Abgeordnetenhaus BERLIN

Drucksache 15/ 1757

15. Wahlperiode

Vorlage – zur Kenntnisnahme –

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

Der Senat legt nachstehende Vorlage dem Abgeordnetenhaus zur Besprechung vor:

Gem. § 29 Abs. 2 Berliner Datenschutzgesetz sowie § 18 Abs. 3 Berliner Informationsfreiheitsgesetz erstattet der Beauftragte für Datenschutz und Informationsfreiheit dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich einen Bericht über das Ergebnis seiner Tätigkeit. Der Regierende Bürgermeister hat dazu gemäß § 29 Abs. 2 des Berliner Datenschutzgesetzes eine Stellungnahme des Senats herbeizuführen und legt diese hiermit dem Abgeordnetenhaus vor.

Berlin, den 3. Juni 2003

Der Senat von Berlin

Wolf
Bürgermeister

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

Stellungnahme des Senats

zum Bericht des

Berliner Beauftragten für

Datenschutz und

Informationsfreiheit

für 2002

(gemäß § 29 Abs. 2 Berliner Datenschutzgesetz)

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

1. Entwicklung des Datenschutzrechts

1.1 Deutschland und Europa

Das ausgehende Jahr 2001 war aus der Sicht des Datenschutzes geprägt von heftigen Diskussionen darüber, welche gesetzgeberischen Konsequenzen aus den monströsen Terroranschlägen vom 11. September zu ziehen sind. Im Laufe des Gesetzgebungsverfahrens war zwar eine Reihe von Vorschlägen der Datenschutzbeauftragten aufgegriffen worden[1], gleichwohl enthält das am 11. Januar 2002 (trotz der damit verbundenen erheblichen Grundrechtseingriffe rückwirkend) verkündete *Terrorismusbekämpfungsgesetz*[2] deutliche Einschränkungen rechtsstaatlicher Grundsätze:

- Die Tendenz der Gesetzgebung im Sicherheitsbereich, Erhebungsbefugnisse zunehmend vom Vorliegen eines tatsächlichen Anfangsverdachts (Strafverfolgung) oder einer konkreten Gefahrenlage (Gefahrenabwehr) abzukoppeln, stellt Prinzipien in Frage, die seit dem 19. Jahrhundert als grundlegende Elemente des Rechtsstaats gelten.

Der vorliegende Entwurf des Gesetzes zur Änderung des Gesetzes über den Verfassungsschutz Berlin bleibt hinter den neuen Befugnissen des Bundes und der übrigen Länder zurück.

- Gleichzeitig verschwimmen damit die Grenzen zwischen Polizei und Nachrichtendiensten, zumal auf der anderen Seite dem Verfassungsschutz zunehmend exekutive Befugnisse zugeteilt werden - wie etwa neue Erhebungsbefugnisse bei Finanzdienstleistern, Post- und Telekommunikationsanbietern oder Verkehrsunternehmen.

In diesem Änderungsentwurf verschwimmen keine Grenzen zwischen Polizei und Nachrichtendiensten. Durch die in Berlin geplante Gesetzesänderung wird weder die Organisation noch die Aufgabe beider Behördenstrukturen betroffen bzw. vermischt.

- Datensammlungen auf Vorrat werden zunehmend hoffähig, obwohl das Bundesverfassungsgericht derartige Verfahren für verfassungswidrig erklärt hat[3].

Die Berliner Verfassungsschutzbehörde hat nach § 5 Absatz 1 VSG Bln die Aufgabe, den Senat und das Abgeordnetenhaus von Berlin, andere zuständige staatliche Stellen und die Öffentlichkeit über Gefahren für die freiheitlich demokratische Grundordnung, den Bestand und die Sicherheit des Bundes und der Länder zu unterrichten. Dadurch soll es den staatlichen Stellen insbesondere ermöglicht werden, rechtzeitig die erforderlichen Maßnahmen zur Abwehr dieser Gefahren zu ergreifen. Dafür sammelt und wertet die Verfassungsschutzbehörde nach § 5 Absatz 2 VSG Bln Informationen, insbesondere sach- und personenbezogene Daten, Auskünfte, Nachrichten und Unterlagen aus.

Der Berliner Änderungsentwurf sieht weitere Datenerhebungsbefugnisse für die Berliner Verfassungsschutzbehörde vor, jedoch nicht die Schaffung von polizeilichen Eingriffsbefugnissen wie Festnahme, Durchsuchung, Sicherstellung usw.

---

[1] JB 2001, 1.1

[2] Gesetz zur Bekämpfung des internationalen Terrorismus, BGBl. I, S. 361

[3] BVerfGE 65, 1 (47)

- Die Aufnahme biometrischer Daten in Identitätspapiere (die bei Deutschen keinerlei Bezug zur Terrorismusbekämpfung hat) kehrt erneut das Prinzip der Unschuldsvermutung um, indem jede Person als potenziell kriminell eingestuft wird[4].

Die Diskussion über Auswirkungen der Antiterrorgesetze wurde im vergangenen Jahr weltweit geführt[5]. Die Parlamentarische Versammlung der *Organisation für Sicherheit und Zusammenarbeit in Europa*, die im Juli in Berlin tagte, sah sich veranlasst, in ihrer Schlusserklärung zu betonen, dass im Kampf gegen den Terrorismus der Schutz der Menschenrechte an erster Stelle stehen müsse.

Gleichwohl muss nüchtern konstatiert werden, dass die faktischen Auswirkungen dieser Gesetzgebung im Gegensatz zu den in den *USA* und anderen Ländern diskutierten Maßnahmen[6] jedenfalls zu keinen für uns beobachtbaren gravierenden Beeinträchtigungen der informationellen Selbstbestimmung geführt haben: Die neuen Befugnisse des Bundeskriminalamtes stellen nur eine Rechtsgrundlage für Verfahren dar, die tendenziell schon bisher durchgeführt wurden; die Erhebungsbefugnisse der Verfassungsschutzbehörden führen nicht zu einer Verpflichtung der angesprochenen Behörden und sind zudem weitgehend noch nicht in Landesrecht umgesetzt; die Aufnahme biometrischer Daten in Identitätspapiere, die ohnehin einer weiteren gesetzlichen Grundlage bedarf, steckt in der Phase der Prüfung des technischen Entwicklungsstandes - offensichtlich mit eher enttäuschenden Ergebnissen[7].

Vielmehr hat sich die öffentliche Diskussion in Deutschland und auch unsere Prüftätigkeit[8] auf die Durchführung der - bislang erfolglosen - *Rasterfahndung* zur Suche nach terroristischen „Schläfern“ konzentriert, die sich auf eine seit Jahren geltende Befugnis im Polizeirecht stützte und bundesweit zur Erhebung, Verarbeitung und Übermittlung von Daten hunderttausender unschuldiger Personen führte.

Sicherlich auch aufgrund der Konzentration der Innenministerien auf die Terrorismusbekämpfung blieben

Allein aus dem nicht explizit vorhandenen Normbefehl an die Verpflichteten kann dieser Schluss nicht gezogen werden. Wenn dies so wäre, würden die maßgeblichen Vorschriften leer laufen.

Auch in Berlin besteht der gesetzliche Handlungsbedarf nicht für das Ersuchen einer Datenübermittlung, sondern für die rechtlich relevante Datenübermittlung selbst.

---

[4] vgl. Garstka, Hansjürgen: Unter Generalverdacht. In: Müller-Heidelberg, Till u. a. (Hrsg.): Grundrechte-Report 2002 (mit Schwerpunkt Antiterrorgesetz). Reinbek: rororo, 2002, S. 41

[5] vgl. z. B. den Bericht der Organisation „Reporter ohne Grenzen” zu den Top 15 der freiheitsbeschränkenden Staaten – Deutschland landete auf Platz 5

[6] Nachdem der USA Patriot Act vom 24. Oktober 2001, H.R. 3162, bereits erheblich tiefere Eingriffe als die deutsche Gesetzgebung vorgesehen hatte, wurden Pläne des US-Justizministeriums bekannt, ein nationales Spitzelsystem „Terrorism Information and Prevention System” aufzubauen, für das allerdings der Kongress keine Gelder bewilligte. Unter der Bezeichnung „Total Information Awareness” plant das Pentagon eine zentrale Datenbank, die alle elektronischen Spuren, die Menschen in ihrem Alltag hinterlassen, verarbeiten soll

[7] vgl. „Die biometrische Identifizierung hat noch Schwächen”. In: Frankfurter Allgemeine Zeitung vom 31. Dezember 2001, S. 24; „Suche nach europäischer Lösung”. In: Berliner Zeitung vom 23. Januar 2002, S. 6

[8] vgl. 4.1.1

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

zwei große Gesetzgebungsvorhaben auf der Strecke, deren Verabschiedung zu Beginn der letzten Legislaturperiode angekündigt worden war: Das Gutachten zur *Modernisierung des Datenschutzrechts*, das im Auftrag des Bundesinnenministeriums gefertigt und im November 2001 übergeben worden war[9], wurde nicht einmal in ein derzeit so modisches „Eckpunktepapier" umgesetzt, die Planungen blieben in einer Länderumfrage stecken, in der vor allem kritische Stimmen zu hören waren. Der nahezu verabschiedungsreife Entwurf eines *Informationsfreiheitsgesetzes* des Bundes wurde in letzter Minute erstaunlicherweise vor allem aufgrund von Kritiken aus der Wirtschaft gestoppt, obwohl gerade diese, wie das amerikanische Vorbild zeigt, davon erheblich profitieren könnte[10]. Nach dem zwischen der SPD und Bündnis 90/Die Grünen abgeschlossenen Koalitionsvertrag sollen beide Vorhaben in der neuen Legislaturperiode wieder aufgenommen werden. Auch das nach dem neuen Bundesdatenschutzgesetz (BDSG) erforderliche *Auditierungsgesetz* ist nicht zustande gekommen.

Die Tragikomödie der Erarbeitung eines *Arbeitnehmerdatenschutzgesetzes* fand auch im vergangenen Jahr ihre Fortsetzung: Trotz allerlei Ankündigungen[11] und vielerlei Gerüchten, in den Schubläden des Arbeitsministeriums lägen Papiere bereit, wurde auch in der vergangenen Legislaturperiode kein Entwurf bekannt. Angesichts der Bemühungen der Europäischen Kommission, eine Richtlinie zu diesem Komplex zu erlassen, ist die Furcht sicherlich nicht unberechtigt, dass man sich in der neuen Legislaturperiode trotz entsprechender Vereinbarungen im Koalitionsvertrag damit herausreden wird, man müsse diese Richtlinie erst abwarten - die zuständige Generaldirektion der Kommission hat hierzu allerdings inzwischen mitgeteilt, es werde 2003 allenfalls zu einer zweiten Konsultationsrunde kommen. Dies bedeutet, dass der Erlass der Richtlinie in weiter Ferne liegt.

Angekündigt im Koalitionsvertrag ist auch, eine Regelung des Umgangs mit *genetischen Daten* zu schaffen, die die vielen Unklarheiten, die derzeit auf diesem Gebiet bestehen, beseitigt.

Über diese Projekte hinausgehend hat sich eine Gruppe von Landesdatenschutzbeauftragten vor der Bundestagswahl an die Parteien gewandt und nach deren Einstellung zu den anstehenden Aufgaben zur Weiterentwicklung des Datenschutzes gefragt[12]. Außer den angesprochenen Themen wurden dabei eingefordert:

Bei Darstellungen der Rechtsentwicklung des Datenschutzes auf Bundesebene und in Europa sieht der Senat nur in besonderen Einzelfällen Veranlassung zur Stellungnahme.

---

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

[10] vgl. 4.9

[11] vgl. z. B. die Antwort der Bundesregierung auf die Kleine Anfrage des Bundestagsabgeordneten Tauss vom Mai 2002

[12] Fragen von Datenschutzbeauftragten an die Parteien und KandidatInnen zur Bundestagswahl 2002, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2002", S. 30

- mehr marktwirtschaftliche Strukturen des Datenschutzes etwa in Form der Auditierung von Verfahren und Zertifizierung von Produkten,

- mehr Förderung datenschutzgerechter Technik („privacy enhanced technologies“),

- Aufrechterhaltung der Möglichkeit, das Internet auch anonym zu nutzen,

- Evaluierung der Eingriffsbefugnisse der Sicherheitsbehörden,

- mehr Schutz von Gesundheitsdaten, insbesondere angesichts der rasanten Entwicklung der Medizininformatik,

- Sicherung der Unabhängigkeit und Effizienz der Datenschutzaufsicht im privaten Bereich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beabsichtigt, die Forderungen zu übernehmen und der Bundesregierung zu übermitteln.

In der Gesetzesanwendung kam naturgemäß der Umsetzung des BDSG 2001 große Bedeutung zu. Wir haben zusammen mit dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein zu den wesentlichen Aspekten eine Broschüre entwickelt, die bundesweit Beachtung gefunden hat. Von erheblicher Bedeutung haben sich dabei die neuen Bestimmungen über besondere Arten personenbezogener Daten[13], den Datentransfer in Drittländer[14] sowie über die Videoüberwachung[15] erwiesen.

Auch die Rechtsprechung hat sich wieder mit einer Vielzahl datenschutzrechtlicher Probleme auseinandergesetzt: Das prominenteste Urteil war sicherlich die Entscheidung des Bundesverwaltungsgerichts[16], dass der ehemalige Bundeskanzler Helmut Kohl einen Anspruch gegenüber der Bundesbeauftragten für die *Stasiunterlagen* auf Unterlassung der Herausgabe personenbezogener Daten hat: Auch *Personen der Zeitgeschichte* haben ein Recht auf Privatsphäre, ein Thema, das weltweit diskutiert wird**.** Prompt folgte eine Novellierung des Stasi-Unterlagen-Gesetzes, die allerdings an der bisher bestehenden Rechtslage kaum etwas ändert.

In der Öffentlichkeit heftig diskutiert wurden die verschiedenen Entscheidungen zur Durchführung der

---

[13] vgl. 3.1

[14] vgl. 4.7.3

[15] vgl. 4.8.4

[16] Urteil vom 8. März 2002, Az.: BVerwG 3 C 46.01

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Rasterfahndung, die in den einzelnen Bundesländern stark voneinander abwichen, am Ende sich aber zunehmend der Auffassung näherten, die Maßnahme sei grundsätzlich zulässig[17].

Der Bundesgerichtshof stärkte die Unabhängigkeit der Datenschutzbeauftragten, indem er den Vorwurf zurückwies, der Sächsische Datenschutzbeauftragte habe durch die Veröffentlichung einzelner Angaben aus den Akten eines Ministeriums im Zusammenhang mit einer Beanstandung einen strafbaren Geheimnisverrat begangen[18].

Das deutsche Datenschutzrecht wird zunehmend mehr durch europäisches Recht vorgeprägt. Nachdem bereits das Bundesdatenschutzgesetz wegen der Europäischen Datenschutzrichtlinie[19], das Telekommunikations- und Teledienstерecht wegen der *Telekommunikationsrichtlinie*[20] sowie der *E-commerce-Richtlinie*[21] novelliert werden mussten, stehen weitere Anpassungen an das Europarecht ins Haus.

