich sein.

Eine Videoüberwachung zum Schutz vor Störungen setzt als Erstes eine Gefährdungsanalyse voraus. Die Gefährdung bezieht sich grundsätzlich auf das Gerichtsgebäude, welches videoüberwacht werden soll. Einzelfälle wie der Überfall auf eine Zahlstelle in einem einzelnen Gerichtsbezirk können nicht dazu führen, bei allen Gerichten eine Notwendigkeit zur Videoüberwachung zu attestieren. Danach ist die Gefährdungsanalyse anhand der in dem jeweiligen Gerichtsgebäude in einer bestimmten Zeit erfolgten „Störfälle“ zu analysieren. Hierbei sollte bei einer Vorabkontrolle als Maßstab berücksichtigt werden, ob die konkret aufgetretenen Störfälle durch eine Videoüberwachung hätten vermieden werden können, denn dies könnte den durch die Videoüberwachung verursachten Grundrechtseingriff rechtfertigen.

Das Landgericht Berlin[186] hält eine Videoüberwachung nicht für erforderlich, wenn der verfolgte Zweck auch durch andere geeignete Maßnahmen zu erreichen ist. Dazu gehören häufigere Kontrollen des Hausmeisters bzw. des Sicherheitspersonals. Die Erforderlichkeitsüberlegungen sollten nicht nur bei dem „Ob" der Videoüberwachung angestellt werden, sondern auch bei der Frage, welche Gebäudeteile überwacht werden.

Auch eine erforderliche Videoüberwachung kann rechtswidrig sein, wenn Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Danach sind etwa permanente Videoüberwachungen in Beratungsstellen oder Rechtsantragsstellen von vornherein rechtswidrig (hier fehlt es allerdings auch an der Erforderlichkeit, da dem Sicherheitsbedürfnis der Mitarbeiterinnen und Mitarbeiter durch einen Alarmknopf eher gedient ist). Die Beratungs-, Rechtsantrags- und Zahlstellen sollten über ein Alarmsystem verfügen; es bestehen keine Bedenken dagegen, dass der Alarm eine Videoaufzeichnung auslöst. Notausgänge könnten bei ihrer Nutzung eine Videoaufzeichnung auslösen.

Eine Videoüberwachung am Eingang des Gerichtsgebäudes erscheint zwar grundsätzlich möglich, allerdings ist die Frage zu klären, welchen Zweck die Videoüberwachung haben soll. Da Gerichtsverhandlungen öffentlich sind, wird man nicht ohne Weiteres unter Zugrundelegung des Hausrechts Zugangsbeschränkungen erlassen können. Die Videoüberwachung kann also nur das Eindringen von Störern verhindern, die schon im Eingangsbereich als solche zu erkennen sind. Videoüberwachungen, die außerhalb der Öffnungszeiten im Gerichtsgebäude nächtliche Einbrüche verhindern oder aufklären sollen, fallen nicht in den Regelungsbereich des § 31 b BlnDSG und sind in der Regel zulässig.

11.2.3 Bestellung und Vertretung von Datenschutzbeauftragten

Die gesetzliche Verpflichtung zur Bestellung von behördlichen Datenschutzbeauftragten bleibt im Land Berlin ein Dauerthema. Weiterhin gibt es Stellen, die sich beharrlich weigern, der gesetzlichen Verpflichtung nachzukommen und diese Positionen zu besetzen.

Im Bereich der Jobcenter trifft dies insbesondere auf das Jobcenter Charlottenburg-Wilmersdorf zu. Dort wird die Meinung vertreten, für unser Anliegen nicht der richtige Ansprechpartner zu sein. Unsere Anfragen werden stets an die Bundesagentur für Arbeit weitergeleitet. Dabei haben jetzt – bis auf dieses Amt – alle

[186] NZM 2001, 707/708

anderen Jobcenter ihre Datenschutzbeauftragten benannt und ihre Vertretung geregelt.

Nach der jüngsten Entscheidung des Bundesverfassungsgerichts muss der Bundesgesetzgeber neue Rechtsgrundlagen für das Arbeitslosengeld II schaffen. Dabei werden wir uns für eine klarstellende Regelung dieser Frage einsetzen. Schon jetzt sind allerdings alle Jobcenter zur Bestellung eigener Datenschutzbeauftragter verpflichtet.

Weiterhin schwierig gestaltet sich die Bestellung eines Stellvertreters des behördlichen Datenschutzbeauftragten im Bezirk Charlottenburg-Wilmersdorf. Obwohl gesetzlich verpflichtet, weigern sich die Verantwortlichen des Bezirks beharrlich, dieser Forderung nachzukommen. Im Bezirk gibt es zwar seit geraumer Zeit einen hauptamtlichen Datenschutzbeauftragten, jedoch fehlt in Zeiten seiner Abwesenheit (u. a. Urlaub, Krankheit) ein Vertreter, der die anfallenden Datenschutzaufgaben wahrnehmen könnte.

Bereits über Jahre hinweg haben weder Mahnungen noch Beanstandungen etwas bewirkt und auch die Einschaltung des Parlaments im Berichtsjahr, in dem in einer Sitzung des Unterausschusses Datenschutz und Informationsfreiheit das Thema auf der Tagungsordnung stand, hat nicht den gewünschten Erfolg gebracht. Hier wird in prekärer Weise deutlich, dass Aufgaben, selbst wenn sie gesetzlich vorgegeben sind, einfach nicht ernst genommen oder gar ignoriert werden, wenn sie nicht ins politische oder aber auch finanzielle Kalkül passen. Der meist vorgeschobene Grund der mangelnden finanziellen Mittel für zusätzliches Personal ist nicht stichhaltig, denn für die Aufgabenbewältigung der Stellvertreteraufgaben reicht auch ein limitiertes Zeitbudget aus, so wie es in den anderen Bezirken ebenfalls praktiziert wird.

11.3 Diskretion in Jobcentern

Auch in diesem Jahr erreichten uns Beschwerden, die auf die fehlende Diskretion in den Abfertigungsbereichen der Jobcenter hinwiesen. Seit Gründung der Jobcenter im Jahre 2005 findet dieses Thema immer wieder Erwähnung in unseren Jahresberichten[187].

[187] JB 2006, 9.3; JB 2005, 3.1

Bei den Jobcentern finden die Gespräche zwischen Bediensteten und Hilfesuchenden an Arbeitsplätzen in Großraumbüros statt. In diesen Büros sind die einzelnen Arbeitsplätze kompakt aneinander gereiht. Diskretion fördernde Elemente wie beispielsweise schalldämmende Wände sind – soweit vorhanden – meist unzureichend.

Insgesamt wurden Kontrollen der Diskretion in drei Jobcentern durchgeführt. Lediglich in einem konnte eine ausreichende Gewährleistung der Vertraulichkeit festgestellt werden. Ansonsten wurde eine beiläufige Kenntnisnahme vertraulicher Daten durch andere Anwesende billigend hingenommen.

Im Vergleich mit der Bearbeitungspraxis im Sozialamt ist diese Entwicklung ein deutlicher Rückschritt. Im Sozialamt wurden Gespräche grundsätzlich in geschlossenen Büros geführt. Die Änderung dieser Praxis in den Jobcentern wurde mit dem Hinweis auf die Transparenz der Bearbeitungsdauer für die Wartenden und mit dem Hinweis auf die höheren Kosten begründet.

Die Jobcenter sind nach den sozialdatenschutzrechtlichen Vorschriften verpflichtet, technische und organisatorische Maßnahmen zu treffen, um die Vertraulichkeit der Gespräche zu gewährleisten. Es ist zu verhindern, dass Sozialdaten Unbefugten zur Kenntnis gelangen können. Bei Beratung von mehreren Hilfesuchenden in einem Raum bedeutet dies, dass das Jobcenter verpflichtet ist, Einzelberatungen in einem separaten Raum anzubieten. Die Betroffenen sind durch gut sichtbare Aushänge auf diese Möglichkeit hinzuweisen. Zusätzlich sollten auch in den Großraumbüros Maßnahmen getroffen werden, die die beiläufige Kenntnisnahme verhindern. Nicht alle Hilfesuchenden sind in der Lage, ihr Bedürfnis nach Vertraulichkeit gegenüber der Sachbearbeiterin oder dem Sachbearbeiter zu offenbaren. Auch diese Personen haben ein Anrecht auf Wahrung des Datenschutzes.

11.4 Einzelfragen der Videoüberwachung

11.4.1 Private Videoüberwachung des eigenen Grundstücks, der Nachbargrundstücke und des öffentlichen Straßenlandes

Im vergangenen Jahr haben wir vermehrt Eingaben von Bürgerinnen und Bürgern erhalten, die sich über private Videoüberwachung durch ihre Nachbarn beschwerten. Diese Überwachung beschränkte sich häufig nicht nur auf das jeweilige Privatgrundstück der für die Kamera verantwortlichen Person, sondern erstreckte sich darüber hinaus oftmals auf

angrenzende Nachbargrundstücke, Bürgersteige und öffentliches Straßenland.

Als Grund für solche Überwachungsmaßnahmen wird in den meisten Fällen vordergründig der Schutz des Eigentums vor Beschädigung und Diebstahl angegeben. Innerhalb seiner Grundstücksgrenzen darf jeder Mensch sein Eigentum auch mit Videotechnik überwachen. Das gilt zumindest dann, wenn das Grundstück nicht von Dritten als Durchgang genutzt wird oder mehrere Personen ein Nutzungsrecht an dem Grundstück haben.

Werden mit privaten Kameras allerdings öffentliche Straßen, Bürgersteige oder gar angrenzende Grundstücke beobachtet, ist dies grundsätzlich unzulässig.

§ 6 b Abs. 1 Bundesdatenschutzgesetz (BDSG) lässt die Videoüberwachung öffentlich zugänglicher Räume wie Straßen, Wege usw. nur sehr eingeschränkt zu. Für private Stellen ist eine solche Überwachung öffentlich zugänglicher Räume regelmäßig nur gestattet, wenn dies „zur Wahrung des Hausrechts“ oder „zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke“ erforderlich ist und keine schutzwürdigen Interessen der Betroffenen verletzt werden. Beispielsweise kann ein Kaufhaus innerhalb seiner Geschäftsräume oder einer Einkaufspassage Videoüberwachung betreiben, um Diebstähle oder Vandalismus abzuwenden. Nach einer Entscheidung des Amtsgerichts Berlin-Mitte aus dem Jahr 2003 dürfen aber selbst Kaufhäuser zum Schutz ihrer Außenfassaden nicht den gesamten angrenzenden Bürgersteig beobachten. Erfasst werden darf nur ein Bereich von höchstens einem Meter vor der Hauswand. Außerdem müssen dann besondere formelle Voraussetzungen beachtet werden wie das Aufstellen von Hinweisschildern.

Die Beobachtung von öffentlichen Straßen durch Privatpersonen ist nahezu stets unzulässig: Die Grundstückbesitzerinnen und -besitzer können sich bei der Videoüberwachung solcher Flächen nicht auf die Wahrnehmung ihres Hausrechts beziehen, weil ihr Hausrecht an der Grenze ihres Grundstücks endet. Ebenso wenig dürfen sie zur Wahrung ihrer berechtigten Interessen weite Teile des öffentlich zugänglichen Raums überwachen. Hierzu sind die öffentlichen Gefahrenabwehr- und Strafverfolgungsbehörden (Polizei, Staatsanwaltschaft) berufen.

Die Rechtsprechung wendet bei der Beurteilung von Videoüberwachung in Nachbarschaftsverhältnissen überwiegend nicht das Datenschutzrecht, sondern allgemeines Zivilrecht an. Das heißt: Falls eine Privatperson eine Videokamera betreibt, die das Nachbargrundstück oder einen Zugang zu diesem Grundstück erfasst, wird die betroffene Nachbarin oder der betroffene Nachbar in ihrem bzw.

seinem allgemeinen Persönlichkeitsrecht beeinträchtigt. In Betracht zu ziehen ist dann ein Abwehranspruch aus §§ 823, 1004 Bürgerliches Gesetzbuch. Nach der Rechtsprechung einiger Gerichte soll dies sogar für Kameraattrappen gelten. Denn maßgeblich ist es, dass die Kamera (oder Attrappe) auf die Betroffenen einen unangemessenen Überwachungsdruck ausübt.

Eine Videoüberwachung kann im Extremfall sogar strafbar sein. Das ist gemäß § 201 a Strafgesetzbuch dann gegeben, wenn jemand von „einer anderen Person, die sich in einer Wohnung oder einem anderen gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch den höchstpersönlichen Lebensbereich verletzt".

Die Videoüberwachung des eigenen Grundstücks durch Privatpersonen ist grundsätzlich zulässig. Die darüber hinausgehende Beobachtung der Nachbargrundstücke oder des öffentlichen Raums ist nur eingeschränkt zulässig und kann bei Verstößen zivil- oder strafrechtlich verfolgt werden.

11.4.2 Forschungsprojekt „Foto-Fahndung" am Mainzer Hauptbahnhof

Im Zeitraum Oktober 2006 bis Januar 2007 führte das Bundeskriminalamt (BKA) Wiesbaden das Forschungsprojekt „Foto-Fahndung" am Mainzer Hauptbahnhof durch. Dieses Projekt sollte mithilfe von Videokameras in Verbindung mit modernen Gesichtserkennungssystemen zeigen, dass bestimmte Personen zuverlässig automatisch erkannt werden können.

Für dieses Projekt stellte die Deutsche Bahn AG (DB AG) einen Teilbereich der Eingangshalle des Hauptbahnhofs Mainz zur Verfügung und gab ihr Einverständnis für die Durchführung des Projekts. Nach Aussage des BKA bot der Hauptbahnhof ideale Voraussetzungen für ein geeignetes Testszenario.

Obwohl die alleinige Verantwortung für das Forschungsprojekt beim BKA und damit die Kontrollzuständigkeit beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) lag, hat auch der Berliner Beauftragte für Datenschutz und Informationsfreiheit, als für die DB AG zuständige Aufsichtsbehörde, den Projektverlauf verfolgt.

Vor Projektbeginn wurden ca. 200 freiwillige Testbeteiligte angeworben und um Abgabe einer Einwilligungserklärung für die Testteilnahme gebeten. Das BKA speicherte von ihnen Gesichtsbilder in biometrischen Systemen. Drei unterschiedliche Gesichtserkennungssysteme verschiedener Anbieter wurden während

der Projektphase getestet. Die Beteiligten erhielten für den Testzeitraum einen Transponder, den sie bei Durchqueren der Eingangshalle des Hauptbahnhofs bei sich tragen mussten. Sie sollten während der Testphase von 12 Wochen regelmäßig (möglichst einmal pro Werktag) den Überwachungsbereich passieren. Dabei wurden die Seriennummern der Transponder mit aktueller Uhrzeit zu Kontrollzwecken protokolliert.

Ziel des Forschungsprojekts war, die gespeicherten Fotos der Beteiligten mit den Gesichtern automatisch in der Menschenmenge am Bahnhof zu vergleichen und wiederzuerkennen. Hierzu wurden vom BKA zusätzliche Kameras auf einen Teil der Treppen in der Eingangshalle ausgerichtet. Diese nahmen alle vorbeigehenden Personen beim Durchqueren der Eingangshalle auf. Personen, die nicht aufgenommen werden wollten, hatten – soweit sie die entsprechenden Schilder mit Hinweis auf das Forschungsprojekt bemerkten – die Möglichkeit, entsprechend auszuweichen und einen anderen Bereich der Treppe zu benutzen.

Der BfDI hat bei der Durchführung des Forschungsprojekts keine datenschutzrechtlichen Mängel festgestellt[188].

Nach Auswertung der Testergebnisse kam das BKA im Februar 2007 zu dem Schluss, dass das polizeiliche Ziel, Terrorverdächtige, Hooligans oder Vermisste mithilfe der eingesetzten computergestützten Kamerasysteme aus einer Menschenmenge „herauszufischen“, mit der derzeit zur Verfügung stehenden Technik nicht zu realisieren ist.

Nach Aussage des Präsidenten des BKA ist der Einsatz solcher Systeme nur sinnvoll, wenn die Trefferquote bei nahezu 100 % liege. Die Treffergenauigkeit des Systems war stark abhängig von den Lichtverhältnissen. So erreichten die Kameras ihre beste Leistung lediglich vom späten Vormittag bis zum frühen Nachmittag, während die Trefferquote vor 8 und nach 17 Uhr nur noch etwa 20 % betrug. Es wurden sowohl bei Dunkelheit als auch bei starker Sonneneinstrahlung oder Gegenlicht besonders große Abweichungen festgestellt.