Die Datenschutzrichtlinie sieht vor, dass die Europäische Kommission eine Evaluierung der Umsetzung in das nationale Recht vornimmt. Dieser Prozess ist in vollem Gange, eine Konferenz Anfang Oktober 2002 hat erste Ergebnisse gezeigt. Mit einiger Wahrscheinlichkeit werden die Ergebnisse, die im Laufe des Jahres 2003 zu erwarten sind, den deutschen Gesetzgeber oder zumindest die Regierungen zwingen, Änderungen an der bestehenden Rechtslage bzw. Verwaltungsorganisation vorzunehmen. Auch die Gesetzgebung zur *Informationsfreiheit* wird nicht unbeeinflusst bleiben können von den im Amsterdamer Vertrag vorgegebenen Bemühungen zur Öffnung der Unterlagen der Institutionen der Europäischen Union[22] sowie zur Kommerzialisierung öffentlicher Daten[23].

Geradezu hektischen Druck erzeugen die europäischen Aktivitäten auf dem Gebiet der Kommunikation. Im Juli wurde die neue Elektronische *Kommunikationsrichtlinie* verabschiedet und veröffentlicht[24], die eine

---

[17] vgl. 4.1.1

[18] Urteil vom 9. Dezember 2002, Az.: 5 StR 276/02

[19] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG L 281

[20] Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, ABl. EG L 24/1 vom 30. Januar 1998

[21] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl. EG L 178/1

[22] Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission, ABl. EG L 145/43

[23] Proposal for a Directive on the re-use and commercial exploitation of public sector information vom 5. Juni 2002

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

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

erneute Änderung des Telekommunikations- und Teledienstrechts notwendig macht. Noch unklar ist, wie sich der Fortgang von Bemühungen aus der „dritten Säule“ entwickelt, zu europaweit verbindlichen Festlegungen der Speicherfristen von Verkehrsdaten zu kommen, die eine Speicherung auch ohne Erforderlichkeit für Telekommunikationszwecke vorschreiben.

Auch das *Umweltinformationsgesetz* wird geändert werden müssen, da die neue Umweltinformationsrichtlinie[25] die bisherige Rechtslage zugunsten der Bürgerrechte verbessert.

Die hier erwähnte Umweltinformationsrichtlinie ist mit Datum vom 14. Februar 2003 in Kraft getreten; sie muss bis Februar 2005 in nationales Recht umgesetzt sein.

Das gleiche gilt für das *Verbraucherkreditrecht*, zu dem ebenfalls eine Richtlinie vorbereitet wird[26], die allerdings beim derzeitigen Erörterungsstand die datenschutzrechtlichen Anforderungen noch nicht hinreichend berücksichtigt.

Das BMU arbeitet bereits an einem Referentenentwurf zu einer dementsprechenden Novellierung des Umweltinformationsgesetzes (UIG).

Schließlich werden die Bemühungen des *Europäischen Konvents* zur Schaffung einer Europäischen Verfassung**,** in die auch das in der Grundrechtecharta enthaltene Grundrecht auf Datenschutz sowie das Recht auf Aktenzugang aufgenommen werden, erneut die Frage aufwerfen, ob es nicht zwingend geboten ist, das Grundgesetz um ein Grundrecht auf informationelle Selbstbestimmung sowie auf Informationsfreiheit zu ergänzen.

Der Senat hat bereits in seiner Stellungnahme zum Jahresbericht 2000 ausgeführt, dass eine solche Transformation rechtlich nicht zwingend ist.

Das in Art. 8 der Grundrechtscharta enthaltene Grundrecht auf informationelle Selbstbestimmung wird im deutschen Verfassungsrecht bereits aus dem allgemeinen Persönlichkeitsrechts gemäß Art 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 GG abgeleitet. Eine Aufnahme des Artikels ins Grundgesetz hätte daher allenfalls deklaratorische Wirkung und wäre ohne rechtliche Konsequenzen.

Darüber hinaus sieht die Grundrechtscharta in Art. 41 ein Recht auf Zugang zu den eigenen Daten und in Art. 42 ein Recht auf Zugang zu den Dokumenten des Europäischen Parlaments, des Rats und der Kommission vor.

Das Recht auf Zugang zu den eigenen Daten ist bereits in dem Grundrecht auf informationelle Selbstbestimmung nach Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 GG enthalten und in einer Vielzahl nationaler Vorschriften einfachrechtlich geregelt.

Das Akteneinsichtsrecht in Art. 42 bezieht sich ausschließlich auf die Dokumente der genannten EU-Organe und kann allenfalls als Impuls für die Schaffung entsprechender Zugangsrechte in den Mitgliedstaaten gesehen werden. Eine rechtliche Verpflichtung zum Erlass entsprechender Regelungen, noch dazu auf Verfassungsebene, ergibt sich hieraus jedoch nicht.

---

[25] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über den Zugang der Öffentlichkeit zu Umweltinformationen

[26] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Harmonisierung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über den Verbraucherkredit

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

In Berlin sind entsprechende Regelungen bereits durch das Berliner Informationsfreiheitsgesetz vom Oktober 1999 geschaffen worden. Hierin sind auch die nötigen Verfahrensvorschriften zur Durchführung des Akteneinsichtsrechts enthalten, so dass es derzeit auch im Hinblick auf oben genannten Artikel der Grundrechtscharta keiner weitergehender Regelungen zur Informationsfreiheit oder gar einer Ergänzung des Grundgesetzes bedarf.

1.2 Berlin

In Berlin standen 2002 vorwiegend Anwendungsprobleme mit dem neuen Berliner Datenschutzgesetz (BlnDSG) sowie dem Informationsfreiheitsgesetz (IFG) im Vordergrund.

Es ist nicht zu bestreiten, dass beide Gesetze sowohl inhaltliche als auch formale Mängel aufweisen, die in der neuen Legislaturperiode beseitigt werden sollten. Im Unterausschuss „Datenschutz und Informationsfreiheit" des Innenausschusses des Abgeordnetenhauses ist dies mit dem Ziel diskutiert worden, möglichst bald entsprechende Initiativen zu entwickeln. Dabei wurde ein Vorschlag aufgegriffen, den wir schon im Jahresbericht 1990[27] vorgebracht haben. Er hat Vorbilder in anderen Staaten (z. B. in Kanada) und ist auch Gegenstand eines Forschungsprojektes, das aufgrund einer Beschlussfassung des Deutschen Juristentages[28] initiiert wurde und nunmehr unter Federführung von Prof. Michael Kloepfer (Humboldt-Universität) durchgeführt wird[29]: Datenschutz- und Informationsfreiheitsrecht sollen in einem einheitlichen *Informationsgesetzbuch* zusammengefasst werden, wobei auch weitere Gesetze, die die Verarbeitung personenbezogener Daten betreffen, einbezogen werden könnten (Informationsverarbeitungsgesetz, Statistikgesetz, Archivgesetz u. a.). Die Senatsverwaltung für Inneres hat sich bereit erklärt, mit uns zusammen in Erörterungen einzutreten, wie dieses Projekt verwirklicht werden könnte[30].

Der Senat teilt die Auffassung, dass in einem gewissen Umfang – jedenfalls im Bereich der Informationsfreiheit – redaktionelle Klarstellungen zur besseren Handhabbarkeit des Gesetzes wünschenswert erscheinen.

Der Senat legt Wert auf die Feststellung, dass zunächst eingehend geprüft werden muss, ob die Schaffung eines solchen (Landes-)Informationsgesetzbuches – welches derzeit weder auf Bundes- noch auf Landesebene ein Vorbild hat – überhaupt sinnvoll und vorteilhaft für die Handhabung der Rechtsbereiche Datenschutz und Informationsfreiheit ist.

Die Senatsverwaltung für Inneres hat sich im Unterausschuss Datenschutz zu entsprechenden Erörterungen bereit erklärt. Diese Erörterungen beziehen sich aber zunächst auf die Frage, ob die Schaffung eines Informationsgesetzbuches überhaupt angestrebt werden sollte und welche Vor- und Nachteile mit einem solch umfangreichen Projekt verbunden sind. Insoweit bestehen aus Sicht des Senats Zweifel im Hinblick auf die Schaffung eines Informationsgesetzbuches und noch erheblicher Klärungsbedarf. Über die tatsächliche Realisierung dieses Projekts ist folglich noch nicht entschieden worden, die Entscheidung wird erst nach der vorgenannten Vorprüfung zu treffen sein.

Bei den datenschutzrechtlichen Spezialbestimmungen

---

[27] JB 1990, 1.2

[28] 62. Deutscher Juristentag in Bremen (22. - 25. September 1998, Ziff. 4 der Beschlüsse der Abteilung Öffentliches Recht

[29] Als erstes Ergebnis ist der Entwurf eines Informationsfreiheitsgesetzes für die Bundesrepublik Deutschland erschienen: Schoch, Friedrich; Kloepfer, Michael: Informationsfreiheitsgesetz (IFG-ProfE). Berlin: Duncker & Humblot, 2002

[30] vgl. Protokoll der 7. Sitzung des Unterausschusses „Datenschutz und Informationsfreiheit" des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses vom 24. September 2002

stand die Frage im Vordergrund, unter welchen Voraussetzungen der Polizei ermöglicht werden sollte, im öffentlichen Raum eine *Videoüberwachung* durchzuführen. Im Gegensatz zu anderen Ländern, wo dies ermöglicht wurde, wurde in Berlin ein Gesetzentwurf erarbeitet, der nicht auf den Raum, sondern auf gefährdete Objekte abstellt. Diese Einschränkung, verbunden mit einer Reihe von sichernden Maßnahmen, konnte von uns gebilligt werden. Das Gesetz ist inzwischen verabschiedet worden.

Andere Gesetzgebungsprojekte betreffen Verfahren, die im Rahmen der Verwaltungsreform und der Weiterentwicklung des *eGovernment* entwickelt werden, die aber nach den Vorgaben des Datenschutzrechts einer eigenen Rechtsgrundlage bedürfen: Hierzu gehören das Projekt einer Personalstatistik[31], der Veröffentlichung von Grundstücksdaten im Internet[32] oder umfangreiche Änderungen des Schulrechts z. B. im Hinblick auf die Einführung von Evaluierungsverfahren[33].

2. Technische Rahmenbedingungen

2.1 Entwicklung der Informationstechnik

Die quantitativen Fortschritte in der Entwicklung der *Informationstechnik* lassen sich am besten in den Werbebeilagen der einschlägigen Discounter in der Tagespresse erkennen. Noch schnellere Prozessoren mit Taktgeschwindigkeiten von 3 Gigahertz, Arbeitsspeicher von 512 Megabyte bis 1 Gigabyte, Festplatten mit 80-100 Gigabyte, CD- oder gar DVD-Brenner als Ausstattungsmerkmal kennzeichnen die Personalcomputer, die wir uns in unsere Wohnzimmer stellen sollen. Die riesigen Kapazitäten wollen mit Daten versorgt werden. Normale Anwendungen wie Textverarbeitung und Tabellenkalkulation oder die Nutzung des Internet, die auch im privaten Leben Bedeutung erlangen können, beanspruchen nur einen Bruchteil der Kapazitäten. Die Speicherung von Musikdaten, die Bearbeitung und Speicherung von Fotografien und Filmen zur Verwendung im „Home-Entertainment-Center" scheinen die „Killer-Applications" (Anwendungen, die eine Technologie zum Durchbruch führen) zu sein, die die technischen Daten der PCs nach oben treiben.

Die Verschmelzung der unterschiedlichen Unterhaltungsmedien in der häuslichen PC-Anwendung, die Verknüpfung mit den unterschiedlichen Ein- und Ausgabemedien (Fotoscanner und –drucker, hochauflösende Fernseher, CD- und DVD-Player und –Brenner, Tonaufnahme- und Wiedergabesysteme) machen den PC zum Zentrum der Freizeitgestaltung.

---

[31] vgl. 4.5.1

[32] vgl. 4.4.4

[33] vgl. 4.5.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Hinzu kommt, dass der PC auch als universelles Kommunikationssystem eingesetzt wird, mit dem E-Mails versandt und empfangen werden, mit dem neue Programme, neue Musik, neue Bilder aus den Tiefen des Internet heruntergeladen werden können und so für eine ständige Anreicherung der häuslichen Unterhaltungsressourcen gesorgt werden kann. Das Internet kommt als Selbstbedienungsladen daher und die Verbraucher sind es gewöhnt, dass dieser Laden keine Kasse hat, dass die meisten Dienstleistungen also kostenlos bereitgestellt werden.

Dies wird sicher auf die Dauer nicht so weitergehen. Anspruchsvollere Dienstleistungen werden nach und nach kostenpflichtig und aus datenschutzrechtlicher Sicht wird es darauf ankommen zu prüfen, ob dies in anonymer Form möglich ist, und falls nicht, welche nutzerbezogenen Daten dafür gesammelt werden. Hinzu kommt, dass die Träger von Urheberrechten nicht mehr länger hinnehmen wollen, dass ihre geschützten Produkte kostenfrei im Internet ausgetauscht und heruntergeladen werden.

Es wird also für die Unternehmen, die im Internet aktiv sind, immer interessanter, mehr über ihre Klientel zu erfahren, die wiederum glaubt, sich im Netz anonym zu bewegen. Dies gibt uns in diesem Jahr den Anlass, die fortschreitenden Bemühungen zu beschreiben, von außen die Aktivitäten der Nutzer im Internet zu beeinflussen, zu steuern und zu kontrollieren, teils über versteckte Funktionalitäten, teils mit dem Angebot komplexer Dienstleistungen.

Was Hard- und Software über uns verraten

Schon in der Vergangenheit mussten wir uns mit den Ausforschungsbemühungen namhafter Unternehmen der IT-Branche beschäftigen:

Im Jahresbericht 1999[34] berichteten wir über den Pentium-III-Prozessor von Intel, dessen *Chip-Identifikationsnummer (Chip-ID)* bei der Internet-Kommunikation mitgesendet oder von außen abgefragt

Der Senat begrüßt, dass in den dargestellten Fällen die Bemühungen Erfolg hatten, die unfreiwillige und nicht erforderliche Übermittlung von Daten einzuschränken bzw. zu unterbinden.

Die speziell bei Windows XP vorhandenen Risiken und die im Bericht aufgezeigten Schutzmaßnahmen müssen bei einem möglichen Einsatz von Windows XP berücksichtigt werden. Es sei aber darauf hingewiesen, dass der landesweite Diskussionsprozess zum zukünftigen Umgang mit Microsoft-Betriebssystemen nicht abgeschlossen ist und damit auch der landesweite Einsatz von Windows XP derzeit nicht aktuell ist.

[34] JB 1999, 2.1

werden konnte. Die Chip-ID sollte für eine sicherere Authentifizierung eines Benutzers sorgen, insbesondere bei Bankgeschäften. Nach massiven Protesten forderte Intel die PC-Hersteller auf, die Chip-ID im BIOS (Basic Input Output System) der PCs standardmäßig zu deaktivieren, und kündigte an, die Zusammenarbeit mit allen Software-Herstellern bei Applikationen zu beenden, die unter Verwendung der Chip-ID arbeiten, sowie die Fertigstellung und Weiterentwicklung solcher Software zu unterbinden.

Etwas später entdeckten amerikanische Fachleute, dass der Software-Marktführer Microsoft bei der Online-Registrierung des Betriebssystems WINDOWS 98 jedem Kunden eine weltweit eindeutige Nummer *(HWID - Hardware Identifikationsnummer)* zuordnete und auf dem Kundenrechner abspeicherte. Die Nummer konnte aus dem Rechner abgefragt werden. Auch hier kam es zu Protesten, die dazu führten, dass Microsoft zunächst ein Service-Pack anbot, mit dem die HWID gelöscht werden konnte. Außerdem sagte die Firma zu, alle Daten in den eigenen Datenbanken zu löschen, deren Übermittlung nicht mit Einwilligung der Kunden geschah.

Das Microsoft-Produkt Office 97 ordnete den damit erzeugten Dokumenten eindeutige Nummern zu, die beim Transport über das Internet etwa als Anhang von E-Mails mitversandt wurden. Microsoft erläuterte hierzu der zuständigen Datenschutz-Aufsichtsbehörde in Deutschland, dass es sich dabei um eine Nummer handele, die mit der HWID nichts zu tun hätte, sondern eine GUID (Global Unique Identifier) sei, die ein Dokument dem Rechner zuordnen kann, in dem es entstanden ist. Diese Nummer diene der Zuordnung von Dokumenten, die in einem Netz zirkulieren, und soll damit die Zusammenarbeit der Netzteilnehmer erleichtern. Die Einwände der Datenschützer führten dazu, dass für die GUIDs ein Löschprogramm bereitgestellt und für zukünftige Versionen auf die GUID verzichtet wurde.

Die beiden genannten großen Firmen waren keineswegs die einzigen „Sünder", die sich für ihre Kunden mehr als datenschutzrechtlich geboten interessierten. Die für dieses Thema nunmehr sensibilisierte Fachwelt fand Juxprogramme und Musikwiedergabeprogramme kleinerer Hersteller, die ebenfalls heimlich Identitätsdaten von den Benutzern an die Herstellerfirmen weiterleiteten. Auch hierüber berichteten wir bereits 1999.

Zwei Jahre später[35] berichteten wir über die Überwachung der Internetkommunikation mit dem Programmsystem *CARNIVORE* durch die amerikanischen Sicherheitsbehörden. Das Programm, das alle E-Mails und Chats, die über einen Provider laufen, nach verdächtigen Inhalten durchsucht, erhielt später den harmloser

[35] JB 2001, 2.1

klingenden Namen DCS 1000 (Digital Collection System 1000). Das EPIC (Electronic Privacy Information Center) geht sogar davon aus, dass sämtliche Internet-Daten damit durchsucht werden können.

Anfang des Jahres berichtete eine amerikanische Tageszeitung, dass der aktuelle Browser von *Netscape* Daten an einen AOL-Server überträgt. So wurden bei Nutzung der integrierten Suchfunktion die aktuelle IP-Adresse des Nutzers, der Suchbegriff, eine Identifikationsnummer und das Installationsdatum gesendet. Netscape gab auf Fragen an, dies sei nur für statistische Zwecke gedacht, nämlich zur Feststellung, wie oft die eigene Suchmaschine genutzt werde.

Vor jetzt einem Jahr hat Microsoft das Betriebssystem *Windows XP* herausgebracht. Auch dieses Betriebssystem ist von bemerkenswerter Geschwätzigkeit, wenn man als Benutzer nichts dagegen tut.

Das neue Betriebssystem verlangt eine Zwangsaktivierung. Welche Daten bei der automatisierten Aktivierung des Betriebssystems über das Internet an Microsoft übermittelt werden, ist allerdings bisher nicht bekannt. Eine anonyme Aktivierung ist telefonisch möglich, wenn dafür Sorge getragen wird, dass die Rufnummer nicht mit übermittelt wird.

Weitere Funktionen von Windows XP nehmen regelmäßig mit Microsoft-Servern Kontakt auf. So prüft eine Updatefunktion regelmäßig, ob Aktualisierungen vorliegen, und falls nicht, lädt es diese auf die Festplatte. Auch andere Applikationen wie z. B. der Internet Explorer prüfen, ob Aktualisierungen vorliegen.

„Ich weiß, was du letzten Sommer geschaut hast" lautete die Schlagzeile eines einschlägigen Online-Dienstes und bezog dies auf die Eigenschaft des *Windows Media Players* für Windows XP, ohne Wissen der Nutzer den Anmeldenamen und die abgespielten Stücke in eine Logdatei auf der Festplatte zu schreiben. Diese Informationen übermittelt der Media Player mit seiner Seriennummer per Internet an die Microsoft-Datenbank. Diese Seriennummer ist zwar nicht personenbeziehbar, solange man sich nicht beim Microsoft Windows Media Newsletter anmeldet. Tut man dies aber, so stehen die Seriennummer, der Nutzername und die E-Mail-Adresse zusammen in der Datenbank. Der Internetzugriff des Media Player kann mit einer Einstellung des Programms unterbunden werden.

Während die Ausforschungsfunktionen von Windows XP weitgehend als Leistungsmerkmale des Systems bekannt gemacht wurden und durch geeignete Einstellungen unterbunden werden können, zeigten die zuvor beschriebenen Fälle, dass die informationelle Selbstbestimmung der Benutzer für die Unternehmen keine Rolle gespielt hatte.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Der elektronische Pass

Den Datenschutz der Benutzer wollen Unternehmen fördern, die *Identitätsmanagement-systeme* im Internet anbieten. Allerdings mischt sich in Freude über solche Werkzeuge zum Schutz der individuellen Netzwerkidentität ein wenig Skepsis.

Der Senat ist ebenso wie der Berliner Beauftragte für Datenschutz und Informationsfreiheit der Ansicht, dass ein „Single-Sign-On"-Ansatz aus Sicht des Datenschutzes grundsätzlich zu begrüßen ist. Eine Nutzung des von Microsoft angebotenen Systems „Passport" im Rahmen der Internet-Nutzung der Berliner Verwaltung steht jedoch nicht zur Debatte.

Für den elektronischen Benutzerpass, der den Zugang zu allen Diensten ermöglicht, bei denen die Benutzer sich authentifizieren müssen, stehen derzeit zwei Konzepte zur Auswahl: Das Passport-Verfahren von Microsoft und als Gegenkonzept das von Sun Microsystems initiierte Liberty Alliance Project.

Beide Authentifizierungsdienste unterstützen das *Single-Sign-On-Konzept*. Die Idee dabei ist, dass der Nutzer mit einer einzigen Anmeldung alle Dienste erreichen kann, bei denen er registriert ist und bei denen er sich sonst mit einer Identität und eigenem Passwort anmelden müsste. Er verfügt also über eine einzige Netzidentität, obwohl er gegenüber allen von ihm genutzten Diensten unterschiedliche Identitäten definiert haben kann. Die verschiedenen Identitäten auf eine einzige zu konzentrieren ist die Aufgabe der Identitätsmanagementsysteme.

Bei der Anmeldung zum Verfahren *Passport* von Microsoft wird eine E-Mail-Adresse und ein vom Nutzer zu vergebendes Passwort benötigt. Weitere persönlichen Daten können zu einem eigenen Benutzerprofil zusammengestellt werden, so dass individuelle Wünsche den Passport-Partnern automatisch übermittelt werden können. Auch Kontoverbindungsdaten, Kreditkartennummern, Rechnungs- und Lieferadressen können bereits angegeben werden, damit sie für den Internet-Einkauf zur Verfügung stehen. Es kann festgelegt werden, welche Daten an Partnersites weitergegeben werden dürfen. Zu jedem Benutzer legt die Datenbank einen eindeutigen 64-Bit-Wert ab, den Passport Unique Identifier (PUID). Dieser Wert wird an alle Benutzerdaten gekoppelt. Diese Daten werden weltweit und zentral auf einem Sicherheitsserver bei Microsoft verschlüsselt hinterlegt.

Danach muss man sich beim Besuch von Websites, die dem Passport-Dienst angeschlossen sind, nicht mehr mit verschiedenen Nutzerkennungen und Passwörtern anmelden, sondern ausschließlich mit der bei der Anmeldung hinterlegten E-Mail-Adresse und dem dazugehörigen Passwort. Die Partner-Websites erhalten die vom Kunden üblicherweise verwandten Voreinstellungen und Kundendaten.

Das mit Passport unterstützte Single-Sign-On ist aus der Sicht der Datensicherheit zu begrüßen. Der ständige Umgang des Benutzers mit unterschiedlichen Identitäten und Passwörtern führt zu Risiken für seine Netz-

authentität, da niemand mehr alle seine Passwörter behalten kann, mit der Folge, dass man sie irgendwo aufschreibt. Damit gerät ihre Vertraulichkeit in Gefahr.

Es gibt aber auch kritische Fragen an dieses Konzept. Der Kunde muss darauf vertrauen, dass das Passport-System nur die vereinbarten Daten an die Partnerunternehmen sendet, kontrollieren kann er es nicht.

Wird der zentrale Sicherheitsserver erfolgreich angegriffen, so können die vertraulichen Kundendaten, die dort in großen Massen hinterlegt sind, missbraucht werden, ein Desaster von kaum abzuschätzendem Ausmaß. Dass dies nicht einfach von der Hand zu weisen ist, zeigt ein Vorfall, der sich im August 2001 zugetragen hat. Mit der Veränderung von drei Zeilen im Programm des Anmeldeservers des E-Mail-Dienstes Hotmail von Microsoft überwand ein IT-Experte die Hacker-Sicherung und konnte so an die Passport-Nutzerdaten gelangen[36]. Dies war möglich, weil jeder, der sich eine kostenlose E-Mail-Adresse bei Hotmail anlegte, auch automatisch bei Passport registriert wurde. In der Zwischenzeit sind weitere Zweifel daran laut geworden, dass Microsoft den Passport-Dienst mit hinreichender Sicherheit betreiben kann[37].

Ein neueres Konzept von Microsoft sieht vor, dass andere Firmen in die Lage versetzt werden, eigene Passport-Datenbanken zu betreiben. Dies würde dem Monopol-Vorwurf entgegenstehen, der auch im Zusammenhang mit Passport gegen Microsoft erhoben wird.

Diese Öffnung stellt eine Verbindung zum Konzept der *Liberty Alliance* her. Sun Microsystems als Initiator der Liberty Alliance beteiligt sich an der Entwicklung eines zu Passport alternativen Systems, das auf offenen Standards beruht. Die 33 Gründerfirmen – inzwischen liegen mehr als 2000 weitere Anfragen nach einer Mitgliedschaft vor - wollen ein Single-Sign-On ohne zentrale Instanz einrichten. Hierbei sollen die Kundeninformationen bei dem Website-Betreiber verbleiben, bei dem der Nutzer sein Konto eingerichtet hat. Nach der Spezifikation 1.0 der Liberty Alliance sollen ausschließlich Authentifizierungsinformationen zwischen den Unternehmen und keine Details über die Identität des Nutzers ausgetauscht werden.

Hier wird es darauf ankommen, ein einheitliches Sicherheitsgefüge zwischen den einzelnen Authentifizierungsdiensten einzurichten und die Kommunikation zwischen den Servern zu steuern. Die aus der Zentralität des Passportservers resultierenden Risiken entfallen

[36] Der Spiegel 44/2001, S. 222

[37] So hat die US-Aufsichtsbehörde Federal Trade Commission (FTC) den Passport-Dienst von Microsoft beanstandet und in einem Vergleich erreicht, dass Microsoft ein umfassendes Sicherheitssystem einrichtet und alle zwei Jahre durch unabhängige Experten überprüfen lässt

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

dagegen beim Konzept der Liberty Alliance.

Bei beiden Diensten ist dem Risiko entgegenzutreten, dass Nutzerprofile entstehen und entsprechend vermarktet werden.

Aufgezwungene Sicherheit

Um die Sicherheit seiner Informationstechnik hat sich der durchschnittliche private Nutzer bisher noch nicht sonderlich gekümmert. Vereinzelt setzt er Virenschutzprogramme ein, bewusste Vielsurfer schützen sich vielleicht auch schon mit einem Firewallprogramm. Aber sonst werden die Risiken eher gelassen gesehen, geht es doch nicht um existenziell wichtige Anwendungen, sondern „nur" um Home Entertainment. Dies soll nach dem Willen der *Trusted Computing Platform Alliance (TCPA)* (Allianz für vertrauenswürdige Computerplattformen) anders werden. Gleichzeitig soll ein technisches Verfahren zum Schutz der Urheberrechte durchgesetzt werden.

Die TCPA ist eine von Compaq, HP, IBM, Intel und Microsoft gegründete Initiative. Ziel dieser Initiative ist die Einführung einer Plattform, die den PC durch den Einbau von Hard- und Software sicherer machen möchte. Hierfür wird in einer ersten Stufe ein Chip eingebaut, der darüber wachen soll, dass weder die Hardware manipuliert, die Software ohne Lizenz genutzt noch auf Dokumente unberechtigt zugegriffen werden kann.

Palladium ist eine Software, die von Microsoft entwickelt wurde und in die zukünftigen Windows-Betriebssystem-Versionen integriert werden soll. Sie soll auf dem TCPA-Konzept aufsetzen und zusätzliche Funktionen wie z. B. eine Verschlüsselung bereitstellen. Noch ist der gewünschte Entwicklungsstand nicht erreicht, doch erste Ansätze sind z. B. durch den oben bereits dargestellten Registrierungszwang bei Microsofts Betriebssystem Windows XP umgesetzt worden.

Die weitere Entwicklung ist noch nicht absehbar. Es ist wahrscheinlich, dass mit TCPA/Palladium eine kombinierte Hard-/Softwarelösung entstehen wird, die in einem geschützten Bereich im Rechner kontrolliert, ob die eingesetzte Software vom Hersteller zertifiziert ist und somit verhindert wird, dass der Nutzer installierte und zertifizierte Anwendungen nachträglich verändern kann.

Die Manipulation einer Anwendung würde dazu führen, dass sich die Software automatisch deaktiviert und ein erneuter Programmstart erst wieder möglich ist, wenn eine erneute Zertifizierung beim Hersteller erfolgt ist. Möglich ist auch, dass über Internet eine automatische Meldung des unberechtigten Vorgangs beim Hersteller ausgelöst wird, der seinerseits auf dem gleichen Wege die Software deaktiviert.

Der Senat wird die weiteren Entwicklungen im Zusammenhang mit TCPA und Palladium aufmerksam verfolgen.

Die illegale Verbreitung von Software kann mit dem digitalen Siegel für installierte oder über das Internet heruntergeladene Programme nachhaltig verhindert werden, da die Programme nur auf dem dafür autorisierten Rechner ablaufen können. Da eine Vireninfektion mit der Veränderung eines Programms verbunden ist, kann man sich auch hier Sicherheitswirkungen versprechen, wenn die Abarbeitung unzulässig manipulierter Programme verhindert wird.