Doch nicht nur ungünstige Lichtverhältnisse erschwerten die Identifizierung von Gesichtern, auch Schal, Kapuze oder Sonnenbrille ließen die Trefferquote erheblich sinken. Die eingesetzten Systeme erreichten daher nur eine durchschnittliche Trefferquote von rund 30 %, bei besten Lichtverhältnissen nicht mehr als 60 %. Das BKA war von – im Schnitt täglich – 23 Falscherkennungen ausge-

[188] BfDI, 21. Tätigkeitsbericht 2005-2006, 5.2.6

gangen. Diese Quote ist jedoch unter datenschutzrechtlichen Aspekten nicht akzeptabel.

Da die eingesetzten Systeme auf einer 2-D-Gesichtserkennung basierten, wäre eine erfolgreiche Erkennung allenfalls mit Frontalaufnahmen des Gesichts zu erreichen gewesen. Größere Hoffnungen für einen effektiven Einsatz verspricht man sich daher künftig von der 3-D-Gesichtserkennung. Experten sind der Meinung, dass die Fehlerquote solcher Systeme bei maximal 10 % liegen könnte. Selbst dann würde die Technik aber nicht die vom Präsidenten des BKA geforderte Treffergenauigkeit von nahezu 100 % bieten.

Videoüberwachung in Verbindung mit biometrischen Gesichtserkennungssystemen ist nach derzeitigem Stand der Technik noch keine zuverlässige Methode, um eine nahezu 100-prozentige Identifizierung von Personen zu gewährleisten.

11.5 Sicherheit beim mobilen IT-Einsatz – Mobil unterwegs: – aber sicher!

Nachdem wir uns im Vorjahr[189] speziell mit der Sicherheit von Notebooks befassten, soll in diesem Jahr die Sicht auf die weiteren mobilen Geräte wie z. B. Personal Digital Assistants (PDAs) oder Handys ausgedehnt werden.

Die modernen Handys haben sich zu leistungsfähigen Mini-Computern (Smartphones) mit einem eigenen Betriebssystem, einer Vielzahl von Funktionen und Schnittstellen mit immer größeren Speicherkapazitäten entwickelt und sind somit den ähnlichen Gefahren wie Notebooks ausgesetzt. Die Mobilität wird immer mehr gefordert und genutzt, womit jedoch auch potenzielle Angreifer immer mehr angelockt werden. Da Schutzmechanismen meist nicht einfach umzusetzen und die Sicherheitsmechanismen bei diesen Miniaturcomputern meist noch nicht entsprechend installiert sind, muss hier nachgebessert werden.

Wir wollen hier einige Ansätze aufzeigen. Kriminelle nutzen auch die Kommunikationsnetze für ihr schädliches Tun und setzen dabei neueste Technologien ein. Schwachstellen, wie z. B. nicht ausreichend geschützte mobile Arbeitsplätze, sind bevorzugte Ziele für Angriffe, z. B. durch „SMiShing“. Dabei erfolgt das Phishing per E-Mail auf Textnachrichten zum Handy, wobei Nutzer dazu verleitet werden sollen, Schadsoftware zu installieren.

[189] JB 2006, 9.5

11.5

Natürlich muss grundsätzlich festgehalten werden, dass schon der umsichtige Umgang mit den Geräten – nicht jede Nachricht muss gelesen werden – vor vielen Gefahren schützen kann. Die Sicherheit fängt aber schon mit der Authentifizierung (Anmeldung) am mobilen Gerät an. Dabei wird ein deutlicher Trend zur Chipkarte gesehen, was bei entsprechender Ausgestaltung ein Plus an Sicherheit bietet, da hier eine Kombination aus Besitz und Wissen (Smartcard in Verbindung mit einer PIN) zum Tragen kommt.

Außerdem sollten öffentliche Stellen und Unternehmen beim Einsatz von mobilen Endgeräten Maßnahmen treffen, die sich bereits in der stationären Datenverarbeitung bewährt haben. Dazu gehören:

- die Erstellung von Sicherheitsregelungen (auch: Sicherheitskonzepten):
  - Vorgaben für die Nutzung von mobilen Endgeräten sowie der darauf gespeicherten Daten,
  - Aufstellung von Regelungen zu Sicherheitsmaßnahmen, z. B. für die Länge des Anmeldepassworts bzw. die Art der Authentisierung;

- der Einsatz von kryptografischen Sicherheitsmaßnahmen wie z. B. die Speicherverschlüsselung;

- die zentrale Verwaltung und Wartung der mobilen Endgeräte:
  - Installation und Einrichtung von Programmen (z. B. Software, die vor schadhafter Software wie Viren, Spyware usw. schützt),
  - regelmäßige Aktualisierung der Security-Patches,
  - Vornahme von Sicherheitseinstellungen;

- klare Vorgaben für die Nutzenden:
  - Regelungen zum Nutzerverhalten, denn der Mensch ist meistens der größte Risikofaktor. Hier sind sich fortwährend wiederholende Sensibilisierungsmaßnahmen, die sich am Stand der Technik orientieren sollten, notwendig.

Zusammenfassend ist der Einsatz von entsprechenden Schutzmaßnahmen zu empfehlen, damit keine sensiblen Daten in die Hände Unberechtigter fallen. Dies kann und muss über den Einsatz von z. B. Firewall und Virenschutz bis zur Kryptografie geregelt werden. Die Art und Weise der Verschlüsselung kann nur nach Abwägung der Risiken für die gespeicherten Daten gewählt werden.

11.6 Umgang mit Passwörtern

Vor ca. 1½ Jahren wurde der Landesbetrieb Krematorium Berlin gegründet. Im Anschluss erfolgte unter anderem eine Bestandsaufnahme der vorhandenen Informationstechnik sowie der installierten Anwendungen bzw. Verfahren, vorgefundene Mängel wurden abgestellt.

> *In einer Eingabe wurde uns dann aber mitgeteilt, dass die Beschäftigten des Landesbetriebs Krematorium Berlin die persönlichen Passwörter per Fax oder Telefon an eine mit dem Betrieb der Informationstechnik beauftragte Firma offenbaren sollten. Hierbei handelte es sich insbesondere um die Passwörter für die E-Mail-Postfächer.*

Grundsätzlich ist jedoch die Preisgabe persönlicher Passwörter an andere ausnahmslos unzulässig. Alle Beschäftigten müssen sicher sein, dass ihnen jeweils nur ihr persönliches Passwort bekannt ist. Dies bedeutet unter anderem, dass von der Systemverwaltung oder von anderen Funktionsträgern vergebene Erstpasswörter nach ihrer ersten Nutzung sofort geändert werden müssen. Die technischen und organisatorischen Maßnahmen nach dem Berliner Datenschutzgesetz verlangen, dass die Aktivitäten der sicher authentifizierten Person – sie hat sich mit ihrer Kennung in Verbindung mit ihrem Passwort am Computersystem angemeldet – zugerechnet werden können. Wenn eine beauftragte Firma fremde Passwörter benutzt, um beispielsweise administrative Aufgaben am System unter einer bestimmten Nutzerkennung durchzuführen, müssen die Beschäftigten damit rechnen, dass festgestellte Unregelmäßigkeiten später ihnen zugerechnet werden.

Gelegentlich kann es erforderlich sein, Passwörter verschlossen zu hinterlegen. Dies ist stets bei der Systemverwaltung der Fall, bei normalen Benutzerinnen oder Benutzern ist dies in der Regel deshalb nicht nötig, weil die Systemverwaltung mit ihren Rechten ersatzweise tätig werden kann. Wenn ihr dies aufgrund besonderer technischer und organisatorischer Maßnahmen nicht möglich ist, dann ist auch die Hinterlegung von Passwörtern der anderen Benutzerinnen oder Benutzer anzuraten.

Die Hinterlegung von Passwörtern setzt jedoch organisatorische Regelungen voraus, die sicherstellen, dass die Betroffenen von der Fremdverwendung ihrer Passwörter und deren Gründen sofort erfahren und Gelegenheit haben, den Vorfall zu überprüfen und das Passwort sofort zu ändern (und evtl. erneut verschlossen zu hinterlegen). So muss nicht nur ein sicherer Aufbewahrungsort zur Verfügung stehen (z. B. Tresor), sondern die Umschläge sollten z. B. einen besonderen Aufdruck enthalten, damit sie nach dem Öffnen nicht einfach von beliebigen Personen ersetzt werden können.

Zuerst ist jedoch immer zu prüfen, ob die Offenlegung des Passwortes, z. B. durch Ausführung der Tätigkeiten vor Ort bei Anwesenheit der Betroffenen, vermieden werden kann.

Grundsätzlich gilt, dass die Preisgabe persönlicher Passwörter an andere ausnahmslos unzulässig ist. Jede Person muss sicher sein, dass ihr persönliches Passwort nur ihr bekannt ist.

12 Telekommunikation und Medien

12.1 Telekommunikationsdienste

12.1.1 Vorratsdatenspeicherung in der Telekommunikation – Ein schwarzer Tag für den Datenschutz

Die Bundesregierung hatte im zurückliegenden Berichtszeitraum einen Gesetzentwurf zur Umsetzung der Richtlinie der Europäischen Union zur Vorratsdatenspeicherung[190] vorgelegt[191]. Er passierte am 21. Dezember 2007 den Bundesrat und ist im Wesentlichen am 1. Januar 2008 in Kraft getreten[192]. Neben den in das Telekommunikationsgesetz (TKG) eingefügten Regelungen zur Vorratsdatenspeicherung enthält das Gesetz auch Änderungen der Strafprozessordnung hinsichtlich der Verwendung dieser Daten sowie zu anderen verdeckten Ermittlungsmaßnahmen[193].

Die Speicherungspflichten für Daten sind in § 113 a TKG festgelegt. Sie gelten für Anbieter, die öffentlich zugängliche Telekommunikationsdienste erbringen[194]. Neu ist insbesondere die Speicherung der den Kundinnen und Kunden beim Internetzugang jeweils zugewiesenen dynamischen IP-Adresse sowie die Verpflichtung für Anbieter von Diensten der elektronischen Post zur Speicherung von Verkehrsdaten in Bezug auf versandte und eingehende Nachrichten, die allerdings erst ab dem 1. Januar 2009 vorgeschrieben wird. Anbieter von E-Mail-Diensten müssen außerdem aufgrund des neu gefassten § 111 Abs. 1 TKG Kennungen der elektronischen Postfächer sowie Namen und Anschrift der Inhaberin oder des Inhabers des elektronischen Postfachs für die Auskunftsverfahren nach den §§ 112 und 113 TKG zur Verfügung stellen, sofern sie diese Daten erheben. Im Gegensatz zu dem Referentenentwurf, der eine pauschale Speicherungsverpflichtung auch für diese Daten enthielt, begründet die jetzt verabschiedete Fassung der Vorschrift eine Speicherungspflicht nur, soweit die Daten erhoben werden. Ob die Daten erhoben

---

190 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates v. 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG; ABl. EU L 105/54, vgl. JB 2006, 10.1.2

191 Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG; BT-Drs. 16/5846

192 BGBl. I 2007, 3198

193 vgl. dazu 5.1

194 Das bedeutet, dass für unternehmensinterne Netze, Nebenstellenanlagen oder E-Mail-Server von Universitäten ausschließlich für dort immatrikulierte Studierende oder Bedienstete sowie die Telematikinfrastruktur im Gesundheitswesen eine Speicherungspflicht nicht besteht; vgl. BT-Drs. 16/5846, S. 69.

werden, bleibt dem Anbieter freigestellt. Auch diese Regelung ist auf Anbieter öffentlich zugänglicher Dienste der elektronischen Post beschränkt[195].

Umfangreiche Bestands- und Verkehrsdaten müssen auch beim Angebot von Festnetz- und Mobilfunkanschlüssen gespeichert werden[196]. Beim Mobilfunk gehören dazu auch die Standortdaten, sodass Bewegungsprofile erstellt werden können. Die Speicherfrist beträgt für alle o. g. Dienste sechs Monate. Die bisherigen Wahlmöglichkeiten zur Verkürzung oder Löschung von Zielnummern sind weggefallen.

Die bisher bestehenden Möglichkeiten zur anonymen Nutzung von Telekommunikationsdiensten, insbesondere aber von Internet-Zugang und E-Mail-Diensten gehören damit ab 2009 überwiegend der Vergangenheit an, wenn das Bundesverfassungsgericht das Gesetz nicht für nichtig erklärt. Insbesondere die Verpflichtung der Access-Provider zur dauerhaften Speicherung der zugewiesenen IP-Adressen ist in diesem Zusammenhang von besonderer Bedeutung, da damit sozusagen ein „Schlüssel" für sämtliche bei Content-Providern – sei es rechtmäßig oder rechtswidrig – gespeicherten Protokolldateien über Abrufe aus deren Angeboten existiert.

Besonders bemerkenswert an diesem Gesetzgebungsverfahren ist, dass die Notwendigkeit für die dort getroffenen Maßnahmen auf kein öffentlich zugängliches empirisches Material gestützt werden kann. Selbst eine Untersuchung des der Sympathie für Anonymität in der Telekommunikation sicherlich unverdächtigen Bundeskriminalamts vom November 2005 konstatiert, dass im Rahmen einer bundesweiten Befragung der Polizeidienststellen nach Ermittlungsverfahren, bei denen Verkehrsdaten fehlten, von dort lediglich 381 Einzelfälle zurückgemeldet wurden[197]. Selbst wenn man die methodischen Schwächen dieser Erhebung beiseitelässt und die Anzahl der Verdachtsfälle zugunsten der Strafverfolgungsbehörden für das gesamte Jahr einfach verdoppelt, entspricht dies, bezogen auf die Gesamtzahl aller statistisch erfassten Straftaten im Jahr 2005[198], einem Prozentsatz von

---

[195] vgl. § 111 Abs. 1 Satz 3 TKG

[196] vgl. § 113 a Abs. 1, 2 TKG

[197] Vgl. Mahnken, Eva: Mindestspeicherungsfristen für Telekommunikationsverbindungsdaten. Rechtstatsachen zum Beleg der defizitären Rechtslage, Stand: 15. November 2005. Die eingemeldeten Fälle betrafen Ermittlungsverfahren, in denen nach Meinung der Strafverfolgungsbehörden die Kenntnis von Verbindungsdaten zu einem erfolgreichen Abschluss des Ermittlungsverfahrens hätte führen können. Die Autorin räumt selbst ein, „... dass gerade die Frage, ob ein nicht vorhandenes Datum nützlich gewesen wäre, schwierig zu beantworten ist, da es ja gerade nicht zur Analyse vorliegt und man sich deshalb im Bereich des Hypothetischen bewegt."; vgl. a. a. O. unter 6. Methodik.

[198] lt. BKA-Kriminalitätsstatistik 2005 bundesweit insgesamt 6.391.715 Einzelfälle

etwas mehr als 0,01 %. Empirisch lässt sich somit die Einführung zusätzlicher umfangreicher Speicherungsverpflichtungen kaum rechtfertigen.

Zugleich beschädigt die Verpflichtung zur Vorratsdatenspeicherung auch die Arbeit von Beratungsstellen, die auf die Möglichkeit zur anonymen Kontaktaufnahme angewiesen sind, wie z. B. die Telefonseelsorge oder die Aids-Beratung. Auch sind Strafverteidiger, Geistliche und Abgeordnete, deren Telefonate nicht abgehört werden dürfen[199], ebenso wenig wie ihre Gesprächspartner davor geschützt, dass ihre Verkehrsdaten für sechs Monate gespeichert werden. Hier zeigt sich, dass das ausdrückliche Verbot, den Inhalt der Kommunikation zu speichern[200], bereits durch die Speicherung aller Verkehrsdaten auf Vorrat unterlaufen wird. Denn schon die Tatsache, dass Betroffene mit einem Geheimnisträger kommuniziert haben, unterlag bisher der Geheimhaltung. Auch der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist gesetzlich zur Verschwiegenheit darüber verpflichtet, wer sich mit einer Eingabe an ihn gewandt hat[201]. Diese Verpflichtung kann er insoweit nicht erfüllen, als Verkehrsdaten über alle mit seiner Dienststelle geführten Telefonate für ein halbes Jahr beim Netzbetreiber gespeichert werden müssen.