Diesen Vorteilen hinsichtlich des Daten- und des Urheberrechtsschutzes stehen jedoch erhebliche Risiken gegenüber:

Die Kontrollmechanismen können in die Privatsphäre jedes Einzelnen eingreifen, wenn die Programme mit ihren Herstellern kommunizieren und wenn bei einer Zertifizierung Daten über den privaten PC-Einsatz an den Hersteller übermittelt werden. Wenn hier nicht streng dem Grundsatz der Datensparsamkeit gefolgt wird, wird aus dem persönlichen Computer, mit dem frei umgegangen werden kann, der kontrollierte Computer, der nur das zu tun erlaubt, was die Hersteller noch zugestehen mögen.

Ein Update des Microsoft *Media Players* 7 löste bereits im Berichtsjahr eine Welle der Empörung aus, da der Anwender durch Akzeptierung der Lizenzbedingungen gezwungen wurde zuzustimmen, dass auf seinem Rechner automatisch eine Kopierschutzsoftware installiert wird. Die Gefahr ist offensichtlich, dass der Nutzer überwacht und bei Verstößen der Hersteller informiert wird. Erste Ansätze zur Umsetzung dieser Strategie sind unter den Begriffen TPM (Trusted Platform Module) oder Fritz Chip (nach dem US-Senator Fritz Hollings benannt) als Hardwarebausteine des TCPA-Konzeptes bekannt.

Der *Fritz-Chip*, welcher vorerst als Extrachip auf dem Motherboard und später im Prozessor integriert werden soll, übernimmt beim Start die Kontrolle des Rechners und führt sowohl eine Benutzerauthentifizierung als auch eine Entschlüsselung des geschützten Bereichs der Festplatte, die beim vorherigen Herunterfahren verschlüsselt worden war, durch. Sollte der Rechnerstart auf Probleme stoßen, so wird ein Fernwartungsprozess ausgelöst, bei dem Daten an eine zur Wartung bereitstehende Stelle gesendet werden, um das Problem zu beheben. Hier ist zu verlangen, dass dem Benutzer die Art der Daten und der Empfänger der Daten transparent gemacht wird.

Es wird eine Gefahr darin gesehen, dass die entwickelnden bzw. mitunterzeichnenden Unternehmen durch diese Technik eine Marktbeherrschung erlangen könnten, zumal insbesondere Microsoft einem solchem Vorwurf ständig ausgesetzt ist. Hier wären Kontrollinstanzen zu schaffen, die nicht von wirtschaftlichen Interessen geleitet werden.

Auch im Microsoft Betriebssystem Windows XP sind TCPA-konforme Spezifikationen eingebaut. So muss nach entsprechenden Änderungen an der Rechnerhardware eine neue Aktivierung bei Microsoft erfolgen. Die mit Windows 2000 eingeführte Treiberzertifizierung führt ebenfalls dazu, dass das Betriebssystem bei der Installation eines nicht von Microsoft zertifizierten Treibers warnt.

Das TCPA-Konzept wirft eine Reihe von praktischen Fragen bei der Internetkommunikation auf: Arbeitet der Rechner auch dann ordnungsgemäß, wenn er im „unsicheren Modus", also nicht unter Kontrolle von außen gestartet wird? Sind dann alle Anwenderdaten zugreifbar? Was geschieht mit Rechnern, die aus Sicherheitsgründen nicht mit dem Internet verbunden werden dürfen? Müssen diese Systeme auf Sicherheitsfunktionen verzichten?
Das TCPA/Palladium-Konzept bietet gleichwohl eine Reihe von Chancen für die informationstechnische Sicherheit:

- Das TCPA-Konzept könnte zur Durchsetzung starker Zugangskontrollen zu personenbezogenen Daten verwendet werden. Beispielsweise könnte eine Behörde oder ein Unternehmen die Mitarbeiter dazu veranlassen, Dokumente mit personenbezogenen Daten mit einem entsprechenden Status zu versehen, so dass nur TCPA-konforme Rechner, die von der Behörde oder dem Unternehmen zertifiziert wurden, die Dokumente bearbeiten können.

- Texte können verschlüsselt werden, so dass sie nur für eine vorher bestimmte Anwenderkonfiguration lesbar oder weiterbearbeitbar sind.

- Die in einem Löschkonzept getroffenen Regelungen können automatisiert ausgeführt werden. So könnte z. B. eine Protokolldatei nach Ablauf der Aufbewahrungsfrist automatisch gelöscht werden.

- Es kann verhindert werden, dass Software, die von einem Anwender in betrügerischer Absicht manipuliert wurde, mit dem zertifizierten Rechner ausgeführt werden kann.

- Unerwünschte Manipulationen der Hardware, z. B. das Anschließen eines USB-Speichergerätes zum illegalen Export von Daten, führen zum Ausfall des gesamten Rechners.

- Patches, die dafür sorgen, dass Sicherheitsschwachstellen unmittelbar nach Entdeckung geschlossen werden, können automatisiert eingespielt werden. Diese Art von Fernwartung ist allerdings auch nicht unproblematisch, weil dafür administrative Berechtigungen notwendig sind, die aus der Ferne ausgeführt werden, jedoch nur vertrauenswürdigen Personen, z. B. Systemadministratoren,

eingeräumt werden können.

2.2 Datenverarbeitung in der Berliner Verwaltung

Die außerordentlichen finanziellen Engpässe, unter denen die Berliner Verwaltung zu leiden hat, verlangen es, die Rationalisierungspotenziale der Informationstechnik auch weiterhin auszuschöpfen. Dienstleistungen, die über das Internet angeboten werden, sind nicht nur modern und bürgernah, sondern können auch helfen, menschliche Arbeitskraft einzusparen. Unter den gegebenen Haushaltsbedingungen ist es demnach auch folgerichtig, wenn in die Automation der Verwaltungsprozesse kräftig investiert wird. Dass sich andererseits das Gebot der Sparsamkeit dahingehend auswirkt, dass Investitionen in die informationstechnische Sicherheit eher zögerlich einsetzen, weil die für die Mittelbereitstellung zuständigen Stellen in der Verwaltung keine gesetzliche Notwendigkeit dafür sehen, wird in Abschnitt 3.5 näher beleuchtet. Hier dürfte es erst der Schaden sein, der die Verantwortlichen klug machen wird.

Der Senat misst der Gewährleistung eines sicheren IT-Einsatzes grundsätzlich einen hohen Stellenwert zu. Dazu werden die notwendigen anforderungsgerechten Sicherheitsmaßnahmen unter Berücksichtigung der bestehenden Haushaltssituation durchgeführt, so dass auf wirtschaftliche Weise mögliche Risiken bereits im Vorfeld ausgeschlossen bzw. auf ein akzeptables Maß begrenzt werden können.

Umsetzung der IT-Politik des Landes

Die Ziele der IT-Politik des Landes liegen im Einsatz moderner Informationstechnik zur Straffung von Verwaltungsabläufen, zur Personaleinsparung, zur Verbesserung der Arbeitsbedingungen der Mitarbeiter und der Verbesserung der Bürgernähe durch schnellere Bedienung, Reduzierung der Behördenwege und Intensivierung der Beratung. Diese Ziele lassen sich nur in kleinen, abgestimmten Schritten erreichen, denn die Einführung erfolgreicher IT-Verfahren ist nicht eine Frage der Investition von ohnehin knappen Geldern, sondern auch der sorgfältigen Planung, der abgestimmten Festlegung von Rahmenbedingungen und auch der Einhaltung gemeinsamer Absprachen. Die Umsetzung der IT-Politik obliegt dem zentralen IT-Management in der Senatsverwaltung für Inneres im Zusammenwirken mit dem *IT-Koordinations- und Beratungsausschuss* (IT-KAB), der IT-Manager aus Haupt- und Bezirksverwaltungen zusammenführt und der vom Landesbetrieb für Informationstechnik, dem Hauptpersonalrat, dem Rechnungshof und von uns beraten wird. Dieses Gremium beschließt die für die IT-Sicherheit erforderlichen Maßnahmen.

Neben den in der IT-Sicherheitsrichtlinie festgelegten jährlich wiederkehrenden Aufgaben des IT-KAB wie die Erstellung und Diskussion eines jährlichen IT-Sicherheitsberichts, die Beschließung eines jährlichen Umsetzungsplans IT-Sicherheit, die Fortschreibung der IT-Sicherheitsrichtlinie und der IT-Sicherheitsstandards standen Vorschläge zur *sicheren Kommuni-*

Die vom IT-Koordinierungsausschuss Berlin (IT-KAB)

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

kation im Berliner Landesnetz zur Debatte. Dabei ging es u. a. um den Einsatz von Anti-Spam-Filtern im Grenznetz des Berliner Landesnetzes zum Internet, die die überbordende Flut unerwünschter E-Mails eindämmen können. Behörden sollen die Wahl haben, ob sie an der einheitlichen Filterung teilhaben wollen oder ob sie ganz darauf verzichten wollen. Behördenspezifische Spam-Filter sind derzeit im Grenznetz nicht möglich. Eine große Schwachstelle besteht darin, dass bestimmte IT-Verfahren von der Funktionsfähigkeit bestimmter Kommunikationsprotokolle und –dienste abhängig sind, die an den dezentralen Firewalls im Landesnetz freigeschaltet werden müssen, so dass die Firewalls hinsichtlich dieser Protokolle und Dienste keine Schutzwirkung mehr entfalten und somit die behördenspezifischen Sicherheitskonzepte unterlaufen werden können.

beschlossenen Regelungen zur sicheren Kommunikation werden derzeit umgesetzt. Im Landesbetrieb für Informationstechnik ist ein zentraler „Spam-Filter“ eingerichtet, der unerwünschte E-Mails aus dem Internet abfangen kann.

Im Vordergrund der IT-politischen Bemühungen des Landes steht – wie auch z. B. die bereits genannten „kleinen Schritte” aufzeigen – die *Vereinheitlichung der IT-Infrastrukturen des Landes*. Auch dazu wurde ein Hearing veranstaltet, welches Erfahrungen aus anderen Bundesländern und von Unternehmen der IT-Branche zusammenbrachte. Eine einheitliche IT-Infrastuktur, von der bisher bestenfalls in den vom LIT betreuten zentralen Infrastrukturkomponenten gesprochen werden kann, würde die Transparenz und Revisionsfähigkeit (Nachvollziehbarkeit) der Datenverarbeitung des Landes entscheidend verbessern, immerhin Kategorien, die als Sicherheitsziele explizit im aktuellen Berliner Datenschutzgesetz genannt werden (§ 5 Abs. 2 BlnDSG).

Der Senat betrachtet die Vereinheitlichung der IT-Infrastruktur als wesentliches Element für einen wirtschaftlichen und sicheren IT-Einsatz.

Zu den Aufgaben des IT-KAB gehört die Vorbereitung des Einsatzes der *Elektronischen Signatur* und des Aufbaus einer *Private Key-Infrastruktur (PKI*) in der Berliner Landesverwaltung. Dazu wurde der Landesbetrieb für Informationstechnik gebeten, ein Grundlagenpapier zu erarbeiten, das auch Lösungskonzepte für sichere E-mail- und Client-Server-Verbindungen sowie für rechtsverbindliche Online-Transaktionen beinhaltet. Der Einsatz der elektronischen Signatur ist nicht nur bedeutsam für die rechtsverbindliche, vertrauliche und authentische Kommunikation zwischen den öffentlichen Stellen des Landes (g2g – Government to Government), sondern auch für die im Rahmen des eGovernment anstehende Kommunikation zwischen den öffentlichen Stellen und Unternehmen (g2b – Government to Business) und Bürgern (g2c – Government to Citizens/Customers). Ambivalent ist derzeit die Diskussion, ob die elektronische Signatur den Anforderungen der fortgeschrittenen oder der qualifizierten Signatur nach dem Signaturgesetz entsprechen soll. Während für die fortgeschrittene Signatur, die geringeren Sicherheitsansprüchen genügt, ausschließlich kurzfristige Kostenargumente sprechen, spricht für die qualifizierte Signatur, dass nur sie – weil die Anbieter von Signaturdiensten einer strikten, staatlich anerkannten Zertifizierung unterliegen – auf längere Sicht zu

Wie im Bericht ausgeführt, ist derzeit die anwendungsorientierte Diskussion über die notwendigen Formen elektronischer Signatur, die im Verwaltungshandeln erforderlich und praxisgerecht sind, noch nicht abgeschlossen. Das Land Berlin beteiligt sich aktiv an der Diskussion, da vor dem übergreifenden Aufbau und Betrieb technischer Lösungen in der Berliner Verwaltung die fachlich-organisatorischen Randbedingungen für den Einsatz elektronischer Signatur abgestimmt sein müssen.

einer einheitlichen bundes- oder gar europaweiten Signaturinfrastruktur führen kann. Wer nur auf die fortgeschrittene Signatur setzt, nimmt in Kauf, dass diese nur in beschränkten Anwendungsbereichen (z. B. nur im Kontakt mit der Berliner Landesverwaltung) nutzbar sein wird.

Landesbetrieb für Informationstechnik

Ein weiteres wichtiges Thema ist die Zukunft des *Landesbetriebes für Informationstechnik (LIT)*. Es ist noch nicht so lange her, dass aus dem Landesamt ein Landesbetrieb wurde, der aus der Kameralistik entlassen wurde und nach kaufmännischen Prämissen geführt wird. Für die meisten Behörden als Kunden des LIT war es gewöhnungsbedürftig, nunmehr für die Dienstleistungen des LIT zur Kasse gebeten zu werden, wenngleich es nur um haushaltstechnische Umschichtungen ging. Sicher wäre es für die Sicherheit der Daten im Berliner Landesnetz vorteilhafter gewesen, wenn z. B. die Entscheidung für einen abgestimmten Einsatz von Verschlüsselungsprodukten „von oben" getroffen werden könnte, und es nicht den an das Landesnetz angeschlossenen Anwendern überlassen bliebe, ob sie die offenbar nicht „auf den Nägeln brennenden" Zusatzinvestitionen tragen wollen[38]. Zur zukünftigen Rechtsform für den LIT hat es ein Hearing gegeben, in dem die sehr unterschiedlichen Erfahrungen anderer Bundesländer vorgestellt wurden. Eine Entscheidung für das Berliner LIT liegt noch nicht vor.

In den laufenden Diskussions- und Abstimmprozessen zum Prozess der Weiterentwicklung des LIT werden auch die vom Berliner Beauftragten für Datenschutz und Informationsfreiheit aufgeworfenen Fragestellungen zur verbindlichen Nutzung von zentral bereit gestellten Dienstleistungen des LIT mit berücksichtigt. Im Übrigen ist darauf hinzuweisen, dass der IT-KAB einstimmig die Maßnahmen zum Schutz der Vertraulichkeit beschlossen hat und somit es nicht den Anwendern überlassen ist, ob sie den entsprechend geschützten (verschlüsselten) Zugang nutzen wollen. Die dezentrale Umsetzung der Maßnahmen muss gleichwohl haushaltsmäßig von den einzelnen Behörden abgesichert werden.

Wichtige Weichenstellungen für den IT-Einsatz in der Berliner Landesverwaltung erfolgen durch die Entwicklung und Befüllung eines *IT-Warenkorbes* für die Berliner Verwaltung. Der IT-Warenkorb enthält für die unterschiedlichen Produktgruppen (z. B. Betriebssysteme, Office-Pakete, Sicherheitsdienste, aber auch branchenspezifische Standardprodukte wie etwa geographische Informationssysteme) Software, deren Einsatz zur Vereinheitlichung der IT-Infrastruktur des Landes empfohlen wird und vom LIT unterstützt werden kann. Es werden solche Softwareprodukte aufgenommen, die bereits in einem größeren Umfang in der Verwaltung eingesetzt werden. Eine wichtige Entscheidung wurde mit der Aufnahme von *Open-Source-Produkten* getroffen, die als wichtiger Ausweg zur Entschärfung des Microsoft-Monopols in den wichtigsten Produktklassen gesehen werden, dies insbesondere im Hinblick auf die neue Lizenzpolitik des Branchenriesen, die als einschränkend und teuer empfunden wird.

Der IT-Warenkorb ist ein wichtiges Element in dem Prozess zur Vereinheitlichung der IT-Infrastruktur. Die Aufnahme von so genannten Open Source Produkten ist unter der bewussten Prämisse erfolgt, praxisgerechte und umsetzbare Alternativlösungen zum dominierenden Einsatz von Produkten der Fa. Microsoft zu finden, um die mit der in wesentlichen Teilen der IT-Infrastruktur bestehenden Abhängigkeit von einem Anbieter verbundenen Risiken zu verringern.

Ehrwürdige IT-Strukturen

Ein zunehmend drängenderes Problem stellt die Notwendigkeit dar, veraltete *Großverfahren* durch moder-

[38] Näheres dazu unter 3.5

ne, den Anforderungen der Informationssicherheit besser entsprechende Verfahren zu ersetzen. Die Verfahren haben zwar nach und nach moderne Hardwareumgebungen erhalten und sind an ihren „Rändern" aufgrund der neu zu bewältigenden Aufgaben um zusätzliche Funktionen oder gar Teilverfahren ergänzt worden, jedoch sie stehen samt und sonders auf einer teilweise lange veralteten Softwarebasis.

Das Landeseinwohneramt betreibt das Großverfahren *Einwohnerwesen – EWW* mit einer ein Vierteljahrhundert alten Software. Es wird daher mit großem Druck daran gearbeitet, mit EWW-neu ein aktuellen Ansprüchen genügendes Verfahren für die Meldebehörden einzuführen. Das Projekt steht in Bezug zur Automatisierung in den bezirklichen Bürgerbüros, die die Aufgaben der Meldebehörde übernommen haben. Zum Berliner Projekt Bürgerdienste haben wir im vorigen Jahr ausführlich berichtet[39]. Alle Überlegungen zur Neugestaltung des Einwohnerwesens, sei es die Einrichtung eines neuen Auskunftsportals für die Auskünfte an andere Behörden, seien es von der Bundesregierung geförderte Studien zum Aufbau *mobiler Bürgerdienste* (MoBüD), werden allerdings von dem seit Jahren bestehenden Rückstand bei der Anpassung des Berliner Landesmeldegesetzes an das Melderechtsrahmengesetz überschattet[40].

Die durch die Senatsverwaltung für Inneres noch zu leistende Umsetzung der Änderungen des Melderechtsrahmengesetzes in das Berliner Meldegesetz führt zu Verzögerungen bei der technischen Neugestaltung des Einwohnerwesens.
Siehe hierzu auch Tz. 4.2.1.

Auf der gleichen uralten Softwarebasis betreibt die Kraftverkehrsabteilung des Landeseinwohneramts auch das *KVA-Verfahren* zur Verwaltung des Bestandes der Kraftfahrzeuge und zur Erstellung der KfZ-Scheine und Briefe. Zwar werden uns wesentliche Ergänzungen des Verfahrens mitgeteilt (z. B. zur Ausgabe von Wunschkennzeichen, zur Durchführung der Erstversteuerung), von einer grundlegenden Modernisierung dieses Verfahrens ist jedoch noch nichts bekannt.

Mit der Inbetriebnahme des 1998 eingeführten neuen KVA-Programms, das sich in den Grundstrukturen und Möglichkeiten wesentlich vom Altverfahren unterscheidet, ist die Bearbeitung von Zulassungsangelegenheiten erheblich verbessert worden. So wurden u.a.

- die Arbeitsmasken bedienungsfreundlich gestaltet
- die bis dahin getrennten Verfahren „KVA2" und „Mikroverfilmung" zusammengeführt
- eine „Historie" geschaffen, die zur Arbeitserleichterung führt, weil damit die Zugriffe auf die Mikroverfilmung reduziert werden,
- die überwiegende Vordruckverwaltung ins Verfahren eingestellt und mit einzelnen Programmschritten verknüpft (Einstellung der manuellen Vordruckbeschaffung)
- eine automatisierte Wiedervorlagenverwaltung eingeführt,
- neue Programme geschaffen.

Das Verfahren „KVA-neu" ist zwischenzeitlich inhaltlich überarbeitet und mit der Einführung der Erst-

[39] JB 2001, 3.5

[40] vgl. 4.2.1

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

	versteuerung und des Steuerrückständeverfahrens am 01.01.2003 durch das Verfahren „EVV“ ersetzt worden. In der Planung befindet sich zur Zeit die Umstellung der Aktenarchivierung von Mikrofilm auf Bildplatte. Die Zulassungsbehörde Berlin verfügt damit über eine moderne und arbeitsgerechte Software, die zur Bewältigung ihrer zulassungsrechtlichen Aufgaben beiträgt.
Auch das polizeiliche Informationssystem *ISVB (Informationssystem Verbrechensbekämpfung)* des Polizeipräsidenten in Berlin weist ein ähnlich ehrwürdiges Alter auf wie das Verfahren EWW . Seit Jahren ist das Nachfolgeverfahren *POLIKS* in Planung und Entwicklung, ohne dass erkennbar ist, wann es das alte Verfahren ablösen kann.	Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat bereits in den Jahren 2000 und 2001 Informationen über den Zeitplan von POLIKS erhalten. Die damals angebotene Teilnahme am Begleitgremium POLIKS wurde vom Berliner Beauftragten für Datenschutz und Informationsfreiheit nicht realisiert. Die aktuelle Einladung der POLIKS-Projektleitung an den Berliner Beauftragten für Datenschutz und Informationsfreiheit zur nunmehr dritten Informationsveranstaltung im Mai 2003 enthält als Anlage das gerade fertiggestellte POLIKS-Sicherheitskonzept. POLIKS soll im April 2004 in den Echtbetrieb gehen.
Uralt ist auch das IT-Verfahren *BOWI* für die Bearbeitung der *Verkehrsordnungswidrigkeiten*. Dieses Verfahren sollte bereits vor Jahren durch das neue Verfahren BOWI II abgelöst werden, welches jedoch an den hohen technischen und rechtlichen Ansprüchen scheiterte, die mit der geplanten papierlosen Archivierung der Vorgänge in Verbindung standen. Inzwischen wird das Verfahren BOWI 21 geplant, bei dem schon die Bezeichnung zum Ausdruck bringen soll, dass ein IT-Verfahren in der Modernität des 21. Jahrhunderts eingeführt wird.	Nach Zustimmung des Hauptausschusses des Abgeordnetenhauses im September 2001 über eine außerplanmäßige Verpflichtungsermächtigung in Höhe von 42,539 Mio € zur Realisierung des Betriebes von BOWI 21 ist zwischen der Polizeibehörde und dem LIT eine Rahmendienstvereinbarung abgeschlossen worden. Hierzu ist das in Niedersachsen verwendete Programm über ein automatisiertes Bußgeldverfahren in die Berliner Strukturen implantiert worden. Der für Anfang 2003 vorgesehene Echtbetrieb konnte allerdings noch nicht aufgenommen werden, weil verschiedene Programmteile und die Anpassung der Hard- und Software an die um 7-fach höheren Berliner Fallzahlen zusätzliche Ergänzungen des Verfahrens erforderten. Zwischenzeitlich ist die Softwareanpassung bis auf die Komponente Gebührenverfahren aber abgeschlossen und wird jetzt erprobt. Ferner wurde nach Ausschreibung die Firma Siemens als Dienstleister für die Vorverarbeitung (Datenerfassung, Scannen, Indexieren) beauftragt. Auch die Auswahl für die Arbeitsplatzausstattung ist jetzt abgeschlossen. Darüber hinaus wurde das System für die Bildauswertung aus den Radarmessungen sowie der automatischen Verkehrsüberwachungskameras integriert und wird erprobt. Die stufenweise Aufnahme des Echtbetriebes von BOWI 21 ist jetzt im 2. Quartal 2003 vorgesehen.
Seit 1994 ist in Berlin das Berliner automatisierte *Sozialhilfe-Informationssystem BASIS I* auf der Grundlage der Standardsoftware *PROSOZ/S* in Betrieb. Über Sicherheitsprobleme dieses Verfahrens berichten wir an anderer Stelle[41]. Das Nachfolgeprojekt BASIS II	siehe Stellungnahme unter 4.4.3: Sozialdaten – Steht die technische Sicherheit noch auf einer guten BASIS?

[41] vgl. 4.4.3

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

bzw. BASIS 3000, welches nicht nur die Sicherheitsprobleme lösen, sondern auch die Funktionalitäten und den Bearbeitungskomfort wesentlich verbessern sollte, musste bereits im Jahr 2000 aufgegeben werden. Unter dem Kürzel *MOPS (**Mo**dernisierte Software **P**RO-**S**OZ/S für Windows)* wurde dann eine Übergangslösung eingeführt, die den Bearbeitungskomfort verbesserte, die Betriebssystemumgebung modernisierte, die Sicherheitsprobleme aber noch verschärfte. Es ist ganz offensichtlich, dass damit noch keine zukunftsweisende Lösung gefunden wurde.

Im Bereich der Jugendhilfe ist unter den gleichen Voraussetzungen die Standardsoftware *PROSOZ/J* im Einsatz. Hier ist jedoch festzustellen, dass sich bei der Senatsverwaltung für Jugend, Bildung und Sport das Projekt *ISBJ (Informationssystem Berliner Jugendhilfe)* derzeit im Planungsstadium befindet, welches dann PROSOZ/J ablösen soll. Über die weitere Entwicklung dieses Großverfahrens werden wir weiter berichten, weil wir uns in die datenschutzrechtlich notwendige Vorabkontrolle eingeschaltet haben.

Das Projekt ISBJ - Integrierte Software Berliner Jugendhilfe - hat zum Ziel, alle IT-Fachverfahren im Jugendbereich hinsichtlich Effizienz, Sicherheit und Kompatibilität untereinander zu überprüfen und in der Folge weiterzuentwickeln bzw. zu ersetzen. In diesem Zusammenhang ist auch die Ablösung von ProSoz/J absehbar.

ISBJ ist kein (monolithisches) Großverfahren, sondern ein Softwaresystem aus zahlreichen Teilverfahren, welche teilweise schon existieren oder in den nächsten Jahren neu entwickelt werden. Erste Ausschreibungen befinden sich momentan unmittelbar vor der Bekanntgabe.

3. Schwerpunkte im Berichtsjahr

3.1 Sensitive Daten

Seit der Umsetzung der Europäischen Datenschutzrichtlinie[42] durch das Bundesdatenschutzgesetz 2001 verfügt nunmehr auch das deutsche Datenschutzrecht über eine Kategorie personenbezogener Daten, die besonderen Verarbeitungsvoraussetzungen unterliegen. Das BDSG selbst nennt sie bürokratisch „besondere Arten personenbezogener Daten". Im Allgemeinen werden sie „sensible" oder – richtiger – *„sensitive" Daten* genannt. Es handelt sich dabei um Angaben, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit der Betroffenen hervorgehen, sowie um Angaben zu Gesundheit oder Sexualleben (Art. 8 Abs. 1 Datenschutzrichtlinie, § 3 Abs. 9 BDSG, § 6 a Abs. 1 BlnDSG).

Einen Teil personenbezogener Daten aufgrund ihrer Art bestimmten Verarbeitungsanforderungen zu unterwerfen, war dem deutschen Datenschutzrecht bisher fremd. Nach bislang einhelliger Auffassung bestimmte sich die Sensitivität von Daten weniger nach ihrer Art, sondern war vielmehr abhängig vom konkreten Kontext der Datenverarbeitung. Eine Vielzahl von Mitgliedstaaten der Europäischen Union hatte jedoch von

Ziffer 3.1 befasst sich – mit Ausnahme der Ausführungen zum Versicherungsombudsmann – mit allgemeinen Fragen von Auslegung und Anwendung des Bundesdatenschutzgesetzes (insbesondere mit §§ 4a und 28 BDSG), ohne dass konkrete Beispiele mit Bezug zur Berliner Verwaltung genannt werden, die sich aus der Tätigkeit des Berliner Beauftragten für Datenschutz und Informationsfreiheit im Berichtsjahr ergeben haben. Der Senat sieht daher keine Veranlassung, diese allgemeinen Ausführungen zu kommentieren.

[42] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG L 281

Anbeginn ihrer datenschutzrechtlichen Gesetzgebung eine besondere Behandlung sensitiver Daten vorgesehen, wobei die Definition, welche Angaben hierzu zu zählen seien, durchaus unterschiedliche Akzente setzte. Bereits die Europarats-Konvention[43] verfügte über einen Katalog besonderer Arten von Daten, deren automatische Verarbeitung nur zulässig sein sollte, wenn das innerstaatliche Recht einen geeigneten Schutz gewährleistet (Art. 8). Erwägungsgrund 11 der Richtlinie erwähnt ausdrücklich dieses Übereinkommen des Europarats und hält fest, dass sie die im Übereinkommen zum Schutz der Personen enthaltenen Grundsätze konkretisiert und erweitert.

Die EU-einheitliche Normierung sensitiver Daten ändert jedoch nichts an der Tatsache, dass der Grad der Sensitivität aufgrund der gesellschaftlichen und historischen Rahmenbedingungen des jeweiligen Mitgliedsstaates unterschiedlich ist. Überdies machen die folgenden Ausführungen deutlich, dass die rechtlichen Vorgaben des BDSG zu sensitiven Daten im täglichen Umgang mit dem Datenschutzrecht einer Konkretisierung und Ausgestaltung bedürfen, um eine praxisbezogene Anwendung des Rechts zu gewährleisten.

Unübersehbar ist jedoch, dass die Verarbeitung der in § 3 Abs. 9 BDSG bzw. § 6 a Abs. 1 BlnDSG genannten Datenarten ein besonderes Risiko für die Betroffenen birgt. Anders als bei allgemeinen Angaben zur Person liegt in ihrer missbräuchlichen Nutzung ein besonderes Diskriminierungspotenzial. Überdies können sie tief gehende Rückschlüsse auf die Privat- oder Intimsphäre der Betroffenen geben. Ihre ausdrückliche Definition im Gesetz kann daher zunächst auch zu einer wünschenswerten Sensibilisierung nicht nur der juristischen Fachwelt, sondern auch der Allgemeinheit führen.