Zwar ist gegen die dem Gesetz zugrunde liegende Richtlinie ein Verfahren vor dem Europäischen Gerichtshof anhängig, das – unter Berücksichtigung der bisherigen Rechtsprechung des EuGH in vergleichbaren Fällen – vermutlich dazu führen wird, dass die Richtlinie für europarechtswidrig erklärt werden wird. Allerdings würde dies keine Auswirkungen auf die Geltung der jetzt beschlossenen Regelungen haben[202].

Wie nicht anders zu erwarten, hat der Bundesrat auch in diesem Gesetzgebungsverfahren weitere Verschärfungen gefordert: So wurde beispielsweise eine Verdoppelung der Speicherfrist von 6 Monaten auf ein Jahr gefordert. Ganz nebenbei sollte auch eine Rechtsgrundlage für die berüchtigte „Online-Durchsuchung“[203] geschaffen sowie eine nochmalige Ausweitung des Straftatenkatalogs erreicht

---

[199] vgl. 5.1

[200] § 113 a Abs. 8 TKG n. F.

[201] § 23 S. 1 Berliner Datenschutzgesetz (BlnDSG)

[202] Ein entsprechender Änderungsantrag der Fraktion Bündnis 90/Die Grünen, der dazu geführt hätte, dass in diesem Fall die §§ 113 a und b TKG wieder abgeschafft und die Regelung des § 100 g StPO in den vorherigen Stand zurückversetzt worden wäre – vgl. BT-Drs. 16/7016 – wurde im Bundestag abgelehnt.

[203] vgl. dazu 2.1

werden[204]. Lobend ist zu erwähnen, dass der Berliner Senat im Bundesratsverfahren insbesondere gegen diese Vorschläge gestimmt hat.

Ausschüsse des Bundesrates wollten die Nutzung der im Rahmen der Vorratsdatenspeicherung anfallenden Daten sogar zur zivilrechtlichen Durchsetzung der Rechte an geistigem Eigentum gestatten und bewegen sich damit weit jenseits des durch die EG-Richtlinie zur Vorratsdatenspeicherung abgesteckten Rahmens, die Nutzung auf die Verfolgung schwerer Straftaten zu beschränken. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung vom 8. Juni 2007 die weiteren durch den Bundesrat geforderten Verschärfungen entschieden abgelehnt[205]. Auch wir haben uns gegenüber den zuständigen Senatsverwaltungen in einer Stellungnahme gegen diese weiteren Verschärfungen ausgesprochen.

Besonders bedauerlich ist, dass die Debatte über Sinn und Unsinn der Einführung der Regelung zur Vorratsdatenspeicherung im politischen Raum den Boden des rationalen Diskurses bereits seit geraumer Zeit verlassen hatte. Die Debatte war überwiegend getragen vom Willen der Bundesregierung, die Regelung zügig einzuführen. Form und Inhalt der vorgetragenen Argumente gingen dabei teilweise bis hart an die Grenze selbst des politisch Redlichen: So ist das immer wieder gern verbreitete Argument, die Bundesregierung setze lediglich EU-Vorgaben in minimaler Weise um[206], durch einen Blick in den Gesetzentwurf leicht zu widerlegen. Dies betrifft insbesondere die umfänglichen Nutzungsbefugnisse für Strafverfolgungsbehörden in der Strafprozessordnung, die weit über den von der Richtlinie bestimmten Umfang hinausgehen. Geradezu humoristisch mutet das Argument an, von einer Erweiterung der Überwachungsmöglichkeiten könne schon deswegen nicht die Rede sein, weil die Daten nicht bei den Strafverfolgungsbehörden, sondern bei den Telekommunikationsanbietern gespeichert seien[207], denn staatlichen Stellen wird gleichzeitig der Zugriff auf die dort gespeicherten Daten umfassend ermöglicht. So sollen nach dem Willen des Gesetzgebers einige der Daten, die im Rahmen der Vorratsdatenspeicherung – und damit ausweislich der zugrunde liegenden Richtlinie 2006/24/EG nur „... zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten..."[208] – erhoben und gespeichert wurden,

---

[204] vgl. die Stellungnahme des Bundesrats; BR-Drs. 275/07

[205] „Telekommunikationsüberwachung und heimliche Ermittlungsmaßnahmen dürfen Grundrechte nicht aushebeln", vgl. Dokumentenband 2007, S. 16

[206] vgl. z. B. Stenografischer Bericht der 124. Sitzung des Deutschen Bundestags am Freitag, den 9. November 2007, Plenarprotokoll 16/124, S. 12994

[207] vgl. a. a. O., S. 12995

[208] Artikel 1 Abs. 1 Richtlinie 2006/24/EG

auch im Rahmen der Auskunftserteilung nach § 113 TKG unter sehr viel weiter gefassten Voraussetzungen übermittelt werden. Dazu zählen die Verfolgung von Straftaten oder Ordnungswidrigkeiten, die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes erforderlich ist[209]. Von einer grundrechtsschonenden Umsetzung der Richtlinie in nationales Recht kann hier wohl kaum noch die Rede sein.

Unmittelbar nach Inkrafttreten des Gesetzes am 1. Januar 2008 wurden zahlreiche Verfassungsbeschwerden beim Bundesverfassungsgericht erhoben. Die Datenschutzbeauftragten haben wiederholt darauf hingewiesen, dass die Einführung der Vorratsdatenspeicherung deutschem Verfassungsrecht widersprechen würde[210]. Der Ausgang des Verfahrens bleibt abzuwarten.

Internet-Nutzende sollten verstärkt die Nutzung – vertrauenswürdiger – Anonymisierungsdienste erwägen. Sie sollten E-Mail-Accounts nur unter Pseudonym und nur bei Anbietern registrieren, die auf die Erhebung von Namens- oder Adressdaten verzichten. Alternativ kann auch ein E-Mail-Anbieter außerhalb der Europäischen Union gewählt werden, bei dem vergleichbare Speicherungspflichten nicht bestehen.

12.1.2 Drohende Aushöhlung des Fernmeldegeheimnisses zum Urheberrecht – reloaded

Bereits im Jahresbericht 2006 hatten wir über den Referentenentwurf für ein „Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ berichtet, mit dem eine europäische Richtlinie[211] umgesetzt und neue Instrumente zum Schutz von Urheber- und anderen gewerblichen Schutzrechten eingeführt werden sollen. Dort hatten wir insbesondere darauf hingewiesen, dass die Richtlinie den Mitgliedstaaten keineswegs zwingend vorschreibt, zur Erfüllung des in Art. 8 vorgesehenen Auskunftsanspruchs die Mitteilung von Verkehrsdaten

[209] vg. § 113 Abs. 1 TKG

[210] vgl. zuletzt Entschließung der 73. Konferenz am 8./9. März 2007 „Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen“; Dokumentenband 2007, S. 9

[211] Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates v. 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums, ABl. EU L 195/16

und damit einen Eingriff in das Fernmeldegeheimnis vorzusehen[212]. Diese Auffassung wird nunmehr gestützt durch ein Urteil des Europäischen Gerichtshof vom 29. Januar 2008[213]. Im Rechtsstreit zwischen spanischen Rechteinhabern und einer spanischen Telefongesellschaft hat der Gerichtshof betont, dass die Mitgliedstaaten nicht dazu verpflichtet sind, Rechteinhabern den Zugriff auf Verkehrsdaten zur Durchsetzung zivilrechtlicher Ansprüche zu gestatten. In jedem Fall müssen die Mitgliedstaaten ein angemessenes Gleichgewicht zwischen den durch die Gemeinschaftsrechtsordnung geschützten Grundrechten sicherstellen. Auch Maßnahmen zur Durchsetzung des Urheberrechts müssen daher das Grundrecht auf Datenschutz und den Verhältnismäßigkeitsgrundsatz wahren.

Im Gegensatz dazu sind bereits sei einiger Zeit Rechteinhaber dazu übergegangen, massenweise Strafanzeigen zu stellen bzw. durch beauftragte Unternehmen oder Anwälte wegen vermuteter Urheberrechtsverletzungen stellen zu lassen. Die Ermittlungen werden zwar regelmäßig eingestellt, ohne dass es zu einer Anklage kommt. Allerdings haben die Strafverfolgungsbehörden in der Vergangenheit die personenbezogenen Daten zu den von den Rechteinhabern aufgelieferten IP-Adressen bei den Access-Providern abgefragt und den Ermittlungsakten hinzugefügt. Nach Akteneinsicht haben die Anwälte der Rechteinhaber die Daten dazu genutzt, die Betroffenen mit Schadensersatzforderungen zu überziehen. Aus dieser Praxis haben einige findige Unternehmen ein regelrechtes Geschäftsmodell gemacht. Die Staatsanwaltschaften sind teilweise mit zehntausenden solcher Anzeigen überhäuft worden, wie in der Presse berichtet[214]. Auch aus Datenschutzsicht ist dieses Vorgehen bedenklich, da hier auf indirektem Wege Daten für die private Rechtsverfolgung in Erfahrung gebracht werden können, für die eine Auskunftserteilung bei den Anbietern von Telekommunikationsdienstleistungen selbst gesetzlich nicht vorgesehen ist.

Es ist daher zu begrüßen, dass sich bereits seit einiger Zeit Gerichte und Staatsanwaltschaften in der Bundesrepublik dieser Praxis zunehmend widersetzen. So hat das Amtsgericht Offenburg in einem Beschluss vom 20. Juli 2007[215] eine von der dortigen Staatsanwaltschaft beantragte Ermittlungsmaßnahme in Bezug auf zwei illegal zum Download bereitgestellte MP3-Dateien „... wegen offensichtlicher Unverhältnismäßigkeit abgelehnt“. Medienberichten zufolge hatte bereits im Früh-

[212] JB 2006, 10.1.3

[213] Rechtssache C-275/06 „Productores de Música de España (Promusicae) gegen Telefónica de España SAU“, Nr. 125

[214] vgl. z. B. FAZ v. 4. Dezember 2007: „10.000 Euro für das Lied, 3.000 Euro für den Anwalt. Tauschbörsen im Internet: Die Methoden der Abmahnanwälte“

[215] 4 Gs 442/07

jahr 2007 die Generalstaatsanwaltschaft Celle die Aufnahme von Ermittlungen bezüglich einer „riesigen Zahl“ von Strafanzeigen gegen mutmaßliche Tauschbörsennutzer abgelehnt und das Vorliegen eines öffentlichen Interesses an der Strafverfolgung verneint. Die Berliner Staatsanwaltschaft hat bereits im Oktober 2006 in einem anderen Fall die Aufnahme von Ermittlungen abgelehnt und den Rechteinhabern vorgeworfen, „…unter dem Deckmantel vorgeblicher Strafverfolgung die zur Durchsetzung zivilrechtlicher Ansprüche erforderlichen Personaldaten unentgeltlich unter Einsatz beschränkter Strafverfolgungsressourcen finanziell zulasten des Berliner Landeshaushalts beschaffen…“ zu wollen. Auch von ihr wird ein öffentliches Interesse an der Strafverfolgung verneint, da es sich ausnahmslos um Bagatellstraftaten handele[216].

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte sich bereits 2006 grundsätzlich gegen die Einführung von Auskunftsansprüchen über Daten, die dem grundrechtlich geschützten Fernmeldegeheimnis unterliegen, für die Durchsetzung privater Interessen gewandt[217]. Demgegenüber hat sich der Bundesrat im Laufe des Gesetzgebungsverfahrens sogar noch für weitere Verschärfungen des Regierungsentwurfs ausgesprochen: So wurde u. a. die Abschaffung des Richtervorbehalts gefordert (lobend zu erwähnen ist, dass Berlin diese Forderung im Bundesrat nicht mitgetragen hat). Die Bundesregierung hat in ihrer Gegenäußerung dieses Ansinnen abgelehnt und darauf hingewiesen, dass der Richtervorbehalt verfassungsrechtlich angezeigt ist[218]. Der Bundesrat hatte darüber hinaus eine Aufhebung der Beschränkung der Auskunftsansprüche bei Verletzung des Urheberrechts auf Rechtsverletzungen im geschäftlichen Verkehr gefordert.

Das Gesetzgebungsverfahren war bis zum Ende des Berichtzeitraums noch nicht abgeschlossen.

Wir bekräftigen unsere Auffassung, dass von der Einführung eines Auskunftsanspruchs zur Durchsetzung von Urheberrechten über die durch das Fernmeldegeheimnis geschützten Verkehrsdaten abgesehen werden sollte. Völlig inakzeptabel sind die Forderungen des Bundesrates nach noch weiter reichenden Auskunftsansprüchen. Keinesfalls dürfen Daten aus der Vorratsdatenspeicherung[219] für die

[216] Heise Newsticker v. 1. August 2007: „Staatsanwaltschaften verweigern Provider-Abfragen zu IP-Adressen“; http://www.heise.de/newsticker/meldung/print/93693

[217] vgl. Entschließung der 71. Konferenz v. 16./17. März 2006 „Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht“, Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2006“, S. 10

[218] BT-Drs. 16/5048, S. 63

[219] vgl. die Empfehlungen des Rechtsausschusses in der BR-Drs. 798/1/07

Auskunftserteilung verwendet werden. Dies gilt umso mehr, als die ökonomischen Auswirkungen des Angebots urheberrechtlich geschützter (Musik-)Werke über P2P-Plattformen umstritten sind und sich auch nur schwer seriös in Zahlen ausdrücken lassen[220].

12.2 Tele- und Mediendienste

12.2.1 Neue Medienordnung

Im zurückliegenden Berichtszeitraum sind das Telemediengesetz (TMG)[221] und der „Neunte Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge“ in Kraft getreten. Über die vorbereitenden Arbeiten zu diesen Vorhaben hatten wir bereits in den vergangenen Jahren ausführlich berichtet[222].

Die Datenschutzbestimmungen für Anbieter von Tele- bzw. Mediendiensten sind nunmehr im Telemediengesetz zusammengeführt. Tele- und Mediendienste sind unter dem neuen Begriff „Telemedien“ zusammengefasst. Zu den wesentlichen materiellen Gesetzesänderungen gehört, dass der Anwendungsbereich des Gesetzes für solche Telemedien, die „überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen“[223] – dazu zählen laut der amtlichen Begründung Internet-Zugang und E-Mail-Übertragung[224] –, auf einige wenige Regelungen, nämlich das Kopplungsverbot und die dazugehörige Bußgeldvorschrift sowie die Befugnisse der Anbieter zur Bekämpfung von Leistungserschleichung, beschränkt worden ist. Internet-Telefonie (Voice over IP – VoIP) soll ausweislich der amtlichen Begründung ebenfalls nicht unter die Telemediendienste fallen[225]. Dies ist wohl ein Ausdruck der an sich begrüßenswerten Absicht des Gesetzgebers, die bisher bestehenden Unklarheiten bei der Abgrenzung zwischen Telediensten und Mediendiensten einerseits und Telekommunikationsdiensten

[220] vgl. Oberholzer, Felix; Strumpf, Koleman: The Effect of File Sharing on Record Sales. An Empirical Analysis, March 2004; http://www.unc.edu/~cigar/papers/FileSharing_March2004.pdf; Anderson, Brigitte; Frenz, Marion: The Impact of Music Downloads and P2P File-Sharing on the Purchase of Music: A Study for Industry Canada (May 2007)

[221] Telemediengesetz (TMG); Artikel 1 des Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz – ElGVG) v. 26. Februar 2007; BGBl. I, 179

[222] zuletzt JB 2006, 10.2.1

[223] § 11 Abs. 3 TMG

[224] vgl. BR-Drs. 556/06, S. 17

[225] vgl. a. a. O., S. 18

andererseits zu beseitigen. Ein sauberer „Schnitt“ ist jedoch auch nach neuem Recht nicht gelungen, da es sich bei den erwähnten Diensten nach wie vor um Telemedien handelt. Auch ist nicht ersichtlich, warum der Gesetzgeber auf die Fortgeltung wesentlicher weiterer Regelungen des TMG – wie z. B. die Verpflichtung zum Angebot anonymer oder pseudonymer Nutzung gemäß § 13 Abs. 6 TMG – verzichtet hat. Warum diese Dienste dieser Schutzvorschrift nicht mehr bedürfen, wird nicht weiter begründet. Neben den „Restregelungen“ des TMG finden für die o. g. Dienste die Datenschutzbestimmungen des Telekommunikationsgesetzes (TKG) Anwendung.