Bei der Frage, ob es sich bei einer bestimmten Information um ein sensitives Datum handelt, gibt es Abgrenzungsprobleme. Noch unproblematisch ist, dass nicht nur die Asthmaerkrankung, sondern auch der Besuch bei einem Lungenarzt ein sensitives Datum ist, obwohl dieser Besuch möglicherweise nur der Vorsorge diente. Auch die Mitgliedschaft im Organ einer Stiftung wie der Heinrich-Böll-Stiftung stellt ein sensitives Datum dar, da hieraus zumindest auf eine politische Nähe zu Bündnis 90/Die Grünen geschlossen werden kann. Teilweise ist aber fraglich, ob bestimmte Daten in den Anwendungsbereich der sensitiven Daten fallen:

In der Regel stellen der Name und die Anschrift kein sensitives Datum dar. Allerdings wird man bei einem Vornamen wie Mohammed mit großer Wahrscheinlichkeit davon ausgehen können, dass der Namensträger Moslem ist, bei dem Nachnamen Ashkenasi spricht

[43] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108 vom 28. Januar 1981)

vieles dafür, dass der Betroffene Jude ist, zumindest, dass er jüdische Vorfahren hat. Bei der Adresse eines betreuten Wohnmodells von Drogenabhängigen bzw. ehemaligen Drogenabhängigen kann auf die Gesundheit der Bewohner geschlossen werden. Der Geburtsort Nairobi deutet darauf hin, dass der Betroffene Farbiger ist. Anhand eines Passbildes ergibt sich nicht nur die ethnische Zugehörigkeit, eine Brille verrät auch Defizite bei der Sehstärke.

Nach einer Auffassung sollen Daten, aus denen nur mit einer statistischen Wahrscheinlichkeit auf Angaben zu den genannten besonderen Kategorien personenbezogener Daten geschlossen werden kann, nicht zu sensitiven zählen[44]. Dieser Auslegung ist zwar zuzustimmen, sie ist aber nicht ausreichend, um die Mehrzahl der genannten personenbezogenen Daten aus dem Anwendungsbereich der besonderen Daten herauszunehmen. Allen diesen Daten ist gemein, dass sie selbst (Name, Adresse usw.) nicht als sensitiv zu bewerten sind, es handelt sich im Gegenteil um Grunddaten, die von den verschiedensten verantwortlichen Stellen benötigt werden. Würde man bei diesen Grunddaten die Datenverarbeitung nach § 4 a Abs. 3 und § 28 Abs. 6 ff. BDSG einschränken, würde dies zu einem wenig praktikablen Ergebnis führen. Es erscheint deshalb sachgerecht, diese Daten nicht als sensitive Daten zu betrachten, sofern die verantwortliche Stelle sie ohne Bezug auf einen etwaigen sensitiven Kern erhebt, verarbeitet oder nutzt und die Sensitivität des Datums für die verantwortliche Stelle zufällig ist (das Autohaus hat einen Kunden Namens Ashkenasi, der Pizzaservice liefert in ein betreutes Wohnhaus für Drogenabhängige etc.). Die einschränkenden Vorgaben für sensitive Daten finden erst Anwendung, wenn die verantwortliche Stelle gespeicherte Grunddaten auf „sensitive Reflexe" untersucht. So wäre etwa bei einer Werbeaktion einer Bank, bei der Kunden mit islamischen Namen auf spezielle Fonds für Moslems (Fonds, die nach den religiösen und ethischen Vorgaben des Islam z. B. hinsichtlich der Zinseinkünfte verwaltet werden) hinweist, als eine Nutzung sensitiver Daten zu würdigen, die ohne Einwilligung des Betroffenen nicht rechtmäßig wäre.
Anders als bei „normalen Daten" setzt eine wirksame *Einwilligung* zur Erhebung, Verarbeitung oder Nutzung besonderer Arten personenbezogener Daten voraus, dass sich die Einwilligung ausdrücklich auf diese Daten bezieht. Bei sensitiven Daten kommt danach eine konkludente Einwilligung des Betroffenen zur Erhebung, Verarbeitung oder Nutzung nicht in Betracht. Allerdings schließt § 4 a Abs. 3 BDSG die mündliche Einwilligung nicht aus, soweit wegen besonderer Umstände eine andere Form als die Schriftform angemessen ist (vgl. § 4 a Abs. 1 Satz 3 BDSG, der auch bei sensitiven Daten anwendbar ist)[45]. Danach

[44] vgl. Dammann, Ulrich; Simitis, Spiros: EG-Datenschutzrichtlinie. Baden-Baden: Nomos, 1997, Art. 8, Rdn. 2.7

[45] anderer Ansicht allerdings Gola, Peter; Schomerus, Rudolf: BDSG. München: C. H. Beck, 2002, § 3, Rdn. 57

ist auch weiterhin eine telefonische Meinungsbefragung zu politischen Themen möglich, sofern der Interviewer ausdrücklich auf die Abfrage sensitiver Daten hingewiesen und der Betroffene insoweit eine Einwilligung gegeben hat.

Bei der Verarbeitung sensitiver Daten sind die verantwortlichen Stellen in einem größeren Umfang verpflichtet, sich für die Erhebung, Verarbeitung und Nutzung dieser Daten die Einwilligung des Betroffenen zu beschaffen, da diese nur nach den engen Vorgaben des § 28 Abs. 6 ff. BDSG auf eine gesetzliche Rechtsgrundlage gestützt werden können. So kann sich die verantwortliche Stelle nicht darauf berufen, dass das sensitive Datum für die Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen erforderlich ist (vgl. § 28 Abs. 1 Nr. 1 BDSG für „normale" Daten). Nach § 28 Abs. 6 Nr. 3 BDSG ist die Erhebung, Verarbeitung und Nutzung sensitiver Daten zulässig, wenn dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt. § 28 Abs. 6 Nr. 3 BDSG ermöglicht somit die gerichtliche und außergerichtliche Geltendmachung von rechtlichen Ansprüchen, die die Verarbeitung sensitiver Daten voraussetzt, sofern kein überwiegendes schutzwürdiges Interesse des Betroffenen erkennbar ist. Nr. 3 setzt Art. 8 Abs. 2 e der EG-Datenschutzrichtlinie um. Hierdurch soll gewährleistet sein, dass verantwortliche Stellen an der Durchsetzung rechtlicher Ansprüche, für die die Verarbeitung sensitiver Daten erforderlich ist, nicht gehindert werden. Nach dieser ratio legis findet Nr. 3 keine Anwendung, wenn es um die Durchsetzung rechtlicher Ansprüche eines Dritten, der in keiner Beziehung zur verantwortlichen Stelle steht, oder um Ansprüche des Betroffenen selbst geht. Insoweit ist der Anwendungsbereich von § 28 Abs. 6 Nr. 3 BDSG stark eingeschränkt.

In verschiedenen denkbaren Konstellationen übersenden Betroffene an verantwortliche Stelle Unterlagen, die sensitive Daten enthalten. Dem Absender geht es regelmäßig darum, dass der Empfänger diese Daten zur Kenntnis nimmt und aufgrund der daraus gewonnenen Erkenntnisse Schritte unternimmt, die dem Interesse des Absenders dienen. Eine ausdrückliche Einwilligung in die Verarbeitung dieser Daten, wie sie bei wörtlicher Anwendung von § 4 a Abs. 3 BDSG zu fordern wäre, liegt in der Regel nicht vor. Typisches Beispiel für eine solche Konstellation ist die Übersendung von Gesundheitsdaten an den *Versicherungsombudsmann*[46] mit der Bitte, Streitigkeiten zwischen der Versicherung und dem Versicherungsnehmer zu klären. Hier kann sich der Versicherungsombudsmann

[46] vgl. 4.6.1

nicht auf § 28 Abs. 6 Nr. 3 BDSG berufen, da Ansprüche des Versicherungsnehmers überprüft werden.

Die unaufgeforderte Zusendung sensitiver Daten durch den Betroffenen selbst, deren Kenntnisnahme durch den Empfänger mit der Übersendung offensichtlich beabsichtigt und gewollt ist, genügt den Anforderungen an die Einwilligung nach § 4 a Abs. 3 BDSG. Daher können diese Daten vom Empfänger gespeichert werden. Zur weiteren Nutzung dieser Daten durch den Empfänger sollte der Datenverarbeiter aber den Betroffenen schriftlich auf die vorgesehene Art der Verarbeitung oder Nutzung der Daten nach § 4 Abs. 1 BDSG hinweisen.

Sollen die Daten im Rahmen der weiteren Verarbeitung an Dritte übermittelt werden - beispielsweise zur Klärung einer Zahlungspflicht der Versicherung -, ist die unaufgeforderte Übersendung der Daten nicht als Einwilligung im Sinne des § 4 a Abs. 3 BDSG zu sehen. Vielmehr bedarf es zu einer solchen Übermittlung einer ausdrücklichen Einwilligung des Betroffenen, die auf Grundlage einer Unterrichtung und in Schriftform zu erfolgen hat (§ 4 a Abs. 3, Abs. 1 S. 2 BDSG). Eine Übermittlung von sensitiven Daten an die Versicherung erscheint allerdings noch ohne ausdrückliche Einwilligung des Betroffenen möglich zu sein, sofern sich aus den dem Ombudsmann vorliegenden Dokumenten ergibt, dass die Versicherung selbst die sensitiven Daten des Betroffenen gespeichert hat. Übermittelt der Betroffene sensitive Daten Dritter (z. B. ein Haftpflichtfall mit Personenschaden, bei dem der Betroffene als Schädiger in Anspruch genommen wird), sollten die sensitiven Daten des Dritten möglichst umgehend geschwärzt werden.

In einem besonders großen Umfang werden sensitive Daten bei der Begründung und Durchführung eines *Arbeitsverhältnisses* erhoben, verarbeitet und genutzt. Bereits im Bewerbungsverfahren kann nach gesundheitlichen Einschränkungen hinsichtlich des konkret ins Auge gefassten Arbeitsplatzes oder nach einer Schwerbehinderung, aus der sich Verpflichtungen des künftigen Arbeitgebers ergeben, gefragt werden. Kirchenzugehörigkeit oder Gewerkschaftsmitgliedschaft ist bei entsprechenden Tendenzbetrieben regelmäßig Einstellungsvoraussetzung. In einem bestehenden Arbeitsverhältnis erhält der Arbeitgeber Informationen über Erkrankungen seiner Mitarbeiter, muss hinsichtlich einer tariflichen Vergütung über eine Gewerkschaftsmitgliedschaft in Kenntnis gesetzt werden oder erfährt durch die Vorlage der Steuerkarte von einer möglichen Kirchenzugehörigkeit seiner Mitarbeiter.

Das Verbot der Verarbeitung sensitiver Daten gilt nach Art. 8 Abs. 2 b Richtlinie nicht, wenn die Verarbeitung erforderlich ist, um den Rechten und Pflichten des Arbeitgebers Rechnung zu tragen. Einen solchen Ausnahmetatbestand mit einem ausdrücklichen Bezug zum Arbeitsrecht sucht man im BDSG vergeblich. Nach

einhelliger Auffassung kann angesichts des besonderen Abhängigkeitsverhältnisses der Arbeitnehmer vom Arbeitgeber die Verarbeitung sensitiver Daten im Arbeitsverhältnis auch nicht auf die Einwilligung der Betroffenen gestützt werden, da die Freiwilligkeit der Einwilligung in diesem Fall grundsätzlich in Frage gestellt werden muss.

Da sensitive Arbeitnehmerdaten in der Regel vornehmlich zur Umsetzung von Arbeitnehmerrechten verarbeitet werden, können Arbeitnehmerdaten in der Regel nur dann verarbeitet werden, wenn nach § 28 Abs. 6 Nr. 3 BDSG auch Informationen zur Klärung von gegen die verantwortliche Stelle gerichteten Ansprüchen erhoben und verarbeitet werden dürfen[47]. Dies kann zumindest dann angenommen werden, wenn man als Reflex aus dem Recht des Arbeitnehmers – möglicherweise eingeschränkte – Rechte des Arbeitgebers herleiten kann. Der Gesundheitszustand des Arbeitnehmers bestimmt den Anspruch des Arbeitgebers auf Abrufung der Arbeitsleistung. Ähnliches gilt für Schwerbehinderungen.

Nach der Rechtsprechung der Arbeitsgerichte kommt es bei der Abfrage von sensitiven Daten vor Vertragsabschluss darauf an, ob ein potenzieller Arbeitgeber, der sensitive Daten erhebt, um zum Vorteil seines Gewerbebetriebs die richtige Personalentscheidung zu treffen, sein grundrechtlich geschütztes Recht auf Gewerbefreiheit ausübt.

§ 28 Abs. 3 Nr. 3 BDSG privilegiert die Nutzung und Übermittlung personenbezogener Daten für Zwecke der *Werbung*. Demgegenüber enthalten § 28 Abs. 6 ff. BDSG keine entsprechende Vorschrift. Der Verkauf sensitiver Daten für Werbezwecke – etwa durch einen Verein zur Förderung von Gehbehinderten an einen Rollstuhlverkäufer – wäre somit rechtswidrig. Auch der Verkauf dieser Daten ohne Angabe des sensitiven Datums wäre unzulässig, da zumindest für den Aufkäufer dieser Daten der sensitive Charakter noch ersichtlich wäre. Das Werbeverbot gilt auch für die Nutzung sensitiver Daten zu eigenen Werbezwecken. Ist aufgrund einer Rechtsvorschrift oder einer ausdrücklichen Einwilligung die Datenverarbeitung im operativen Geschäft gestattet, so muss im Einzelfall überprüft werden, ob eine Information an den Betroffenen sich noch im Rahmen des operativen Geschäfts bewegt oder schon eine unzulässige Nutzung sensitiver Daten zu Werbezwecken darstellt. So würde in dem Verein zur Förderung von Gehbehinderten die Information über neue Serviceangebote noch ins operative Geschäft fallen, nicht jedoch der Aufruf zu einer Spende. Fraglich ist, ob ein sensitiver Datenbestand für Werbezwecke benutzt und verarbeitet werden kann, wenn sensitive Daten mit nichtsensitiven Daten gemischt werden,

[47] vgl. Gola, Peter: Die Erhebung und Verarbeitung „besonderer Arten personenbezogener Daten" im Arbeitsverhältnis. In: RDV 3/2001, S. 125, 127

also etwa in einem Verein zur Förderung von Gehbehinderten die Daten der Kunden (Gehbehinderten) mit den personenbezogenen Daten von Nichtgehbehinderten wie Fördermitgliedern und Interessenten (Herauswaschen des sensitiven Datums). Auch wenn dieser Weg noch gangbar erscheint, haben wir einem Verein zur Förderung von Gehbehinderten geraten, sich eine Einwilligung von seinen Kunden in die Nutzung und Übermittlung ihrer Daten für Werbezwecke geben zu lassen.

Tatbestandsvoraussetzung des § 28 Abs. 6 Nr. 1 BDSG ist, dass die Verarbeitung zum *Schutz lebenswichtiger Interessen* des Betroffenen oder eines Dritten erforderlich ist und der Betroffene aus psychischen oder rechtlichen Gründen, z. B. Bewusstlosigkeit, schwere psychische Störungen etc., nicht in der Lage ist, seine Einwilligung zu geben. Das Gleiche gilt, wenn der Betroffene aus sonstigen tatsächlichen Gründen nicht um seine Einwilligung gebeten werden kann, etwa weil er sich auf einer Weltreise befindet oder unbekannt verzogen ist[48]. Der Anwendungsbereich von Nr. 1 ist dadurch eingeschränkt, dass die psychischen und rechtlichen Gründe ursächlich dafür sein müssen, dass keine Einwilligung nach § 4 a Abs. 3 BDSG vorliegt, der Betroffene ohne die Hinderungsgründe ansonsten seine Einwilligung erteilt hätte (mutmaßliche Einwilligung)[49]. Zu Wertungswidersprüchen mit anderen Gesetzen führt, dass Abs. 6 Nr. 1 lebenswichtige Interessen des Betroffenen oder eines Dritten von dem mutmaßlichen Willen des Betroffenen abhängig macht.

Falls durch die Nichtübermittlung des sensitiven Datums eine gemeine Gefahr entsteht, kann die Nichtübermittlung des sensitiven Datums eine unterlassene Hilfeleistung nach § 323 c StGB darstellen. Ein Arzt, der die Aidserkrankung eines uneinsichtigen Patienten mit häufig wechselndem ungeschütztem Geschlechtsverkehr übermittelt, leistet Hilfe zur Abwendung einer gemeinen Gefahr. Selbst wenn die Nichtübermittlung der sensitiven Daten nicht als unterlassene Hilfeleistung gewertet werden kann, liegt eine rechtswidrige Verletzung des Privatgeheimnisses dann nicht vor, wenn die Datenübermittlung nach § 34 StGB in rechtfertigendem Notstand zur Abwehr der dort genannten Rechtsgüter erfolgte. Aufgrund der Einheit der Rechtsordnung sollten deshalb über den Anwendungsbereich des § 28 Abs. 6 Nr. 1 BDSG hinaus Übermittlungen sensitiver Daten dann nicht als rechtswidrig betrachtet werden, soweit die verantwortliche Stelle sich auf § 34 StGB berufen kann bzw. die Nichtübermittlung nach § 323 c StGB als unterlassene Hilfeleistung gewertet werden würde. Überdies kann die Verarbeitung sensitiver Daten zum Schutz lebenswichtiger Interessen des

---

[48] vgl. Berliner Beauftragter für Datenschutz und Informationsfreiheit/Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Materialien zum Datenschutz Nr. 30: Neuregelungen im Bundesdatenschutzgesetz. Berlin 2001, S. 28

[49] vgl. Dammann/Simitis, a. a. O., Art. 8, S. 165

Betroffenen auch auf § 28 Abs. 8 Satz 2 BDSG gestützt werden, sofern dadurch eine erhebliche Gefahr für die öffentliche Sicherheit abgewehrt wird.

§ 28 Abs. 6 Nr. 2 erlaubt das Erheben, Verarbeiten und Nutzen sensitiver Daten, wenn diese vom Betroffenen *offenkundig öffentlich* gemacht worden sind. Nicht ausreichend ist, dass die Daten allgemein zugänglich sind, wie dies in § 28 Abs. 1 Nr. 3 BDSG für andere personenbezogene Daten vorgesehen ist. Vielmehr muss die Öffentlichkeit der Daten auf einer eigenständigen Entscheidung des Betroffenen beruhen. Dieser Tatbestand muss überdies offenkundig sein, mithin dürfen Zweifel daran, dass der Betroffene selbst die Daten öffentlich gemacht hat, nicht bestehen. Bei Meldungen in den Medien kann von einer Offenkundigkeit im Sinne von § 28 Abs. 6 Nr. 2 BDSG nicht automatisch ausgegangen werden. Anders verhält es sich, wenn sensitive Daten in einem Interview durch den Betroffenen selbst öffentlich gemacht werden, oder gar im Rahmen einer Selbstdarstellung à la Big Brother.

Organisationen, die politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtet sind, verarbeiten aus der Natur der Sache heraus sensitive Daten, insbesondere ihrer Mitglieder. Daten zur Kirchenmitgliedschaft geben Auskunft über die religiöse Einstellung der Betroffenen, auf die politische Meinung einer Person kann geschlossen werden, wenn sie in der Mitgliederdatenbank einer politischen Partei aufgeführt ist, aus den Mitgliederverzeichnissen von Gewerkschaften geht per se die Gewerkschaftszugehörigkeit der Betroffenen hervor. Um diesen Organisationen die Datenverarbeitung im Rahmen ihrer Tätigkeit zu ermöglichen, sieht § 28 Abs. 9 BDSG besondere Verarbeitungsbefugnisse vor. Die Erhebung, Verarbeitung oder Nutzung sensitiver Daten ist danach zulässig, soweit dies für die Tätigkeit der Organisation erforderlich ist.

Daneben gibt es Vereinigungen, die aufgrund ihrer Tätigkeit in großem Umfang sensitive Daten verarbeiten müssen, ohne eine Rechtsgrundlage nach § 28 Abs. 6 ff. BDSG zu haben. Ein Verein, der sich zum Ziel gesetzt hat, die Mobilität von Gehbehinderten durch entsprechende Hilfsangebote zu verbessern, ist weder ein Medizinischer Dienst nach § 28 Abs. 7 BDSG noch eine Organisation nach § 28 Abs. 9 BDSG. Soweit der Verein keine eigenen Rechtsansprüche geltend macht (§ 28 Abs. 6 Nr. 3 BDSG), benötigt er für sein operatives Geschäft die ausdrückliche Einwilligung der Gehbehinderten in die Verarbeitung ihrer sensitiven Daten (§ 4 a Abs. 3 BDSG). Es ist nicht zu verkennen, dass dies zu einem nicht unerheblichen bürokratischen Aufwand führt.

Ob eine Datenverarbeitung im Rahmen der Tätigkeit einer Organisation i. S. v. § 28 Abs. 9 BDSG erfolgt, hängt von der Zielsetzung bzw. dem Zweck der Organisation ab. Bei eingetragenen Vereinen oder Stiftungen sind diese in einer Satzung festgehalten. Soweit die

Datenverarbeitung für die beschriebene politische, philosophische, religiöse oder gewerkschaftliche Zweck- bzw. Zielbestimmung erforderlich ist, ist sie nach § 28 Abs. 9 BDSG zulässig. Bei der Frage, ob sich eine Datenverarbeitung noch im Rahmen der operativen Tätigkeit einer Organisation bewegt, ergeben sich allerdings Schwierigkeiten. Die „Werbung" einer Gewerkschaft zur Teilnahme an einer Demonstration zum 1. Mai wie auch übliche Spendenaufrufe einer Partei sind zulässig. Nicht mehr operatives Geschäft – und somit auch nicht mehr im Rahmen von § 28 Abs. 9 BDSG zulässig – ist die Nutzung von Daten der Mitglieder einer Organisation, um diesen Gruppenversicherungsverträge oder Urlaubsreisen anzubieten.

Der Begriff der „Organisation" im Sinne von § 28 Abs. 9 BDSG ist nicht an eine juristische Person gebunden. Wenn beispielsweise eine Gewerkschaft, die als eingetragener Verein organisiert ist, neben diesem Verein eigenständige Untergruppierungen (Jugendorganisation, Bildungswerk, etc.) unterhält, sind diese als Teil der Gesamtorganisation zu sehen, soweit sie den grundsätzlichen gewerkschaftlichen Anliegen verpflichtet sind. Anders verhält es sich bei Einrichtungen einer solchen Organisation, die zwar im Interesse der Mitglieder tätig werden, den Rahmen der politischen, philosophischen, religiösen oder gewerkschaftlichen Tätigkeit jedoch verlassen. So gehört etwa ein von einer Partei oder Gewerkschaft betriebenes Reisebüro, das besonders günstige Reiseangebote für die Mitglieder bereithält, nicht mehr zur Organisation i. S. v. § 28 Abs. 9 BDSG. Eine Übermittlung von Mitgliederdaten durch die Organisation wäre unzulässig. Da die Tätigkeit eines solchen Reisebüros überdies einen Erwerbszweck verfolgt, käme § 28 Abs. 9 BDSG schon aus diesem Grunde nicht zum Zuge.

§ 28 Abs. 9 BDSG privilegiert die Verarbeitung personenbezogener Daten sowohl der Mitglieder der Organisation als auch von Personen, die im Zusammenhang mit dem Tätigkeitszweck der Organisation regelmäßig Kontakt zu ihr unterhalten. Ob die zweite Alternative, die auf die Nähe von Personen zu der Organisation abstellt, zur Anwendung kommt, hängt davon ab, ob aus der Art des Kontaktes auf ihre eigene Einstellung Rückschlüsse gezogen werden können. So sind die Daten eines Referenten, der regelmäßig bei Fortbildungsveranstaltungen einer Gewerkschaft auftritt, aber selbst nicht Mitglied dieser Gewerkschaft ist, nicht sensitiv und können im Rahmen der Vertragsabwicklung nach § 28 Abs. 1 Nr. 1 BDSG verarbeitet werden. Gleiches gilt auch für Personen, die regelmäßig im Rahmen von Werkverträgen für Parteien Werbematerialien erstellen oder andere Dienstleistungen erbringen. Sensitive Daten können wiederum vorliegen, wenn eine Person regelmäßig an Veranstaltungen einer politischen Stiftung teilnimmt oder von dieser regelmäßig Materialien anfordert. Soweit eine Organisation die Beschäftigung von der Mitgliedschaft oder zumindest von der persönlichen Identifikation mit ihren Zielen

abhängig macht, ist auch das Mitarbeiterdatum ein sensitives.

Nach § 28 Abs. 9 Satz 3 BDSG ist die Übermittlung sensitiver Daten an Personen oder Stellen außerhalb der Organisation nur zulässig, wenn hierzu die ausdrückliche *Einwilligung* der Betroffenen, die sich auf diese Daten bezieht, vorliegt (§ 4 a Abs. 3 BDSG). Diese Formulierung macht deutlich, dass auch in diesem Zusammenhang eine Organisation im Sinne von § 28 Abs. 9 BDSG nicht an den Begriff einer juristischen Person gebunden ist. So wäre die Übermittlung von Mitgliederdaten einer Landespartei an die Bundespartei zulässig, soweit die Mitgliedschaft auch zur Bundespartei gegeben ist. Anders verhält es sich, wenn dem Bundesverband einer Gewerkschaft lediglich die einzelnen Landesverbände als juristische Person angehören. Möchten diese die Mitgliederdaten an den Bundesverband übermitteln, so setzt dies die Einwilligung der Mitglieder voraus. Eine Übermittlung sensitiver Daten an Stellen außerhalb der Organisation ist ohne Einwilligung der Betroffenen generell unzulässig. Sollen die Teilnehmerdaten einer Fortbildungsveranstaltung einer Gewerkschaft an ein privat betriebenes Hotel übermittelt werden, so bedarf es der Einwilligung der Betroffenen, die mit der Anmeldung zu der Veranstaltung eingeholt werden sollte. Bei Rücküberweisungen von zuviel gezahlten Mitgliedsbeiträgen sollte auf den Hinweis auf dem Überweisungsträger verzichtet werden, dass es sich um Mitgliedsbeiträge handelt, weil insoweit eine Übermittlung der Angabe einer Gewerkschaftsangehörigkeit des Betroffenen an die Bank vorliegt. Ausnahmsweise ist die Übermittlung sensitiver Daten an Stellen außerhalb der Organisation zulässig, wenn dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat (§ 28 Abs. 9 Satz 4 i. V. m. Abs. 3 Nr. 2 BDSG).

3.2 Unternehmensregelungen als Garantie für den Datenschutz in Drittstaaten

Ein *Export von personenbezogenen Daten* in Länder außerhalb der Europäischen Union und der weiteren Staaten des Europäischen Wirtschaftsraums (Norwegen, Island, Liechtenstein) ist nur dann zulässig, wenn ein angemessenes Datenschutzniveau im datenimportierenden Land herrscht (Art. 25 Europäische Datenschutzrichtlinie, § 4 b Abs. 2 Satz 2 BDSG). Dieses Erfordernis erfüllen bis heute lediglich die Schweiz, Ungarn und (mit Einschränkungen) Kanada[50] . Ausnahmsweise kann jedoch ein Datenexport erfolgen, wenn einer der Ausnahmetatbestände des § 4 c Abs. 1 BDSG (vgl. Art. 26 Abs. 1 Europäische Datenschutz-

[50] ABl. EG vom 25. August 2000, L. 215/1, L 215/4; ABl. EG vom 4. Januar 2002, L 2/13

richtlinie) vorliegt oder wenn beim datenimportierenden Unternehmen ausreichende Datenschutzgarantien geschaffen werden.

Nach § 4 c Abs. 2 Satz 1 BDSG können sich diese Garantien „insbesondere aus Vertragsklauseln oder verbindlichen *Unternehmensregelungen* ergeben"[51]. Der bundesdeutsche Gesetzgeber hat also dem in der Europäischen Datenschutzrichtlinie[52] beispielhaft genannten Instrument der Vertragsklauseln ein weiteres hinzugefügt. Die verbindliche Unternehmensregelung soll dazu führen, innerhalb eines global tätigen Unternehmens mit Tochter- (oder auch Mutter-) Gesellschaften in Drittländern ohne angemessenes Datenschutzniveau ausreichende Datenschutzgarantien auch dort zu schaffen. Da das deutsche Datenschutzrecht keinen „Konzerndatenschutz" kennt, sind die weltweit tätigen (Teil-)Unternehmen eines Konzerns rechtlich als selbständige Einheiten zu betrachten. Nach § 3 Abs. 7 BDSG ist der in Deutschland ansässige Teil eines Unternehmens verantwortliche Stelle. Dritter ist jede Stelle außerhalb der verantwortlichen Stelle (§ 3 Abs. 8 BDSG). Dies bedeutet, dass auch zwischen selbständigen Teilunternehmen internationaler Konzerne die Weitergabe von Daten als Übermittlung i. S. v. § 3 Abs. 4 Satz 2 Nr. 3 BDSG anzusehen ist.

In der unternehmerischen Praxis wird anstelle des Begriffs „verbindliche Unternehmensregelung" gern und häufig der Begriff *„Code of Conduct"* genutzt, obgleich dies bei wörtlicher Übersetzung eher einem Verhaltenskodex oder einer Verhaltensregel gleichkommt. Diesen Begriff gebraucht das BDSG in § 38 a allerdings in einem anderen Zusammenhang und meint damit branchenspezifische Regelungen zum Datenschutz in einem bestimmten Sektor, beispielsweise innerhalb eines Berufsverbandes. Derartige Verhaltensregeln beinhalten nicht notwendigerweise Regelungen für den internationalen Datentransfer, erfordern andererseits aber einen „branchenspezifischen Mehrwert" an Datenschutz.