Durch den Verbleib der Dienste im Regelungsbereich des TMG fehlt es auch an einer sauberen Trennung der aufsichtsbehördlichen Zuständigkeiten, da die Datenschutzkontrolle für Anbieter von Telemedien den Ländern obliegt, während Telekommunikationsdiensteanbieter durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kontrolliert werden. Wie diese gemeinsame Kontrollkompetenz praktisch umgesetzt werden soll, dazu schweigen sowohl Gesetzestext als auch amtliche Begründung.

Bedauerlicherweise hat der Gesetzgeber die Auskunftsverpflichtung der Diensteanbieter über den bisherigen Umfang hinaus auf die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes ausgedehnt[226]. Selbst für die Durchsetzung der Rechte am geistigen Eigentum müssen solche Auskünfte zukünftig erteilt werden, soweit bei der um Auskunft ersuchenden Stelle eine entsprechende Erhebungsbefugnis besteht. Diese Vorhaben hatten wir bereits in unserem letzten Jahresbericht kritisiert und den Gesetzgeber aufgefordert, auf ihre Einführung zu verzichten[227].

Dies sollte im Rahmen der nächsten Novellierung des TMG korrigiert werden. Bei der Schaffung einer eventuellen Verarbeitungsbefugnis zu Zwecken der Datensicherheit muss auch darauf geachtet werden, dass die besonders strengen Regelungen zur Zweckbindung aus § 31 Bundesdatenschutzgesetz (BDSG) mit übernommen werden.

12.2.2 Datenschutz bei Suchmaschinen

In unserem letzten Jahresbericht hatten wir über die Entschließung der 28. Internationalen Konferenz der Datenschutzbeauftragten am 3. November 2006 in

[226] § 14 Abs. 2 TMG

[227] JB 2006, 10.2.1

London zum Datenschutz bei Suchmaschinen berichtet[228]. Nicht zuletzt aufgrund dieser Entschließung haben einige Anbieter von Suchmaschinen ihre Speicherpraxis in der Zwischenzeit geändert. So hat Google bereits im Frühjahr 2007 angekündigt, die Speicherdauer für Suchanfragen auf 18 bis 24 Monate zu beschränken. Bisher hat das Unternehmen Suchanfragen für eine unbeschränkte Zeitdauer gespeichert. Im Rahmen eines öffentlich dokumentierten Schriftwechsels zwischen Google's Global Privacy Counsel und der Art. 29-Datenschutzgruppe hat das Unternehmen unterdessen angekündigt, den Speicherzeitraum auf 18 Monate verkürzen zu wollen. Gleichzeitig ist jedoch auch deutlich geworden, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für die Zukunftsplanung des Unternehmens eine zentrale Rolle spielt: Google's Geschäftsführender Direktor (CEO) Eric Schmidt ließ in einem Interview mit der Financial Times verlauten, das Ziel des Unternehmens sei, möglichst viele persönliche Daten zu sammeln, sodass man den Nutzern in der Zukunft sagen könne, welche Arbeitsangebote sie akzeptieren und was sie morgen tun sollten[229].

Andere Suchmaschinenbetreiber glauben, mit noch kürzeren Speicherzeiträumen auskommen zu können: So kündigte Yahoo! im Juli 2007 an, Recherchedaten nach „nur noch" 13 Monaten anonymisieren zu wollen. Microsoft hingegen hält 18 Monate für erforderlich. Ask.com kündigte demgegenüber die Einführung eines neuen Werkzeugs mit Namen „AskEraser" an, mit dem Nutzer ihre Suchhistorie selbst löschen können. Der Metasuchmaschinen-Anbieter Ixquick sichert den Nutzern gar zu, Nutzungsdaten innerhalb von 24 Stunden zu löschen. Ausgesprochen erfreulich ist, dass sich hier eine Art Wettbewerb um den besten Datenschutz abzuzeichnen scheint.

Hinsichtlich der überwiegenden Mehrzahl der Anbieter ist die Situation allerdings nach wie vor unbefriedigend: So sind bisher keine überzeugenden Gründe dargelegt worden, die mehrmonatige Speicherfristen für Nutzungsdaten über Suchanfragen überzeugend rechtfertigen können.

Die Art. 29-Datenschutzgruppe hat eine Umfrage bei Suchmaschinenanbietern über die Verarbeitungspraxis hinsichtlich personenbezogener Daten gestartet, deren Ergebnisse gegenwärtig ausgewertet werden. Die Arbeitsgruppe plant, im Frühjahr 2008 ein Arbeitspapier zum Datenschutz bei Suchmaschinen zu veröffentlichen.

---

[228] JB 2006, 10.2.3

[229] http:// www.ft.com/cms/s/2/c3e49548-088e-11dc-b11e-000b5df10621.html

Große Aufmerksamkeit in den Medien erfuhr im zurückliegenden Berichtszeitraum auch der geplante Zusammenschluss von Google mit dem Online-Werbeanbieter Doubleclick. Die amerikanische Wirtschaftsaufsichtsbehörde (Federal Trade Commission) prüft derzeit kartellrechtliche Aspekte dieses geplanten Zusammenschlusses. Bereits im April 2007 hatte sich eine amerikanische Bürgerrechtsorganisation mit der Forderung an die FTC gewandt, im Rahmen der kartellrechtlichen Überprüfung auch mögliche Auswirkungen des geplanten Zusammenschlusses auf die Privatsphäre von Internetnutzern in Betracht zu ziehen[230]. Eine ähnliche Forderung haben in der Zwischenzeit auch einige amerikanische Senatoren gegenüber der FTC erhoben[231]. Dennoch hat die FTC den Zusammenschluss inzwischen genehmigt.

Auch die Europäische Kommission hat im November 2007 eine vertiefte Untersuchung des geplanten Unternehmenszusammenschlusses eröffnet[232]. Es wird erwartet, dass die Kommission im Rahmen der wettbewerbsrechtlichen Überprüfung des geplanten Zusammenschlusses mögliche Auswirkungen auf den Schutz der Privatsphäre von Internetnutzern einbeziehen wird.

12.2.3 Bewertung von Hochschullehrern im Internet

Ein eingetragener Verein mit Sitz in Berlin bietet im Internet eine Bewertungsplattform für Lehrveranstaltungen an deutschen, österreichischen und schweizerischen Hochschulen an, die personenbezogene Daten von mehreren zehntausend Dozentinnen und Dozenten an diesen Hochschulen enthalten. Registrierte Studierende können einzelne Veranstaltungen von Dozentinnen und Dozenten bewerten. Der Betreiber bereitet die eingemeldeten Bewertungen datenbankmäßig auf, berechnet die Durchschnitte sowie „Top- und Flop-Listen". Die Bewertungen sind für jedermann im Internet ohne vorherige Registrierung abrufbar.

Bereits im Jahr 2005 hatten wir über eine Internetplattform für Produktinformationen und Produktvergleiche berichtet, die im Rahmen ihres Angebots registrierten Nutzerinnen und Nutzern die Möglichkeit eröffnete, die Leistung von Hochschullehrkräften durch Vergabe von Sternen in Form von sog. Testberichten zu bewerten. Die Beurteilungen standen jedermann zum Abruf über das Internet zur

[230] http://www.epic.org/privacy/ftc/google

[231] http://www.epic.org/privacy/ftc/google/sen_anti_111907.pdf

[232] http://ec.europa.eu/comm/competition/mergers/cases/index/m94.html#m_4731

Verfügung[233]. Diesem Anbieter hatten wir seinerzeit mitgeteilt, dass das Angebot jedenfalls in der damaligen Form datenschutzrechtlich unzulässig war. Der Anbieter hat daraufhin den entsprechenden Teil des Angebots eingestellt.

Auch das Angebot des Berliner Vereins verstößt in der gegenwärtigen Form gegen geltendes Datenschutzrecht, jedenfalls für diejenigen Dozentinnen und Dozenten, die gegenüber dem Betreiber in die Veröffentlichung ihrer Daten nicht eingewilligt haben. Dies ist die überwiegende Mehrzahl der derzeit dort verzeichneten Dozentinnen und Dozenten. Zwar hat der Anbieter im Laufe der mit uns geführten Gespräche bzw. des geführten Schriftwechsels einige aus Datenschutzsicht wünschenswerte Veränderungen bzw. Verbesserungen vorgenommen, allerdings werden andere wesentliche datenschutzrechtliche Bestimmungen nach wie vor nicht eingehalten:

Für die Erhebung, Verarbeitung und insbesondere Veröffentlichung von Bewertungen von Lehrveranstaltungen derjenigen Lehrkräfte, die nicht eingewilligt haben, bedarf es einer Rechtsgrundlage nach dem Bundesdatenschutzgesetz. Vorliegend richtet sich die Verarbeitung nach den Bestimmungen des § 29 des BDSG, da der Anbieter personenbezogene Daten zum Zwecke der Übermittlung verarbeitet. Dies gestattet die genannte Rechtsvorschrift allerdings nur unter bestimmten Bedingungen: So sind die Betroffenen bei erstmaliger Übermittlung nach § 33 Abs. 1 BDSG über diese Tatsache und die Art der übermittelten Daten zu benachrichtigen, ebenso über die Kategorien von Empfängern solcher Übermittlungen. Auf diese Rechtspflicht haben wir die Daten verarbeitende Stelle mehrfach hingewiesen. Der Verein bestreitet jedoch die Verpflichtung zur Benachrichtigung und hat es bisher unterlassen, unsere Aufforderung umzusetzen. Wir haben uns daher gezwungen gesehen, ein Ordnungswidrigkeitenverfahren nach § 43 Abs. 1 Nr. 8 BDSG einzuleiten. Das Verfahren war zum Ende des Berichtzeitraums noch nicht abgeschlossen.

Darüber hinaus erfüllt die derzeitige Praxis der Daten verarbeitenden Stelle auch in anderer Hinsicht die Voraussetzungen des § 29 BDSG nicht: So haben die betroffenen Lehrkräfte ein schutzwürdiges Interesse schon am Ausschluss der Erhebung, Speicherung oder Veränderung der Bewertung gemäß § 29 a Abs. 1 Nr. 1 BDSG, da die Daten verarbeitende Stelle bisher nicht hinreichend sicherstellt, dass nur solche Studierende eine Veranstaltung bewerten können, die sie tatsächlich auch besucht haben. Gegenwärtig kann sich vielmehr jedermann (also auch z. B. Nachbarn, Konkurrenten usw.) auf der Plattform registrieren und dort Bewertungen abgeben. Auch die gegenwärtige Form der Veröffentlichung der Daten

[233] JB 2005, 5.2

widerspricht dem geltenden Datenschutzrecht, da in § 29 Abs. 2 Nr. 1 a BDSG vorgesehen ist, dass Dritte, denen die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft darlegen müssen. Auf die Umsetzung dieser Darlegungspflicht – und erst recht ihrer mindestens stichprobenartigen Überprüfung – verzichtet der Anbieter bisher. Hinsichtlich dieser weiteren Verstöße prüfen wir ebenfalls die Einleitung aufsichtsbehördlicher Maßnahmen.

Das Grundrecht auf freie Meinungsäußerung[234], auf das sich die Nutzerinnen und Nutzer (nicht aber die Betreiber der Plattform) berufen können, entbindet die Betreiber der Plattform nicht von der Einhaltung datenschutzrechtlicher Bestimmungen.

Wenn ein Anbieter personenbezogene Daten Dritter datenbankmäßig aufbereitet zum Abruf im Internet bereithält, so ist dies nur unter den Bedingungen des § 29 BDSG zulässig, sofern die Betroffenen nicht eingewilligt haben. Dem steht auch nicht entgegen, dass die einzelnen Beiträge (Bewertungen) möglicherweise durch das Recht auf Meinungsäußerung aus Artikel 5 GG gedeckt sind.

12.3 Soziale Netzwerke

Online-Communities sind Webangebote, die es ermöglichen, private Profile ähnlich einer privaten Homepage anzulegen und sich mit anderen Mitgliedern der Online-Community auszutauschen. Dazu schickt man sich beispielsweise einander Nachrichten, verlinkt andere Profile als Freunde, schreibt in Gästebücher und tauscht sich in Gruppen zu unterschiedlichen Themen aus. Viele Nutzerinnen und Nutzer stellen sich in ihren Profilen recht offenherzig dar. Von den Anbietern wird dies unterstützt, indem Eingabefelder für die verschiedensten persönlichen Daten wie z. B. Name, Alter, Wohnort, Interessen, Ausbildung und Arbeitsplatz vorgesehen sind. Dies betrifft auch Daten, die vom Gesetzgeber nicht ohne Grund als besonders sensibel eingestuft wurden, wie beispielsweise die politische und religiöse Überzeugung und die sexuelle Orientierung. Ein weiteres Datenschutzrisiko stellt die Möglichkeit dar, Fotos zu veröffentlichen, auf welchen man zudem die Profile der dargestellten Personen verlinken kann – oft ohne deren vorherige Einwilligung. Die Nutzerinnen und Nutzer sind sich überwiegend nicht bewusst, dass – je nach den Umständen des Einzelfalls – die unbefugte Veröffentlichung von Bildern nach

[234] Artikel 5 Grundgesetz (GG)

einer wenig bekannten Vorschrift aus dem Kunsturhebergesetz mit Freiheits- oder Geldstrafe geahndet werden kann[235].

Im Ergebnis entsteht eine oft für jedermann nach konkreten Kriterien durchsuchbare Personendatenbank, die nicht nur die obigen Daten und Fotos zu jeder Person enthält, sondern außerdem auch das gesamte Beziehungsgeflecht der Personen untereinander. Zwar ermöglichen einige Dienste die Einschränkung von Zugriffen auf das eigene Profil – beispielsweise auf die selbst gewählten Freunde –, aber derartige Optionen sind meist entweder nicht ausreichend, nicht praktikabel genug oder werden nur „versteckt" angeboten. Außerdem sind die von den Betreibern vorgesehenen Voreinstellungen häufig wenig datenschutzfreundlich gewählt.

Ein weiteres entscheidendes Dilemma ist die geringe Sensibilität der Nutzerinnen und Nutzer bezüglich der eigenen Daten. Übersehen werden oft die möglichen Folgen für das spätere Leben: Es ist sehr schwer bis unmöglich, selbst unbequeme Daten wieder zu löschen, wenn sie erst einmal im Internet veröffentlicht sind. Das Internet kennt bisher kein Vergessen. Schon der einzelne Internetnutzer ist prinzipiell in der Lage, Inhalte beliebiger Webseiten, also auch die Online-Profilseiten anderer Personen, zu kopieren und damit im privaten Umfang zu archivieren. Vermehrt gibt es auch Dienste wie die Personen-Suchmaschinen „spock.com" und „yasni.de", die u. a. explizit Profile aus Online-Communities in ihren Suchergebnissen auflisten. Es steht zu befürchten, dass derartige Suchmaschinen bzw. andere Dienstleister auch alte Versionen von möglicherweise längst gelöschten Nutzerprofilen in Online-Communities protokollieren und zahlenden Interessenten zur Verfügung stellen. Vereinfacht wird dies von der neuen Technik „OpenSocial", die eine standardisierte Schnittstelle zu vielen Online-Communities schafft und so ein sehr einfaches Auslesen und Abgleichen von Daten über Community-Grenzen hinweg ermöglicht.

Ein weiteres Problem stellen beispielsweise die Aktivitäten der amerikanischen Online-Community „Facebook" im Bereich Online-Werbung dar. Zur Individualisierung der Werbebotschaften werden hier nicht nur die persönlichen Daten, sondern sogar das persönliche Umfeld herangezogen. So wurde z. B. eine Art Empfehlungswerbung stark kritisiert, bei der der Freundeskreis eines Facebook-Nutzers informiert wird, dass dieser ein bestimmtes Video ausgeliehen oder ein bestimmtes Buch gekauft hat.

[235] vgl. § 33 Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG)

Unserer Aufsicht unterliegen die in Berlin ansässigen Online-Communities „studiVZ“ und „schülerVZ“. Die im letzten Jahr bekannt gewordenen akuten Sicherheitslücken konnten erfreulicherweise beseitigt werden[236]. Auch wurden problematische Funktionen, wie beispielsweise die Möglichkeit, auf Fotos abgebildete Personen mit dem jeweiligen Nutzerprofil zu verlinken, so eingeschränkt, dass ein Missbrauch jedenfalls erschwert wird. Einige weitere aus unserer Sicht notwendige Änderungen wurden zwar von den Betreibern zugesagt, ihre Umsetzung stand aber zum Ende des Berichtszeitraums noch aus. Außerdem kündigten die Betreiber von „StudiVZ“ Ende 2007 an, personalisierte Werbung auf ihrer Plattform einführen zu wollen, was neue gravierende datenschutzrechtliche Fragen aufwarf, die bei Redaktionsschluss noch ungelöst waren.

Online-Communities stellen den Datenschutz vor neue Herausforderungen, die wahrscheinlich nicht allein mit aufsichtsrechtlichen Maßnahmen gelöst werden können. Notwendig sind auch eine Sensibilisierung der Nutzerinnen und Nutzer bezüglich der von ihnen freiwillig veröffentlichten Daten und Forschungsaktivitäten für einen möglichst idealen Weg, um ein hohes Datenschutzniveau zu erreichen und zugleich die zukunftsweisenden Funktionalitäten der Community-Plattformen zu erhalten.

12.3.1 Speicherung vollständiger IP-Adressen bei Content-Providern

Das Landgericht Berlin hat am 6. September 2007 das Bundesministerium der Justiz dazu verurteilt, es zukünftig zu unterlassen, die IP-Adressen von Nutzerinnen und Nutzern der Website des Ministeriums über das Ende des jeweiligen Nutzungsvorgangs hinaus zu speichern[237].

Wir haben bereits in der Vergangenheit in unserer Kontrollpraxis – und vielfach zum Erstaunen der Betreiber von Internetangeboten – immer wieder darauf hingewiesen, dass es sich bei IP-Adressen (auch wenn sie dynamisch durch den Access-Provider vergeben werden) um personenbezogene Daten handelt. Diese Daten dürfen nach den Bestimmungen des Telemediengesetzes (TMG) über das Ende der Verbindung hinaus nur verarbeitet werden, soweit sie für die Abrechnung der Inanspruchnahme von Telemedien erforderlich sind[238] oder die Betroffenen

[236] JB 2006, 10.2.4
[237] 23 S 3/07
[238] § 15 TMG

eingewilligt haben[239]. Daneben haben wir lediglich eine kurzfristige Speicherung und Auswertung der IP-Adressen unter dem Gesichtspunkt der Gewährleistung der Datensicherheit in der IT-Infrastruktur in Einzelfällen für zulässig erachtet[240].

12.3.2 Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

Der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im zurückliegenden Berichtszeitraum die Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz überarbeitet. Die Orientierungshilfe wurde an die neue Rechtslage nach Inkrafttreten des Telemediengesetzes angepasst. Außerdem sind Empfehlungen zum datenschutzgerechten Einsatz von Virenscannern und Spamfiltern überarbeitet bzw. neu aufgenommen worden. Die Orientierungshilfe kann in unserem Internetangebot abgerufen werden[241].

12.4 Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation

Die Arbeitsgruppe hat auf ihren turnusmäßigen halbjährlichen Treffen unter dem Vorsitz des Berliner Beauftragten für Datenschutz und Informationsfreiheit drei Arbeitspapiere verabschiedet:

- Das Arbeitspapier zum grenzüberschreitenden Telemarketing enthält Empfehlungen zum Schutz der Privatsphäre bei grenzüberschreitenden Werbeanrufen[242].

- Das Arbeitspapier zu elektronischen Fahrscheinen im öffentlichen Personenverkehr gibt Empfehlungen zum Schutz der Privatsphäre beim „Electronic Ticketing“. Insbesondere wird auf die Notwendigkeit hingewiesen, die Möglichkeit zur anonymen Nutzung der Verkehrsmittel zu gewährleisten[243].

---

239 § 12 Abs. 1, 2 TMG

240 JB 2004, 5.2

241 http://www.datenschutz-berlin.de/recht/de/rv/tk_med/OH_Internet_und_e-mail_am_%20Arbeitsplatz_Oktober_2007.pdf

242 vgl. Dokumentenband 2007, S. 98

243 vgl. a. a. O, S. 100

- Das Arbeitspapier zu Datenschutzfragen bei der Verteilung digitaler Medieninhalte und beim digitalen Fernsehen erläutert die mit dem Übergang vom Analog- zum Digitalfernsehen und dessen Verbreitung über Breitband-Netzwerke einhergehenden Risiken für den Schutz der Privatsphäre der Nutzerinnen und Nutzer. Es wird insbesondere auf die Konvergenz[244] der verschiedenen Netzwerke hingewiesen und auf die neuen Möglichkeiten, die sich durch den Medienkonsum auf mobilen Geräten ergeben. Die neuen Technologien bieten erstmals das Potenzial für eine umfassende Registrierung des Nutzungsverhaltens. Es könnten Aufzeichnungen darüber entstehen, wer wann welche Sendung im Fernsehen gesehen hat. Die Arbeitsgruppe weist insbesondere auf die Notwendigkeit hin, die Möglichkeit zur anonymen Nutzung und ggf. Bezahlung auch unter den Bedingungen des digitalen Fernsehens zu erhalten[245].

Die zwischen 1983 und 2006 von der Arbeitsgruppe verabschiedeten Dokumente („Gemeinsame Standpunkte“ und „Arbeitspapiere“) sind im zurückliegenden Berichtszeitraum in einer Broschüre „Internationale Dokumente zu Datenschutz bei Telekommunikation und Medien“ zusammengefasst herausgegeben worden, die bei uns bezogen werden kann. Die Broschüre steht auch in unserem Internetangebot zum Abruf bereit[246].

12.5 Internationales Symposium „Datenschutz beim digitalen Fernsehen“

Unser diesjähriges Symposium zum Datenschutz im Rahmen der Internationalen Funkausstellung befasste sich mit dem Datenschutz beim digitalen Fernsehen. Bei der bis vor einigen Jahren üblichen analogen Ausstrahlung von Fernsehsignalen konnte durch niemanden nachvollzogen werden, wer wann welche Sendungen sieht. Die analoge Übertragung wird jedoch in absehbarer Zeit der Vergangenheit angehören, allein schon weil die gegenwärtig dafür reservierten Frequenzen bald nicht mehr zur Verfügung stehen werden.

Die neue digitalisierte Infrastruktur könnte erstmals eine Registrierung des individuellen Mediennutzungsverhaltens ermöglichen. Auch die zunehmende Individualisierung von Angeboten (etwa Spartenkanälen, Video on Demand oder Pay-

[244] vgl. dazu grundsätzlich 1.1

[245] vgl. Dokumentenband 2007, S. 103

[246] http://www.datenschutz-berlin.de/doc/int/iwgdpt/IWGDPT_WP_brochure.pdf

per-View) und die Nutzung neuer Vertriebswege (z. B. Internet-, Handy-TV) könnten diesen Trend weiter verstärken.

Auf dem Symposium wurden die damit verbundenen Risiken diskutiert und inwieweit diese Entwicklung zukünftig die Möglichkeit zur anonymen Nutzung von Fernsehprogrammen und damit das Grundrecht auf Meinungs- und Informationsfreiheit gefährden könnte. Internationale Experten aus Wissenschaft, Wirtschaft und Verwaltung diskutierten, welche Lösungen sich bieten und wie z. B. Rundfunkveranstalter, Plattformbetreiber und Hersteller den Schutz der Privatsphäre der Nutzerinnen und Nutzer bei der Gestaltung von digitalen Angeboten berücksichtigen. Darüber hinaus wurde die Fragestellung erörtert, ob es Unterschiede zwischen den verschiedenen Technologien gibt, die zur Übertragung digitalen Rundfunks genutzt werden, und ob der vorhandene Regulierungsrahmen ausreicht, um einen wirksamen Schutz der Privatsphäre der Nutzerinnen und Nutzer zu gewährleisten. Materialien zu den Vorträgen der einzelnen Referentinnen und Referenten können in unserem Internetangebot abgerufen werden[247].

Der Empfang von Rundfunk über das Internet scheint für viele Anbieter ein Erfolg versprechendes Geschäftsmodell zu sein. So ist es nicht verwunderlich, dass im Laufe des Jahres 2007 weitere Angebote dieser Art auf den Markt gekommen sind. Einige dieser Angebote sind werbefinanziert. Einige Anbieter lassen sich in Online-Fragebögen von ihren Kundinnen und Kunden über deren Interessen informieren und nutzen diese Daten – wie auch Nutzungsdaten über die abgerufenen Inhalte – zum Einspielen zielgerichteter Werbung. Eine solche Nutzung wäre nach deutschem Recht für hier ansässige Anbieter nur mit ausdrücklicher Einwilligung der Nutzerinnen und Nutzer gestattet. Diese Regelung findet jedoch keine Anwendung auf Anbieter, die nicht in Deutschland belegen sind.

Nutzerinnen und Nutzer sollten sich vor dem Abschluss eines Abonnements zum digitalen Fernsehen darüber informieren, von wo aus ein Angebot bereitgestellt wird und welches Datenschutzrecht in diesem Land gilt, sowie darüber, ob und ggf. wofür der Anbieter Nutzungsdaten über einzelne Sendungen – z. B. zu Werbezwecken – verarbeitet.

[247] http://www.datenschutz-berlin.de/aktuelle/termine/07/bln/symposium_2007.htm

13 Informationsfreiheit

13.1 Entwicklungen für mehr Transparenz

Eine Expertengruppe des Europarats hat den *Entwurf einer Konvention zur Informationsfreiheit* erarbeitet, der im nächsten Frühjahr von seinem Lenkungsausschuss für Menschenrechte abschließend beraten wird. Die Bemühungen des Europarats sind zu begrüßen, wird damit doch ein für seine 47 Mitgliedstaaten völkerrechtlich verbindliches Übereinkommen geschaffen. Allerdings ist der Entwurf verbesserungsbedürftig, denn er bleibt hinter der Empfehlung des Europarats von 2002 zurück, aber auch hinter der deutschen Gesetzgebung. Dies betrifft vor allem den Anwendungsbereich, der ausschließlich die öffentliche Verwaltung umfasst, Gesetzgebung und Justiz aber unberechtigterweise vollständig ausnimmt. Außerdem sind private Einrichtungen auch dann nicht vom Informationszugang erfasst, wenn öffentliche Aufgaben auf sie übertragen wurden. Schließlich fehlt ein Beschwerderecht für den Fall, dass der Informationszugang nicht innerhalb einer bestimmten Frist gewährt wurde. Die *Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK*, ehemals bezeichnet als AGID, Arbeitsgemeinschaft der Informationsfreiheitsbeauftragten in Deutschland) hat diese Unzulänglichkeiten der Expertengruppe mitgeteilt und an sie appelliert, den Standard der Europaratsempfehlung beizubehalten und diese für rechtlich verbindlich zu erklären.

Die Europäische Kommission hat im Rahmen ihrer „Europäischen Transparenzinitiative“ eine Überprüfung der Verordnung (EG) Nr. 1049/2001[248] über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (*„EU-Transparenz-Verordnung“*) initiiert und deshalb ein öffentliches Konsultationsverfahren eingeleitet, das Aufschluss geben soll über Erfahrungen mit dem Recht auf Zugang der Öffentlichkeit zu Dokumenten im Besitz der Organe der Europäischen Gemeinschaft. Die IFK hat eine gemeinsame Stellungnahme zur Überarbeitung der Transparenz-Verordnung abgegeben und für eine aktive Verbreitung von Informationen sowie für eine einheitliche Regelung des Zugangs zu Schriftstücken und Umweltinformationen plädiert, aber auch für eine eindeutiger gefasste Ausnahmeregelung, nach der die Offenbarung wegen geschäftlicher oder wirtschaftlicher Interessen Dritter nicht in Betracht kommt.

[248] ABl. L 145 v. 31. Mai 2001, S. 43

Zu diesem Themenkomplex, dem *Schutz von Betriebs- und Geschäftsgeheimnissen*, hat die IFK zudem eine Entschließung gefasst[249], weil sich deutschlandweit beträchtliche Rechtsunsicherheiten bei Anwendung dieses Ausnahmetatbestandes gezeigt haben, die zu einer allzu restriktiven Handhabung des Informationsrechts führten.

Wieweit dieser Schutz reicht, hat das *Oberverwaltungsgericht (OVG) Berlin-Brandenburg* in mehreren Berufungsverfahren gegen das Land Berlin entschieden[250]. Danach unterliegen sowohl die Genehmigung der Berliner Wassertarife als auch die für die Abfallentsorgung sowie die von den Unternehmen (BWB und BSR) vorgelegten Kalkulationsunterlagen dem Informationszugang, soweit die Unterlagen Daten enthalten, die das jeweilige Berliner Monopolgeschäft der genannten Betriebe betreffen.

Auch das *Bundesverfassungsgericht* hat eine Entscheidung für mehr Transparenz getroffen. Es hat die Anträge von Bundestagsabgeordneten zurückgewiesen, die sich im Wege der Organklage gegen den Verhaltenskodex des Deutschen Bundestages von 2006 wandten[251]. Danach sind sie zur Offenlegung ihrer Nebeneinkünfte gegenüber dem Bundestagspräsidenten verpflichtet. Dieser reagierte auf die Entscheidung sofort mit der Veröffentlichung der bis dahin zurückgehaltenen Nebeneinkünfte im Internet, die in drei Einkommensstufen dargestellt werden. Manchen geht dies nicht weit genug. Sie fordern die Offenlegung der konkreten (Neben-)Einkünfte, denn die Öffentlichkeit habe ein Recht zu wissen, wie sich die Vergütung der Abgeordneten zusammensetzt.

Deshalb tritt auch der *EU-Bürgerbeauftragte* für mehr Transparenz bei den Vergütungen der Parlamentarier ein. Er fordert nach einer Konsultation des Europäischen Datenschutzbeauftragten sogar, Einzelheiten über die finanziellen Zuwendungen an die Abgeordneten öffentlich zugänglich zu machen, wozu die allgemeinen Ausgaben, Reisekosten und Tagegelder gehören.

Wo (Steuer-)Gelder dem Staat ab- oder zufließen, ist das Interesse der Bevölkerung an Transparenz naturgemäß am größten. Deshalb ist die Entscheidung der Bundesregierung zu begrüßen, künftig die Sponsoren der Bundesbehörden namentlich (wenn auch erst ab einer Zuwendungshöhe von 5.000 Euro) im alle zwei Jahre erscheinenden *Sponsoringbericht* zu veröffentlichen.

---

[249] Entschließung v. 11. Juni 2007 „Informationsfreiheit bei Betriebs- und Geschäftsgeheimnissen stärken!“, vgl. Dokumentenband 2007, S.107

[250] Urteile v. 2. Oktober 2007 – OVG 12 B 9., 11. und 12.07

[251] BVerfG, Urteil v. 4. Juli 2007 – 2 BvE 1/06, 2 BvE 2/06, 2 BvE 3/06, 2 BvE 4/06

Auch in der *Landesgesetzgebung* sind Fortschritte zu verzeichnen. So hat Thüringen als nunmehr neuntes Bundesland ein Informationsfreiheitsgesetz verabschiedet, leider ohne einen Informationsfreiheitsbeauftragten vorzusehen. Die Landtage von Hessen und Sachsen-Anhalt haben Anhörungen veranstaltet, bei denen die IFK eine gemeinsame Position bezogen hat bzw. wir vor Ort eine Stellungnahme abgegeben haben.

13.2 Informationsfreiheit im Land Berlin

Einen *Sponsoringbericht für die öffentliche Verwaltung in Berlin* einzuführen, ist eine politische Forderung[252], die wir unterstützen. Eine Berichtspflicht, die es nicht nur auf Bundesebene, sondern auch in Bundesländern wie Baden-Württemberg, Hamburg, Niedersachsen und Sachsen geben soll, sehen wir als Meilenstein für mehr Transparenz im „juristischen Graubereich" des Sponsorings.

Als ähnlich bedeutsam stufen wir die *Transparenz im Subventionsbereich* ein[253]. Wer öffentliche Fördermittel in Anspruch nimmt, hat nicht von vornherein ein schutzwürdiges Interesse, dass dies geheim bleibt. Allerdings sollte eine künftige Regelung vorsehen, dass Interessentinnen und Interessenten vorab darauf hingewiesen werden, in welchem Umfang personenbezogene Daten im Internet veröffentlicht werden. Das Abgeordnetenhaus[254] hat den Senat beauftragt, nach dem Vorbild der EU[255] die rechtlichen Grundlagen zu schaffen für eine Internet-Veröffentlichung der Zuwendungsempfänger einschließlich der Adresse, des Zwecks der Finanzhilfe und der Höhe der Zuwendung. Hierzu sollen die Ausführungsvorschriften (AV) zu § 44 Landeshaushaltsordnung (LHO) geändert werden. Bei dem uns vorgelegten Entwurf sind wir insbesondere dafür eingetreten, dass die inzwischen gängige, von der Rechtsprechung geprägte Definition des „Betriebs-/Geschäftsgeheimnisses" aufgenommen wird, weil sie den Verwaltungen häufig nicht bekannt ist.

Daneben sind *weitere Transparenzinitiativen* zu erwähnen, die den Staat bürgerfreundlicher machen. So hat die Senatsverwaltung für Integration, Arbeit und Soziales den *„Runden Tisch Pflegequalität"* gegründet, dem Vertreterinnen und

[252] Antrag der FDP-Fraktion, Abgh.-Drs. 16/0966

[253] vgl. dazu Antrag der Fraktion Bündnis 90/Die Grünen „Transparenz bei Zuwendungen schaffen", Abgh.-Drs. 16/0250

[254] 19. Sitzung v. 11. Oktober 2007

[255] bereits JB 2006, 11.2

Vertreter von Heimbetreibern, Pflegekassen, Einrichtungen des Verbraucherschutzes und Betroffeneninitiativen angehören. Er hat ein Muster für einen „Freiwilligen Transparenz- und Qualitätsbericht“ erarbeitet. Damit sollen Patientinnen, Patienten und Angehörige künftig die Qualität der Pflege in den ca. 300 Berliner Pflegeheimen besser vergleichen können. Dazu gehört auch die Veröffentlichung der Ergebnisse von Prüfungen durch die Heimaufsicht und den Medizinischen Dienst der Krankenversicherung. Die Ergebnisse werden online abrufbar sein.

Ein weiteres positives Beispiel für mehr Transparenz ist der *Bezirk Marzahn-Hellersdorf*. Dort wird bereits seit 2002 eine Statistik über Anträge nach Berliner Informationsfreiheitsgesetz (IFG) geführt und neuerdings zur Beschlussfassung dem Bezirksamt und zur Information der BVV vorgelegt. Die jüngsten Zahlen belegen die informationszugangsfreundliche Haltung im Bezirk, die sich zudem durch eine bürgerfreundliche Gebührenerhebung auszeichnet.

Diese guten Beispiele können allerdings nicht darüber hinwegtäuschen, dass in Berlin bisher fast flächendeckend ein zentraler Pfeiler für Transparenz nicht beachtet wird, der gesetzlich vorgesehen ist: Nach § 17 Abs. 4 IFG hat jede öffentliche Stelle Verzeichnisse zu führen, die geeignet sind, die Aktenordnung und den Aktenbestand sowie den Zweck der geführten Akten erkennen zu lassen. Darüber hinaus hat jede öffentliche Stelle Register, Aktenpläne, Aktenordnungen, Aktenverzeichnisse, Einsenderverzeichnisse, Tagebücher und Verzeichnisse im Sinne von Satz 1 allgemein zugänglich zu machen. Die Behörden trifft mithin eine umfassende Veröffentlichungspflicht hinsichtlich aller vorhandenen Informationszusammenstellungen. Diese sachgebietsunabhängigen allgemeinen Publizitätspflichten des Staates sind Grundvoraussetzung für die eigenständige Wahrnehmung der Informationszugangsmöglichkeiten des Menschen. Wir veröffentlichen unsere Aktenpläne in unserem Internetprogramm seit Jahren.

13.2.1 Der Gefangene und das Gutachten zur Privatisierung des Strafvollzugs

Ein in Baden-Württemberg Inhaftierter hatte bei der Senatsverwaltung für Justiz die Übersendung von Kopien des „Gutachtens zur Untersuchung alternativer Realisierungsformen der Justizvollzugsanstalt Heidering des Landes Berlin“ sowie das erläuternde Schreiben der Senatsverwaltung beantragt. Nach drei Monaten teilte sie dem Petenten mit, dass die Übersendung von Kopien „entbehrlich“ sei, da die Unterlagen allgemein zugänglich veröffentlicht und im Internet (unter einer konkret benannten Adresse) abrufbar seien. Der Petent hat sich daraufhin Hilfe suchend an

uns gewandt. Aufgrund unserer Intervention hat die Senatsverwaltung ihre Entscheidung überprüft. Sie kam zu dem Ergebnis, dass der Übersendung von Kopien möglicherweise Urheberrechte entgegenstehen. Denn das Gutachten, das aus 150 Seiten zuzüglich 30 Seiten Anlagen besteht, beinhalte auch individuelle Vertragsgestaltungen. Da Urheberrechte zumindest nicht auszuschließen seien, solle die Einwilligung der Berechtigten eingeholt werden. Sie wurde trotz der Verfügbarkeit der Unterlagen im Internet teilweise verweigert.

Nach § 13 Abs. 5 Satz 1 IFG sind der Antrag stellenden Person Ablichtungen anzufertigen und zur Verfügung zu stellen. Das Gesetz sieht eine Einschränkung oder den Ausschluss dieses Anspruchs in Fällen, in denen die öffentliche Stelle die Informationen über das Internet allgemein zugänglich gemacht hat, nicht vor. Für eine entsprechende Auslegung des IFG ist angesichts der detaillierten Einschränkungen des Informationszugangsrechts kein Raum. Selbst wenn dem so wäre, war im vorliegenden Fall die Tatsache zu berücksichtigen, dass der Petent als Inhaftierter nicht über einen Internetzugang verfügt. Er kann auch nicht darauf verwiesen werden, wie ein „Unmündiger" einen Ausdruck bei einem Vollzugsbediensteten zu beantragen. Nach § 13 Abs. 5 Satz 2 IFG ist von der öffentlichen Stelle die Einwilligung der Berechtigten einzuholen, soweit der Überlassung von Ablichtungen Urheberrechte entgegenstehen. Diese *urheberrechtliche* Regelung betrifft allein die *Verwertung* der erlangten Informationen, nicht aber den Informationszugang als solchen. Zudem kann der Einwand dann nicht gelten, wenn die Unterlagen ins Internet gestellt wurden, wo sie von jedermann abgerufen und ausgedruckt werden können – aber eben nicht von Inhaftierten.

Nach § 13 Abs. 5 Satz 3 IFG besteht kein Anspruch auf Ablichtungen, wenn die Berechtigten die Einwilligung verweigern. Angesichts der bereits erfolgten Veröffentlichung im Internet war die Verweigerung der Einwilligung von zwei der drei Berechtigten für uns zunächst überraschend, dann aber nachvollziehbar, weil die Senatsverwaltung – entgegen der Absprache mit uns – die Berechtigten nicht auf die bereits erfolgte Veröffentlichung im Internet hingewiesen hatte. Wir hatten diese Vorgehensweise, die Einwilligung der Berechtigten einzuholen, ausnahmsweise befürwortet, weil sie weniger zeitaufwändig schien als die eigentlich vorrangige Prüfung, ob tatsächlich Urheberrechte der Überlassung von Kopien entgegenstehen. Dies war nicht der Fall, wie die Senatsverwaltung für Justiz letztendlich feststellen musste. Deshalb waren die Weigerungen der Berechtigten nach § 13 Abs. 5 Satz 2 IFG nicht relevant.

13.2

Die Urheberrechtsklausel in § 13 Abs. 5 IFG betrifft nur die Frage der Verwertung erlangter Informationen. Sie steht dem Informationszugang als solchem (durch Herausgabe von Kopien) nicht entgegen.

13.2.2 Asbestgutachten über eine Grundschule

Besorgte Eltern haben über einen Rechtsanwalt bei der Schulbehörde Tempelhof-Schöneberg Einsicht in die Asbestgutachten zu einer Grundschule beantragt, die seit 1994 erstellt worden sind. Darüber hinaus wurde Einsicht in diejenigen Akten verlangt, die die schulorganisatorischen Maßnahmen zur Asbestsanierung bzw. Schließung der Grundschule beinhalten. Die Schulbehörde bewilligte die Akteneinsicht in die Gutachten, untersagte aber das Kopieren, da „keine Genehmigung des Gutachters vorliegt". Die darüber hinausgehende Akteneinsicht wurde unter Hinweis auf den schützenswerten „allgemeinen Willensbildungsprozess innerhalb von und zwischen Behörden" abgelehnt. Als Verwaltungsgebühr wurde die höchste von 511,29 Euro festgesetzt.

Nach dem eindeutigen Wortlaut von § 13 Abs. 5 Satz 2 IFG ist die Einwilligung des Gutachters erst dann einzuholen, wenn das Amt zuvor festgestellt hat, inwieweit durch die Überlassung von Kopien überhaupt Urheberrechte des Gutachters entgegenstehen. Aus der Formulierung folgt zugleich, dass dies nicht immer der Fall ist. Da die Schulbehörde eine entsprechende Prüfung nicht vorgenommen hat, ist die verweigerte Einwilligung des Gutachters unerheblich gewesen. Wir haben dies der Schulbehörde mitgeteilt und gebeten, bei der Abfassung des Widerspruchsbescheides zu berücksichtigen, dass nur eine urheberrechtswidrige Verwertung der Informationen berücksichtigt werden darf. Eine solche Verwertung wäre etwa dann gegeben, wenn Dritte die Feststellungen des Urhebers als eigene ausgeben. Ein derartiges Vorgehen stand allerdings nicht im Raum. Die Eltern wollten lediglich wissen, welche Feststellungen der Gutachter seinerzeit gemacht hat. Daneben haben wir eine Neuberechnung der Verwaltungsgebühr empfohlen, weil die Festsetzung der Höchstgebühr nicht nachvollziehbar war und prohibitiv wirkte[256].

Die Urheberrechtsklausel des § 13 Abs. 5 IFG betrifft nur die Verwertung erlangter Informationen, nicht jedoch den eigentlichen Informationszugang. Entgegenstehende Urheberrechte sind von der Behörde zu prüfen, bevor die Einwilligung der Berechtigten eingeholt wird.

[256] hierzu bereits JB 2000, 3.5

13.2.3 Verkehrsvertrag mit der S-Bahn

Ein Petent wollte wissen, mit welcher Hilfe Rollstuhlfahrer rechnen können, wenn sie bei der S-Bahn aufgrund von Betriebsstörungen (z. B. defekte Aufzüge) oder Bauarbeiten (nicht nutzbarer Schienenersatzverkehr) auf der Strecke bleiben. Hierzu wandte er sich an die Senatsverwaltung für Stadtentwicklung, die unter Hinweis auf den Verkehrsvertrag mit der S-Bahn Berlin GmbH mitteilte, dass hiernach eine Verpflichtung bestünde, bei der Einrichtung von Ersatzverkehr die Belange behinderter Menschen zu berücksichtigen. Da sich diese Auskunft nicht mit der Antwort des Senats auf eine Kleine Anfrage einer Abgeordneten[257] deckte, nach der die S-Bahn Berlin GmbH erklärt habe, dass „auf Anforderung durch den Kunden ein Taxidienst angeboten würde", beantragte der Petent die Einsicht in den Verkehrsvertrag, soweit Belange von Rollstuhlfahrern betroffen sind. Die Senatsverwaltung hat den Antrag zurückgewiesen, da der Verkehrsvertrag Betriebs- und Geschäftsgeheimnisse enthalte und die S-Bahn einer Einsichtnahme nicht zugestimmt habe.

Wir haben den Petenten in seiner Auffassung unterstützt, dass der Verkehrsvertrag nicht in Gänze als schützenswertes Betriebs- und Geschäftsgeheimnis anzusehen ist. Zwar hat die Senatsverwaltung für Stadtentwicklung zur Begründung ihrer Auffassung die in der Rechtsprechung gängige Definition von Betriebs-/Geschäftsgeheimnissen herangezogen[258]. Allerdings hat sie nicht berücksichtigt, dass dies nicht pauschal auf alle Vertragsregelungen zutreffen muss, sondern bei einzelnen Regelungen (z. B. zugunsten von Rollstuhlfahrern) möglicherweise nicht der Fall ist. Unsere Erfahrungen haben gezeigt, dass die Frage, was im konkreten Fall als Betriebs-/Geschäftsgeheimnis anzusehen ist, häufig sehr schwierig zu beantworten ist. Um einen sich abzeichnenden langwierigen Rechtsstreit zu verhindern, haben wir nach Absprache mit dem Petenten angeboten, durch eine eigene Einsicht des Verkehrsvertrages zu prüfen, ob die (vom Petenten auf unsere Bitte konkretisierten) Fragestellungen dort überhaupt beantwortet werden. Unsere Prüfung vor Ort hat ergeben, dass dies ganz überwiegend nicht der Fall war. Andererseits konnten wir die Senatsverwaltung davon überzeugen, dass zwei Vertragsanlagen zur Abgeltung des Schienenersatzverkehrs mit Bussen sowie zur Ermittlung der Kundenzufriedenheit keine Betriebs-/Geschäftsgeheimnisse darstellen und dem Petenten zumindest auszugsweise zu überlassen sind.

---

[257] Abgh.-Drs. 16/10 411

[258] vgl. 13.1, JB 2003, 4.9.3

Verträge mit dem Land Berlin sind nicht in Gänze als schützenswertes Betriebs-/Geschäftsgeheimnis anzusehen. Gegebenenfalls muss ein beschränkter Informationszugang nach § 12 IFG gewährt werden.

13.2.4 Die Bauakte im Bezirksamt Steglitz-Zehlendorf

Der Petent beantragte beim Bezirksamt Steglitz-Zehlendorf die Einsicht in eine bestimmte Bauakte, um die historische Entwicklung des Grundstücks in Bezug auf seine Größe nachvollziehen zu können. Er hatte Interesse an den Unterlagen von 1910 bis 1980, jedoch nicht an personenbezogenen Daten. Gleichwohl forderte das Amt den Petenten auf, sein Einsichtsinteresse näher darzulegen.

Das Privatinteresse nach § 6 Abs. 1 IFG[259] ist nicht zu ermitteln, wenn eine Offenbarung von personenbezogenen Daten nicht in Betracht kommt. Hierauf haben wir das Bezirksamt hingewiesen. In unserer Funktion als Schiedsstelle[260] haben wir ein zweistufiges Verfahren vorgeschlagen, weil wir dem Bezirksamt eine Überprüfung von ca. 360 Seiten auf Personenbezug und eine entsprechende Schwärzung dieser Daten einerseits und dem Bürger Kopierkosten andererseits ersparen wollten. So wurde in unserem Beisein dem Petenten zunächst Akten*auskunft* gewährt. Soweit sich hierbei ergab, dass bestimmte Unterlagen für ihn besonders interessant waren, wurden sie für eine spätere Akten*einsicht* (Herausgabe als Kopie) vorgemerkt. Dies betraf letztlich ca. 60 Seiten, die von uns in einem Protokoll festgehalten wurden, welches wir in Kopie dem Bezirksamt und dem Petenten überlassen haben.

Ein zweistufiges Vorgehen (zunächst Akten*auskunft*, dann beschränkte Akten*einsicht*) kann einvernehmlich dann sinnvoll sein, wenn es für die Beteiligten effektiver ist, als sämtliche Unterlagen vor der eigentlich beantragten Akteneinsicht auf einschränkende Tatbestände nach § 5 ff. IFG zu prüfen.

13.2.5 Bauvorhaben im Bezirk Reinickendorf

Ein Bürger begehrte über seinen Rechtsanwalt Einsicht in die Verwaltungsvorgänge zur Planung und Baudurchführung eines Bauvorhabens in

[259] hierzu JB 2001, 4.9 (Problemfelder)
[260] § 18 IFG

Frohnau mit Ausnahme der Ausschreibungs- und Vergabeunterlagen. Das Bezirksamt Reinickendorf fragte daraufhin zurück, worin das Allgemeininteresse bestehe. Nach der Begründung des Gesetzes sei die Verfolgung von Individualinteressen nicht erfasst.

Wir haben das Bezirksamt darauf hingewiesen, dass ein etwaiges Privatinteresse nach ständiger Rechtsprechung der Berliner Verwaltungsgerichte als Bestandteil des Informationsinteresses nach § 1 IFG anzusehen ist. Beispielhaft haben wir auf eine Entscheidung des Verwaltungsgerichts Berlin von 2004[261] hingewiesen, die gegen dasselbe Bezirksamt in Zusammenhang mit einer begehrten Akteneinsicht in Bauakten eines anderen Bauvorhabens ergangen ist. Die begehrte Akteneinsicht wurde daraufhin gewährt.

Nach ständiger Rechtsprechung ist weder der Nachweis eines berechtigten Interesses noch die Angabe des Verwendungszwecks für die begehrten Informationen erforderlich. Das Privatinteresse an ihnen ist jedenfalls Bestandteil des Informationsinteresses nach § 1 IFG.

13.2.6 Bauvorhaben im Bezirk Mitte

Der Petent war als Ingenieur an einem Bauvorhaben beteiligt, das die Instandsetzung, Modernisierung und den Einbau eines Aufzuges beinhaltete. Der Bauherr beendete die Tätigkeit des Petenten vor Erfüllung des Auftrags und ließ diesen von einem anderen Architekten ausführen. Der Petent beantragte Akteneinsicht. Er wollte prüfen, ob die von ihm gefertigten Entwürfe unter Verstoß gegen Urheberrechte weiterverwendet wurden. Das Bauamt gewährte unter Hinweis auf einen privatrechtlichen Streit zwischen dem Petenten und dem Bauherrn keine vollständige Akteneinsicht, sondern legte im Termin nur einzelne Bauzeichnungen vor. Hierfür wurde unter Hinweis auf die Tarifstelle 1004 der Verwaltungsgebührenordnung eine Gebühr von 71 Euro berechnet.

Wir haben das Bezirksamt auf eine Entscheidung des Verwaltungsgerichts Berlin[262] hingewiesen und um Beachtung der dortigen Grundsätze gebeten. Darin war in einem vergleichbaren Fall, in dem es um eine möglicherweise urheberrechtswidrige Weiterverwendung von Planungsentwürfen ging, entschieden worden, dass die Akteneinsicht in die Bauakten des Bauvorhabens zu gewähren ist, soweit sie keine

[261] VG 23 A 1.04
[262] VG 23 A 1.04

personenbezogenen Daten enthalten. Darüber hinaus haben wir darauf hingewiesen, dass die teilweise Ablehnung der begehrten Akteneinsicht einen belastenden Verwaltungsakt darstellt, der mit den im Verwaltungsrecht üblichen Rechtsbehelfen angreifbar sein muss. Die Einzelheiten der Gebührenberechnung waren dem Bescheid nicht zu entnehmen. Hierzu wurde uns mitgeteilt, dass eine „ersatzweise" Ermittlung anhand der bautechnischen Prüfungsverordnung vorgenommen wurde, weil sie aktueller sei als die von der Senatsverwaltung für Finanzen für Amtshandlungen nach dem IFG festgesetzten Stundensätze. Dies war unzulässig. Durch unsere Intervention wurde die Gebühr um mehr als die Hälfte herabgesetzt. Auf die nachträgliche schriftliche Bescheidung hat der Petent verzichtet.

Bei nur teilweiser Gewährung des Informationszugangs besteht ein Anspruch auf einen „rechtsmittelfähigen" Bescheid, der auch nachträglich erteilt werden kann. Wird Informationszugang nach IFG gewährt, sind bei der Gebührenfestsetzung allein die hierfür maßgeblichen Stundensätze heranzuziehen.

13.2.7 Mieterverzeichnis von sanierungsbedürftigen Wohnungen im Bezirk Friedrichshain-Kreuzberg

Der Petent hat als Mitglied einer Mieterinitiative beim Bezirksamt Friedrichshain-Kreuzberg die Herausgabe einer Kopie des Mieterverzeichnisses verlangt, aus dem sich ergibt, welche (60 von insgesamt 140) Wohnungen durch die Hausverwaltung zu sanieren sind. Die Hausverwaltung war zur Sanierung dieser Wohnungsanzahl nach einem Rechtsstreit mit dem Bezirksamt rechtskräftig verurteilt worden. Das Bezirksamt hat die Herausgabe des Mieterverzeichnisses aus Datenschutzgründen abgelehnt, nachdem das Rechtsamt einen Rechtsanwalt mit der Prüfung dieser Frage betraut hatte.

Nach den in § 6 Abs. 2 IFG genannten Regelbeispielen dürfen grundsätzlich bestimmte personenbezogene „Kerndaten" beim Informationszugang offenbart werden. Der Gesetzgeber hat hier eine eigene Abwägung zwischen dem Informationsinteresse und den Datenschutzbelangen Dritter getroffen. Die Herausgabe des Mieterverzeichnisses haben wir als von § 6 Abs. 2 Satz 1 Nr. 1 Buchst. d) IFG gedeckt angesehen. Im Gegensatz zu Buchstaben a) bis c)[263] darf hier mehr als die bloße Tatsache der Mietereigenschaft offenbart werden. Denn dieses Regelbeispiel würde keinen Sinn machen, wenn nur diese Tatsache ohne Zusatzinformation offengelegt werden dürfte. Diese lag hier darin, dass die Mietparteien eine Wohnung

[263] JB 2006, 11.3.6

mit Sanierungsbedarf haben[264]. Dass das Rechtsamt einen Rechtsanwalt beauftragt hat, statt uns zu kontaktieren, haben wir angesichts der Tatsache, dass der Gesetzgeber uns eigens mit der Klärung derartiger Fragestellungen beauftragt hat, mit Befremden zur Kenntnis genommen. Mit unserer Hilfe hat der Petent die Informationen schnell erhalten.

Nach § 6 Abs. 2 IFG dürfen nur die dort genannten personenbezogenen „Kerndaten" offenbart werden. Bei den Regelbeispielen a) bis c) darf zusätzlich die *Tatsache* der Verfahrensbeteiligung bzw. der rechtlichen Stellung der Betroffenen offenbart werden, bei den Regelbeispielen d) und e) darüber hinaus eine Zusatzinformation.

13.2.8 Zwischenbericht zur Evaluation des Pilotprojekts zur Videoüberwachung bei der BVG

Die Bürgerrechtsorganisation Humanistische Union hat bei der BVG die Herausgabe einer Kopie des Zwischenberichts des evaluierenden Instituts über das von der BVG abgebrochene Pilotprojekt zur Videoüberwachung beantragt. Der Antrag wurde unter Hinweis auf den zu schützenden Prozess der Willensbildung nach § 10 Abs. 4 IFG und – „wegen der Thematik des Berichts" – auf Betriebs-/ Geschäftsgeheimnisse nach § 7 IFG zurückgewiesen, ohne dies näher zu begründen.

Wir haben die BVG darauf hingewiesen, dass der Willensbildungsprozess nach seinem Abschluss nicht mehr schützenswert ist und dem Informationszugang unterliegt[265], da die BVG die flächendeckende Einführung der Videoüberwachung auf U-Bahnhöfen in Form von 24-Stunden-Aufzeichnung bereits beschlossen hatte. Auch wenn dies noch nicht der Fall gewesen wäre, wäre der Bericht entsprechend § 10 Abs. 1 Satz 3 IFG zu offenbaren. Danach sind „Ergebnisse von Beweiserhebungen" – auch wenn sie Teil eines noch nicht beendeten Verfahrens wären – nicht schutzbedürftig und damit zugänglich zu machen. Die Berufung auf Betriebs-/Geschäftsgeheimnisse, die „wegen der Thematik des Berichts" betroffen seien, griff zu kurz. Ein Bescheid, der keine Aussagen hierzu trifft, ist per se rechtswidrig. Jedenfalls muss die Abwägungsklausel des § 7 Satz 1 IFG, die im Bescheid ebenfalls nicht berücksichtigt wurde, bei einem vorhandenen Informationsinteresse der Öffentlichkeit zu einer Offenbarungspflicht führen, wenn ein wirtschaftlicher Schaden hierdurch nicht entstehen kann. Dass dies der Fall sein könnte, wurde

[264] Entsprechendes dürfte auch für Buchst. e) gelten.

[265] JB 2000, 3.5 (Einschränkungen)

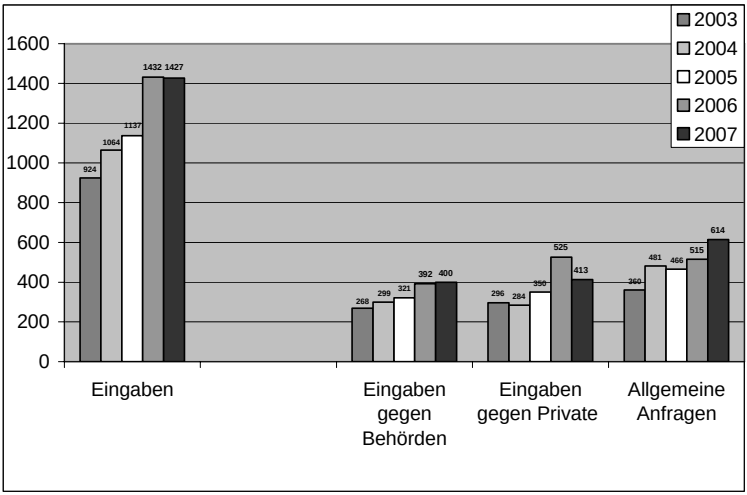
nicht vorgetragen. Letztlich hat die Petentin eine (sogar ungeschwärzte) Kopie des Zwischenberichts erhalten.

(Zwischen-)Berichte zur Evaluation eines in der Öffentlichkeit massiv diskutierten Projektes unterliegen dem uneingeschränkten Informationszugang.

14 Aus der Dienststelle

14.1 Entwicklungen

In unverändert starkem Maße haben sich im zurückliegenden Jahr Bürgerinnen und Bürger mit Eingaben an uns gewandt. Die entsprechenden Zahlen zeigen eine Stabilisierung auf hohem Niveau. Dabei sind in die Übersicht die weit über hundert Eingaben nicht eingeflossen, die den Berliner Beauftragten für Datenschutz und Informationsfreiheit Ende 2007 aus Anlass der Änderung der Allgemeinen Geschäftsbedingungen bei dem sozialen Netzwerk studiVZ erreichten. Insgesamt zeigen die Berlinerinnen und Berliner eine Hohe Sensibilität für Fragen des Datenschutzes, wozu möglicherweise auch der „Überbietungswettbewerb“ beigetragen haben mag, den Politikerinnen und Politiker im vergangenen Jahr mit Vorschlägen für immer neue Befugnisse der Sicherheitsbehörden ausgetragen haben[266].



Entwicklung der Anzahl der Eingaben (schriftlich und elektronisch) beim Berliner Beauftragten für Datenschutz und Informationsfreiheit

[266] so der Richter am Bundesverfassungsgericht Di Fabio, vgl. Einleitung

14.2

Wir sind bestrebt, den Beschwerden von Bürgerinnen und Bürgern weiterhin so zeitnah wie möglich nachzugehen, auch wenn wir dabei zuweilen an die Grenzen unserer Kapazitäten als kleinste oberste Landesbehörde geraten. Unser Ziel bleibt es, mit den Ressourcen und Befugnissen, die uns zur Verfügung stehen, eine möglichst große Wirkung zu erzeugen.

Die datenschutzrechtliche Problematik weltweit im Internet agierender Suchmaschinen[267] verschärft sich zunehmend. Wir haben uns deshalb dazu entschlossen, in unserem Geschäftsverteilungsplan[268] nur noch den Berliner Beauftragten für Datenschutz und Informationsfreiheit, seine beiden Vertreter und die Pressesprecherin namentlich zu nennen. Die Aufgabengebiete und Telefonnummern aller übrigen Mitarbeiterinnen und Mitarbeiter werden weiterhin veröffentlicht, um den Bürgerinnen und Bürgern eine direkte Kontaktaufnahme zu ermöglichen.

14.2 Zusammenarbeit mit dem Abgeordnetenhaus

Im vergangenen Jahr hat der Unterausschuss „Datenschutz und Informationsfreiheit“ des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses die Beratung der Stellungnahme des Senats zum Jahresbericht 2005 abgeschlossen und gleichzeitig zahlreiche aktuelle Fragen des Datenschutzes und der Informationsfreiheit erörtert. Diese Fragen werden in aller Regel parteiübergreifend einheitlich beurteilt, was sich in der konstruktiven Zusammenarbeit im Unterausschuss widergespiegelt hat. Mehrfach sind Empfehlungen des Berliner Beauftragten für Datenschutz und Informationsfreiheit vom Unterausschuss aufgegriffen worden, den Senat zu Verbesserungen in diesen Bereichen aufzufordern. Das Abgeordnetenhaus hat die vom Unterausschuss zum Jahresbericht 2005 gegebenen Beschlussempfehlungen in der Sitzung am 19. September 2007[269] beschlossen.

14.3 Zusammenarbeit mit anderen Stellen

Datenschutzbeauftragte erscheinen in der Öffentlichkeit – entsprechend ihrer Amtsbezeichnung – häufig als „Einzelkämpfer“. In Wirklichkeit stimmen sie sich eng untereinander ab, sowohl auf nationaler sowie auf internationaler Ebene. Täten sie dies nicht, gäbe es kein einheitliches Datenschutzniveau. Eine uneinheitliche

[267] vgl. dazu 12.2.2
[268] vgl. Anlage 3
[269] vgl. Anlage 1

Aufsichts- und Prüfpraxis kann aber weder im Interesse der Bürgerinnen und Bürger noch der Daten verarbeitenden Stellen sein. Die *Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, in der die Datenschutzbeauftragten Fragen der Datenschutzkontrolle im öffentlichen Bereich erörtern, tagte im Berichtsjahr unter dem Vorsitz des Thüringer Landesbeauftragten für den Datenschutz am 8./9. März 2007 in Erfurt und am 25./26. Oktober 2007 in Saalfeld. Dabei und auch zwischen den Konferenzen wurden insgesamt 10 Entschließungen gefasst, die vor allem aktuelle Fragen des Datenschutzes betreffen, auch soweit sie nicht im Mittelpunkt der öffentlichen Diskussion stehen[270]. Für 2008 hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit turnusgemäß den Konferenzvorsitz übernommen.

Die Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich tagten 2007 im *„Düsseldorfer Kreis“* unter dem Vorsitz des Hamburgischen Datenschutzbeauftragten am 19./20. April 2007 und am 8./9. November 2007 in der Freien und Hansestadt Hamburg. Auch der Düsseldorfer Kreis ist erfreulicherweise dazu übergegangen, seine Beschlüsse öffentlich bekannt zu machen. Im zurückliegenden Jahr hat er acht Beschlüsse gefasst, die vor allem Fragen des Versand- und Adresshandels, des Kredit-Scoorings und des internationalen Datenverkehrs betrafen[271].

Fragen der Informationsfreiheit werden in Deutschland bei der *Konferenz der Informationsfreiheitsbeauftragten* diskutiert, die im vergangenen Jahr unter dem Vorsitz des Leiters des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein und des Landesbeauftragten für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen tagte. Sie hat am 11. Juni 2007 eine Entschließung zur Stärkung der Informationsfreiheit bei Betriebs- und Geschäftsgeheimnissen gefasst[272]. Im ersten Halbjahr 2008 wird der Landesbeauftragte für Datenschutz und Informationsfreiheit des Saarlandes den Vorsitz in der Konferenz der Informationsfreiheitsbeauftragten übernehmen.

In der *Arbeitsgruppe nach Art. 29 der Europäischen Datenschutzrichtlinie* vertritt der Berliner Beauftragte für Datenschutz und Informationsfreiheit seit jeher die Bundesländer auf europäischer Ebene. Diese Arbeitgruppe beschloss zahlreiche Stellungnahmen zu den Fragen des Datenschutzes, die im vergangenen Jahr im

[270] vgl. Dokumentenband 2007, S. 9 ff.
[271] vgl. a. a. O., S. 24 ff.
[272] vgl. a. a. O., S. 107

Zentrum des Interesses standen, wie die Übermittlung von Fluggastdatensätzen in die USA[273].

Bei der *29. Internationalen Konferenz der Datenschutzbeauftragten* vom 26.-28. September 2007 in Montreal wurden drei Resolutionen beschlossen, die die internationale Standardisierung des Datenschutzes, aber auch die Intensivierung der internationalen Datenschutzbehörden betreffen[274].

Unter dem Vorsitz des Berliner Beauftragten für Datenschutz und Informationsfreiheit tagte die *Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group“* am 12./13. April 2007 in St. Peter Port (Guernsey) und am 4./5. September 2007 im Anschluss an das Internationale Symposium im Rahmen der Funkausstellung in Berlin[275]. Die Arbeitsgruppe verabschiedete dabei Arbeitspapiere zu Fragen der Telekommunikation im grenzüberschreitenden Telemarketing, beim e-Ticketing in öffentlichen Verkehrsmitteln und bei der Verbreitung digitaler Medieninhalte sowie beim digitalen Fernsehen[276].

Vom 26.-29. November 2007 fand die *Internationale Konferenz der Informationsfreiheitsbeauftragten* unter dem Vorsitz des neuseeländischen Ombudsmann in Wellington statt.

Im Zeitraum Oktober 2007 bis März 2008 waren im Rahmen des von der Europäischen Union geförderten Leonardo da Vinci-Programms fünf Mitarbeiterinnen und Mitarbeiter der polnischen Datenschutzbehörde für jeweils eine Woche in der Dienststelle des Berliner Beauftragten für Datenschutz und Informationsfreiheit zu Gast, um sich über die Arbeitsweise unserer Dienststelle zu informieren und eigene Erfahrungen einzubringen.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat bei einer Anhörung im Rechts- und Verfassungsausschuss des Landtages Sachsen-Anhalt Stellung zu Entwürfen für ein Landesinformationsfreiheitsgesetz genommen.

---

[273] vgl. a.a.O., S. 68. Die übrigen Stellungnahmen sind online abrufbar unter http://www.ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_de.htm

[274] vgl. a. a. O., S. 90 ff.

[275] vgl. 12.4

[276] vgl. Dokumentenband 2007, S. 98 ff.

14.4 Öffentlichkeitsarbeit

Im zurückliegenden Jahr wurde erstmals der vom Europarat initiierte Europäische Datenschutztag am 29. Januar begangen. Anlass hierfür war der Jahrestag der Unterzeichung der Datenschutzkonvention des Europarats am 28. Januar 1981. Hierzu hatte der Vorsitzende der Datenschutzkonferenz, der Landesbeauftragte für den Datenschutz Sachsen-Anhalt Dr. von Bose, zu einer Podiumsdiskussion eingeladen, an der der Bundesminister des Innern Dr. Schäuble, die Richterin am Bundesverfassungsgericht Dr. Hohmann-Dennhardt, der frühere Hessische Datenschutzbeauftragte Prof. Dr. Simitis, der Abgeordnete des Europäischen Parlaments Alvaro und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Schaar teilnahmen. Das Interesse an dieser Veranstaltung war groß, zumal es sich dabei um die zentrale Veranstaltung zum Europäischen Datenschutztag in Deutschland handelte.

Gegen Ende des Berichtszeitraumes wurden die Vorbereitungen für den 2. Europäischen Datenschutztag am 28. Januar 2008 getroffen. Gemeinsam mit dem Bundesbeauftragten für Datenschutz und Informationsfreiheit planten wir in der Robert-Jungk-Oberschule eine Veranstaltung zum Thema „Datenschutz 2.0 – Web 2.0“, zu der alle Berliner Schülerinnen und Schüler einer bestimmten Klassenstufe eingeladen werden sollten. Erfreulicherweise hat die Senatsverwaltung für Bildung, Wissenschaft und Forschung die Teilnahme der Jugendlichen befürwortet. Wir hätten uns aber gewünscht, zur Versendung unserer Einladungen ihren elektronischen E-Mail-Verteiler nutzen zu dürfen. Dies wurde mit der Begründung abgelehnt, unsere Veranstaltung würde zu Unterrichtsausfall führen.

Daneben haben wir uns im Berichtszeitraum erneut an mehreren öffentlichen Veranstaltungen beteiligt:

- Tag der offenen Tür des Abgeordnetenhauses am 23. Juni 2007
- 36. Tag der offenen Tür der Berliner Polizei am 9. September 2007
- Jugendverbraucherschutztag im Freizeit- und Erholungszentrum Wuhlheide am 10. Oktober 2007

14.4

Das Interesse, auf das wir bei diesen Veranstaltungen gestoßen sind, ermutigt uns dazu, unsere öffentliche Präsenz auch in Zusammenarbeit mit anderen Institutionen soweit möglich zu verstärken.

Berlin, 2. April 2008

Dr. Alexander Dix
Berliner Beauftragter für Datenschutz und Informationsfreiheit

Beschlüsse des Abgeordnetenhauses vom 13. September 2007

Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2005

Zu: **Datenschutzfreundliche Änderungen beim Neugeborenen-Screening?**
(4.5.1, Drs S. 108 ff.)

Der Senat wird aufgefordert, darauf hinzuwirken, dass in allen Berliner Geburtseinrichtungen korrekte Einwilligungen sowohl für das kombinierte Neugeborenen-Stoffwechsel- und Hörscreening als auch für die Adressnutzung bei auffälligen oder fehlenden Befunden eingeholt werden.

Zu: **Das automatisierte Abrufverfahren für die BVG**
(4.2.1, Drs. S. 77 ff.)

Der Senat wird aufgefordert, darauf hinzuwirken, dass die BVG beim automatisierten Meldedaten-Abrufverfahren zur Identitätsprüfung von Schwarzfahrenden geeignete organisatorische Maßnahmen zur Verbesserung des Datenschutzes trifft. Hierzu gehören insbesondere ein wirksames Qualitätsmanagement und regelmäßige Stichprobenkontrollen der Meldedatenabrufe. Die Anfragen des Berliner Beauftragten für Datenschutz und Informationsfreiheit sind zeitnah zu beantworten.

Zu: **Hartz IV und kein Ende**
(3.2, Drs. S. 33 ff.)

Der Senat wird aufgefordert, darauf hinzuwirken, dass die verantwortlichen Stellen (JobCenter, Bezirksämter) bei der Bearbeitung von Sozialleistungsanträgen die „Gemeinsamen Hinweise zur datenschutzgerechten Ausgestaltung der Anforderung von Kontoauszügen“ vollständig beachten, die die Datenschutzbeauftragten der Länder Berlin, Brandenburg, Hamburg, Mecklenburg-Vorpommern und Schleswig-Holstein erarbeitet haben.

Anlage 1

Rede des Berliner Beauftragten für Datenschutz und Informationsfreiheit am 13. September 2007 im Abgeordnetenhaus von Berlin zur Beschlussfassung über den Jahresbericht 2005

Herr Präsident,
sehr geehrte Damen und Herren,

erfreulicherweise können Sie heute über den Jahresbericht 2005 des Berliner Beauftragten für Datenschutz und Informationsfreiheit abschließend beraten. Erfreulich ist dies deshalb, weil der Ausschuss für Inneres, Sicherheit und Ordnung zu dem Berichtszeitraum 2005 eine Beschlussempfehlung geben konnte, obwohl sich das Abgeordnetenhaus und seine Ausschüsse erst im vergangenen Herbst neu konstituiert haben. Möglich gemacht hat dies die konzentrierte und konstruktive Behandlung des Berichts und der Stellungnahme des Senats hierzu im Unterausschuss „Datenschutz und Informationsfreiheit". Dafür danke ich vor allem den Mitgliedern des Unterausschusses herzlich.

Die Ihnen vorliegenden Empfehlungen betreffen zum einen die datenschutzgerechte Gestaltung des **Stoffwechsel- und Hörscreenings bei Neugeborenen**, zum anderen die gesetzeskonforme **Anforderung von Kontoauszügen durch die Jobcenter**, zu der die Datenschutzbeauftragten in Berlin, Brandenburg, Hamburg, Mecklenburg-Vorpommern und Schleswig-Holstein gemeinsame Hinweise gegeben haben.

Schließlich soll der Senat auch in einem dritten Bereich aufgefordert werden, darauf hinzuwirken, dass die datenschutzgerechten Mindeststandards eingehalten werden: bei den Berliner Verkehrsbetrieben. Für **Abruf von Meldedaten** bei der Kontrolle von Schwarzfahrenden hat sich die BVG bisher nicht in der Lage gesehen, das nötige Qualitätsmanagement einzuführen, um die Rechtmäßigkeit des jeweiligen Abrufs überprüfen zu können. Statt den Datenschutz als lästige Mehrarbeit zu behandeln, sollten die Berliner Verkehrsbetriebe ihn in allen Bereichen als Qualitätsmerkmal ihrer Dienstleistungen begreifen, so wie dies etwa im Bereich des **electronic ticketing** bereits geschieht.

Lassen Sie mich in diesem Zusammenhang auch etwas zu dem umstrittenen Thema **Videoüberwachung im öffentlichen Personennahverkehr** sagen. Mit dem heute in erster Lesung behandelten Gesetzentwurf des Senats zur Änderung des Polizeirechts und des Datenschutzrechts sollen hierfür neue Rechtsgrundlagen geschaffen werden. Ohne den Ausschussberatungen hierzu vorgreifen zu wollen, möchte ich

eines unterstreichen: der künftige Rechtsrahmen für die Videoüberwachung in öffentlichen Verkehrsunternehmen sollte möglichst einheitlich gestaltet werden und sich an dem Konzept orientieren, das die Deutsche Bahn zusammen mit der Bundespolizei mit unserer Zustimmung als Aufsichtsbehörde seit Jahren praktiziert. Die Fahrgäste würden es nicht verstehen, wenn z.B. im U-Bahnhof Stadtmitte nach anderen Regeln und extensiver videographiert wird als im Berliner Hauptbahnhof. Noch wichtiger ist aber die Erkenntnis, dass Kameras keine Menschen ersetzen können, auch wenn sie weniger Geld kosten. Es nützt dem Fahrgast als Opfer einer Straftat wenig, wenn er weiß, dass der Täter bald gefasst wird. Die präventive Wirkung von Videoüberwachung wird, das zeigen alle vorhandenen Untersuchungen, bei schweren Straftaten allgemein überschätzt. Deshalb macht Videoüberwachung nur Sinn als Teil eines Sicherheitskonzepts, das ein schnelles Eingreifen in Gefahrensituationen bindend vorschreibt. Ich werde mich für eine solche Regelung einsetzen.

In der gegenwärtigen Debatte über neue Sicherheitsgesetze deuten manche Vorschläge etwa zur **heimlichen Online-Durchsuchung** von PCs im Vorfeld jedes Verdachts und jeder konkreten Gefahr darauf hin, dass grundlegende rechtsstaatliche Prinzipien in Frage gestellt werden. Allein der öffentlich geäußerte Gedanke, man könne Schadsoftware als Anhang für elektronische Mitteilungen von Behörden auf privaten Rechnern platzieren, konterkariert die vielfältigen Bemühungen für ein **vertrauenswürdiges E-Government**, die auch in Berlin seit Jahren unternommen werden. Es ist zudem ein Irrtum zu glauben, man könne eine so einschneidende Maßnahme zielgerichtet auf mutmaßliche Terroristen beschränken. Auch ist der Kernbereich der privaten Lebensgestaltung Unbeteiligter nicht wirksam vor dem Zugriff des Staates zu schützen, wenn man diese Büchse der Pandora öffnet. Das Vertrauen der Wirtschaft und der Bevölkerung in die Sicherheit der Informationstechnik droht deshalb grundlegend erschüttert zu werden, falls der Staat Hackermethoden legalisiert.

Ich hoffe, meine Damen und Herren, dass der Senat von Berlin bei den demnächst anstehenden Beratungen im Bundesrat seinen Einfluss dafür geltend machen wird, dass in der Bundesgesetzgebung zur inneren Sicherheit nicht jedes Maß verloren geht. Diese Gefahr besteht und sie darf auch angesichts der terroristischen Bedrohung nicht in Kauf genommen werden.

Vielen Dank für Ihre Aufmerksamkeit.

Auszug aus dem Geschäftsverteilungsplan

Stand: 31. Dezember 2007

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

Dr. Alexander Dix **App. 202**	**Berliner Beauftragter für Datenschutz und Informationsfreiheit**
Dipl.-Informatiker **Hanns-Wilhelm Heibey** **App. 400**	Vertreter
Anja-Maria Gardain **App. 204**	Pressesprecherin
App. 200	Sekretariat, PRIvacy MAgazine, Veranstaltungen, Dienstreisen für den Zentralen Bereich
	Zentraler Bereich
Dr. Alexander Dix **App. 202**	Bereichsleiter
	Zentrale Aufgaben
App. 204	AG: Internationaler und europäischer Datenschutz, Abgeordnetenhaus, Bezirksverordnetenversammlungen, Informationsfreiheit

Anlage 3

App. 211	AG: Telekommunikation, Tele- und Mediendienste, Presse und Runkfunk
App. 213	Redaktion von Veröffentlichungen, Bibliothek, Rechtsprechungssammlung, Intranet, Referendare, Konferenzvorbereitungen
App. 310	Besondere Aufgaben, Veranstaltungen
	Allgemeine Verwaltung
Dipl.-Informatiker Hanns-Wilhelm Heibey App. 400	Ständiger Vertreter des Bereichsleiters für die Allgemeine Verwaltung
App. 230	Beauftragte für den Haushalt, Haushaltsplanung und -bewirtschaftung, Personalangelegenheiten, Büroorganisation, Ausbilderin
App. 232	Sekretariat Allgemeine Verwaltung, Rechnungsstelle
	Bereich Recht
Dr. Thomas Petri App. 300	Bereichsleiter, Vertreter des BlnBDI für den Bereich AG: Senatskanzlei, Rechnungshof, Justiz, Grundsatzangelegenheiten des Datenschutzrechts sowie des Sicherheits- und Ordnungsrechts, Parteien, Nachrichtendienste, Integration (Ausländerrecht)
App. 302	Sekretariat

	BürgerOffice
App. 111	Leitung; Öffentlichkeitsarbeit
	AG: Finanzen, Schule, Sport
App. 112	AG: Inneres, Bezirksämter
App. 100	Archiv des Bereichs Recht, Schreibarbeiten
App. 102	Geschäftsstelle BürgerOffice, Ausgangspost, Broschürenversand, Schreibarbeiten
App. 104	Geschäftsstelle BürgerOffice, Eingangspost, Schreibarbeiten
	Recht
App. 305	AG: Wissenschaft, Forschung und Statistik
App. 315	AG: Arbeit und Soziales, Jugend
App. 309	AG: Wirtschaft, Zivilrecht, Verbraucherschutz
App. 311	AG: Arbeitnehmerdatenschutz, Wirtschaft, Personaldaten
App. 304	AG: Stadtentwicklung, Kultur, Umwelt, Presserecht, Rundfunkgebühren
App. 212	Stellvertretender Pressesprecher
	AG: Gesundheit, eGovernment

	Bereich Informatik
Dipl.-Informatiker Hanns-Wilhelm Heibey App. 400	Bereichsleiter, Vertreter des BlnBDI als Dienststellenleiter und für den Bereich **Q:** Recht und Politik der Informationstechnik (u. a. DV im Auftrag), Landesübergreifende Infrastrukturprojekte außer Netze, Elektronische Zahlungssysteme, Organisation von Rechenzentren, Proprietäre Betriebssysteme, Kryptografie, Chipkarten, Koordination bei komplexen Beratungs- und Kontrollprojekten
App. 402	Sekretariat
App. 408	**Q:** Berliner Landesnetz, Telekommunikationssysteme **R:** Inneres (außer Standesämter), Wissenschaft und Forschung **I:** Systemkoordination
App. 405	**Q:** Beratung der behördlichen und betrieblichen Datenschutzbeauftragten, Koordination der Kontrollen im privaten Bereich, Organisation des Datenschutzes, Unterrichtungspflicht nach § 24 Abs. 3 Satz 3 BlnDSG, Nichtautomatisierte Datenverarbeitung **R:** Verfassungsorgane, Senatskanzlei, Stadtentwicklung, Justiz, Betriebe, Finanzen, Wirtschaft **I:** Behördlicher Datenschutzbeauftragter
App. 404	AG: Datenschutz und IT-Sicherheit im Internet
App. 406	**Q:** Microsoft-Betriebssysteme, Bürosysteme, Lokale Netze (u. a. kabellos), Mobile Computer **R:** Gesundheit, Verkehr **I:** Informatik-Bibliothek, Virenschutzbeauftragter des Hauses
App. 407	**Q:** UNIX, LINUX, SAP R/3, Firewalls, Wartung und Fernwartung, Personalinformationssysteme **R:** Soziales, Inneres (Standesämter), Arbeit, Jugend

	I: IT-Haushalt
App. 410	**Q:** Biometrie, Überwachungssysteme (z. B. Videoüberwachung), Ubiquitous Technologies (u. a. RFID), Grundsatzfragen **R:** Kultur, Bildung, Schule, Sport
App. 411	Führung des Registers nach §§ 4d, 4e BDSG, Sachbearbeitung, Buchung der Dienstreisen im Bereich Informatik und Recht, Jahresbericht
App. 409	**I:** Systemverwaltung und Benutzerbetreuung, Anwendungsprogrammierung, Webmaster, TK-Anlage

Agenda:
AG = Arbeitsgebiet
Q = Querschnittszuständigkeit
R = Ressortzuständigkeit
I = Interne Aufgaben

Anlage 3

Stichwortverzeichnis