Problematisch ist die Rechtsnatur einer Unternehmensregelung. Da sie regelmäßig nicht als Vertrag des Mutterunternehmens mit den Tochtergesellschaften ausgestaltet ist, kann sie auch nicht als Vertrag zugunsten Dritter angesehen werden (aus dem der Betroffene unmittelbar eigene Rechte herleiten könnte). Dies ist jedoch kaum von Bedeutung. Für die Verbindlichkeit ist vielmehr maßgeblich, dass die Unternehmensregelung als Handlungsanweisung des Arbeitgebers gegenüber den Arbeitnehmern ausgestaltet wird. Die Unternehmensteile und alle Mitarbeiter müssen verpflichtet sein, die Unternehmensregelung einzuhalten. Dies sollte durch innerbetriebliche Disziplinarmaßnahmen

[51] vgl. bereits JB 2001, 4.7 Datenübermittlungen ins Ausland

[52] Art. 26 Abs. 2

umgesetzt werden (praktische Verbindlichkeit). Daneben ist jedoch erforderlich, dass die Unternehmensregelung rechtlich durchsetzbare Verpflichtungen der Unternehmensteile und rechtlich durchsetzbare Rechte der Betroffenen, deren Daten übermittelt werden, beinhalten (rechtliche Verbindlichkeit).

Die Form einer Unternehmensregelung sollte von den Gegebenheiten im Unternehmen, z. B. von der Art und Anzahl der unternehmerischen Aktivitäten und der Anzahl der Länder, in denen das Unternehmen Niederlassungen hat, abhängig gemacht werden. Ihre Ausgestaltung kann derart erfolgen, dass sie einen Mindestdatenschutzstandard vorsieht, den einzelne Unternehmensteile je nach Standort verschärfen dürfen. Das bietet sich an, wenn ein internationaler Konzern ein weltweit einheitliches Datenschutzniveau in allen Konzernniederlassungen anstrebt, unabhängig davon, ob die Daten aus den Unternehmensteilen in der Europäischen Union in Drittländer übermittelt werden oder aus anderen Drittländern übermittelt oder nur dort erhoben und verarbeitet werden. Dann könnte über den festgelegten Mindestdatenschutzstandard hinaus in einem weiteren Papier der europäische Mehrwert für Datenübermittlungen aus dem europäischen Raum festgelegt werden. Denkbar ist auch die Aufspaltung der Unternehmensregelung in einen allgemeinen Teil mit für alle Situationen geltenden Prinzipien und einen besonderen, bereichsspezifischen Teil, der Sonderanforderungen je nach Regelungsbereich z. B. für Personal-, Finanz- oder Gesundheitsdaten beinhaltet. Ein Unternehmen kann als weitere Möglichkeit mehrere Unternehmensregelungen für einzelne Datenarten, z. B. Personaldaten einerseits, Kundendaten andererseits, schaffen[53].

Eine Unternehmensregelung muss die inhaltlichen Anforderungen erfüllen, die sich aus der Europäischen Datenschutzrichtlinie bzw. dem jeweiligen nationalen Datenschutzrecht ergeben. Dabei wird häufig verkannt, dass wesentlicher Regelungsgegenstand weniger die Kriterien für eine zulässige Datenübermittlung in Drittländer sind, denn diese Kriterien werden durch die Europäische Datenschutzrichtlinie vorgegeben. Wichtiger ist, dass mit der Unternehmensregelung ausreichende Datenschutzgarantien für die Verarbeitung im Drittland gegeben werden. Dabei sind die Kriterien zu berücksichtigen, die die Art. 29-Datenschutzgruppe in ihrem Arbeitspapier WP 12 vom 27. Juli 1998 entwickelt hat[54].

Die wesentlichen Grundsätze sind

- der Grundsatz der Beschränkung der *Zweckbe-*

[53] so die Codes of Conduct der DaimlerChrysler AG; vgl. 4.7 und Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2002", S. 38

[54] „Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Art. 25 und 26 der Datenschutzrichtlinie der EU", vgl. Anlagenband „Dokumente zum Datenschutz 1998", S. 29 ff.

stimmung (keine Zweckerweiterung nach Übermittlung der Daten, es sei denn, dies ist mit der Zweckbestimmung der Übermittlung nicht unvereinbar);

- der Grundsatz der *Datenqualität* und *Verhältnismäßigkeit* (die Daten müssen sachlich richtig und aktuell und dürfen im Hinblick auf die Zweckbestimmung nicht exzessiv sein);

- der Grundsatz der *Transparenz* (der Betroffene ist über die Zweckbestimmung der Verarbeitung und die Identität des Datenimporteurs aufzuklären);

- der Grundsatz der *Sicherheit* (insbesondere sind die Daten vor dem Zugriff Unbefugter zu schützen);

- das Recht auf Zugriff, Berichtigung und Widerspruch (der Betroffene muss das Recht haben, Auskunft über die ihn betreffenden Daten zu erhalten, sowie das Recht auf Berichtigung dieser Daten, wenn sie falsch sind. In bestimmten Situationen muss er Widerspruch gegen die Verarbeitung einlegen können);

- die Beschränkung der *Weiterübermittlung* der Daten in andere Drittländer (Übermittlungen vom ursprünglichen Bestimmungsdrittland in ein anderes Drittland sind nur zulässig, wenn das zweite Drittland ebenfalls ein angemessenes Schutzniveau aufweist).

Daneben gibt es im WP 12 weitere Grundsätze für sensible Daten, für das Direktmarketing sowie für automatisierte Einzelentscheidungen.

Neben diese materiellen Anforderungen treten die verfahrensrechtlichen Voraussetzungen. Zum einen müssen die verantwortlichen Stellen eine gute *Befolgungsrate* der materiellen Normen gewährleisten. Darüber hinaus ist der Betroffene im Konfliktfall bei der Durchsetzung seiner Rechte zu unterstützen. Schließlich muss bei Verstoß gegen die Bestimmungen eine angemessene Entschädigung für die geschädigte Partei gewährleistet sein.

Eine gewisse Spezifizierung der Anforderungen (die das WP 12 unabhängig davon aufstellt, ob ein Drittland insgesamt auf die Angemessenheit des Schutzniveaus oder ob eine selbstregulierende Maßnahme der Wirtschaft auf ausreichende Datenschutzgarantien überprüft wird) erfolgt durch die Entscheidung der Europäischen Kommission hinsichtlich *Standardvertragsklauseln* für die Übermittlung personenbezogener Daten in Drittländer[55]. Damit wurden insbesondere die Pflichten konkretisiert, die die datenexportierende und die daten-

[55] ABl. EG L 181/19; vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2001", S. 37

importierende Stelle erfüllen müssen. Von grundlegender Bedeutung sind die Haftungsregelung bei Schäden des Betroffenen sowie eine Aussage über die Zusammenarbeit mit den Kontrollstellen.

Praktisch bedeutet dies für die Abfassung von verbindlichen Unternehmensregelungen aus der Sicht der deutschen Aufsichtsbehörden Folgendes:

- Der Anwendungsbereich der Regelung muss festgelegt werden. Soll sie für Datenübermittlungen aus der EU in Drittländer gelten und die Verarbeitung dort regeln oder auch die Datenverarbeitung in dem Fall erfassen, in dem die Daten nur in einem Drittland verarbeitet oder in ein anderes übermittelt und dort verarbeitet werden? Eine umfassende Unternehmensreglung hätte den praktischen Vorteil, dass bei der Verarbeitung im Drittland keine Unterscheidung getroffen werden muss zwischen den Datenbeständen aus der EU und solchen aus Drittländern. Andererseits ist nicht zu verkennen, dass diese praktische Erwägung für die deutschen Aufsichtsbehörden im Rahmen der Beurteilung, ob ausreichende Datenschutzgarantien im Drittland für die aus der EU übermittelten Daten nach § 4 c Abs. 2 BDSG vorliegen, keine Rolle spielt.

- Eine Aussage über die Geltung einzelstaatlichen Rechts ist erforderlich: Bei der Datenübermittlung aus der Bundesrepublik (bzw. aus dem EWR) „reist" deutsches Recht (bzw. das jeweilige Recht des EWR-Staates) „mit" und ist für die Verarbeitung dieser personenbezogenen Daten im Drittland anzuwenden. Bestehende einzelstaatliche gesetzliche Regelungen im Drittland sind nur vorrangig zu berücksichtigen, wenn die gesetzlichen Regelungen positive Abweichungen enthalten, also ein „Mehr" an Datenschutz gewähren als die Unternehmensregelung.

- Eine Regelung über die Zusammenarbeit mit der Aufsichtsbehörde ist ebenso elementar wie die Beschreibung eines Beschwerdemechanismus: Der Betroffene muss sich bei behaupteten Datenschutzverstößen sowohl an den Konzerndatenschutzbeauftragten bzw. die datenimportierende Stelle als auch die Aufsichtsbehörde für den Datenschutz wenden können. Bei allen Anfragen der Aufsichtsbehörde am Sitz der datenexportierenden Stelle müssen Konzerndatenschutzbeauftragter und die datenimportierende Stelle mit der Aufsichtsbehörde kooperieren und ihre Feststellungen im Hinblick auf die Verarbeitung der übermittelten Daten respektieren.

- Haftungsregelung und Drittbegünstigungsklausel: Nach den Grundsätzen der gesamtschuldnerischen Haftung kann der Betroffene im Schadensfall gegen den Datenexporteur oder den Datenimporteur

oder gegen beide gerichtlich vorgehen. Die alleinige Haftung des Datenexporteurs kann nur unter der Voraussetzung akzeptiert werden, dass er auch für die Datenverarbeitung der im Drittland befindlichen Stelle einsteht. Der Betroffene muss darüber hinaus berechtigt sein, unmittelbar Rechte gegen das Unternehmen im Drittland geltend zu machen. Hierbei ist ausreichend, dass in der Unternehmensregelung eine Aussage dahingehend getroffen wird, dass der Betroffene seine Rechte (z. B. Auskunfts-/Berichtigungsrechte) auch in Ansehung der Datenverarbeitung im Drittland gegen den in Deutschland/dem EWR befindlichen Datenexporteur geltend machen kann.

Eine Unternehmensregelung, die diese Mindestanforderungen berücksichtigt, kann nach § 4 c Abs. 2 Satz 1 BDSG als Grundlage für zu genehmigende Datenübermittlungen genutzt werden. Dabei ist nicht die Unternehmensregelung selbst als Genehmigungsgegenstand zu betrachten, sondern – so der eindeutige Gesetzeswortlaut – nur die konkrete Datenübermittlung oder bestimmte Arten von Übermittlungen. Einzelheiten des Genehmigungsverfahrens, aber auch die Frage, ob bei Verwendung von Unternehmensregelungen überhaupt die Genehmigung der Aufsichtsbehörde einzuholen ist, sind unter den deutschen Aufsichtsbehörden umstritten[56]. Anzuerkennen ist jedoch das Bedürfnis der Wirtschaft nach Verfahrensvereinfachungen, wenn eine Unternehmensregelung mit weltweiter Gültigkeit geschaffen worden ist. Andererseits sind die Vorgaben der Europäischen Datenschutzrichtlinie zu berücksichtigen, die von der Genehmigungspflichtigkeit in Fällen außerhalb des Art. 25 und 26 Abs. 1 ausgeht (vgl. Art. 26 Abs. 2).

3.3 Erste DNA-Reihenuntersuchung in Berlin

Nach dem Mord an einem Säugling im Juli 2002, dem so genannten *„Babyklappenmord"*, gab es in Berlin die erste *DNA-Reihenuntersuchung*. Offensichtlich hatte die Person, die das tote Baby in die Babyklappe eines Krankenhauses legte, dort Ortskenntnisse. Die Polizei hat deshalb in Absprache mit der Staatsanwaltschaft – nachdem alle anderen Spuren mit hohem Aufwand in alle Richtungen verfolgt wurden – die auf dem Krankenhausgelände beschäftigten Frauen um die Abgabe einer Speichelprobe gebeten. Die Betroffenen haben nicht den Status von Beschuldigten. Es liegen zwar Aussagen von Zeugen vor, die in der Nähe zwei Frauen gesehen haben wollen. Daraus ergibt sich aber nicht zwangsläufig, dass es sich um auf dem Krankenhausgelände Beschäftigte handelt.

Nach dem Mord an einem Säugling im Juli 2002 fand in Berlin die erste DNA-Reihenuntersuchung statt.
Nach Auffassung auch des Berliner Beauftragten für Datenschutz und Informationsfreiheit wurden die für die Durchführung entwickelten rechtsstaatlichen Kriterien einer Reihenuntersuchung im Wesentlichen berücksichtigt. So war insbesondere der Grundsatz der Verhältnismäßigkeit gewahrt. Eine schwerwiegende Straftat war aufzuklären. Andere Ermittlungsanhaltspunkte lagen nicht mehr vor. Die schriftliche Einwilligung der Betroffenen wurde nach umfangreichen Informationen über die Hintergründe und die weitere Vorgehensweise eingeholt. Die Verarbeitung erfolgte streng zweckgebunden.

Den Grundsatz der Verhältnismäßigkeit sieht die Polizei gewahrt. Es gab keine andere Spur. Das Instrument

Bei Vorliegen einer Einwilligung der Betroffenen zur Entnahme, Analyse und Speicherung molekular geneti-

[56] vgl. 4.7

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

der Öffentlichkeitsfahndung – auch im Internet aufgrund richterlicher Beschlüsse - ist ohne nennenswerten Erfolg genutzt worden. Die Betroffenen haben in die Entnahme der DNA-Proben schriftlich eingewilligt. Zuvor hat die Polizei umfangreiche Aufklärungsarbeiten im Rahmen einer Personalversammlung geleistet, bei der die Hintergründe und das Vorhaben ausführlich erläutert wurden. Zusätzlich erhielten die Betroffenen ein Info-Schreiben. Darüber hinaus befand sich ein Polizeimitarbeiter ständig im Krankenhaus, der den Kontakt zu den Beschäftigten hielt und insbesondere für Informationsgespräche zur Verfügung stand.

Die vorliegenden Speichelproben befanden sich zum Berichtszeitpunkt noch in einem Stahlschrank beim Landeskriminalamt und sollten von einem Kölner Institut untersucht werden. Der Grund liegt darin, dass die Finanzierung der Auswertung noch nicht gesichert war.

Molekulargenetische Untersuchungen sind – ungeachtet der Frage, ob es sich um die Proben eines Beschuldigten oder einer anderen Person handelt – vom Richter anzuordnen (§ 81 f. StPO). Die Rechtsgrundlagen hierfür reichen allerdings nicht aus. Die Polizei stützt die Zulässigkeit deshalb auf die Einwilligung der Betroffenen.

Die Datenschutzbeauftragten des Bundes und der Länder vertreten die Auffassung[57], dass die Einwilligung zur Entnahme, Analyse und Speicherung molekulargenetischen Körpermaterials keine Grundlage für einen derartigen Eingriff sein kann; eine wirksame Einwilligung setzt voraus, dass sie frei von jeglichen – auch psychischen – Zwängen freiwillig erfolgt. Da die Betroffenen annehmen können, dass eine nicht erteilte Einwilligung Auswirkungen auf die Akzeptanz im sozialen Umfeld – hier: am Arbeitsplatz – haben kann und sie mit weiteren Besuchen der Polizei vor den Augen der Nachbarschaft oder Ermittlungen beim Arbeitgeber und damit rechnen können, dass die Polizei parallel zur oder nach erfolglosem Abschluss der molekulargenetischen Untersuchung ihre Ermittlungen auf diejenigen Personen konzentrieren wird, die eine freiwillige Teilnahme verweigert haben, kann von einer Freiwilligkeit nicht mehr die Rede sein. Ausschlaggebend für die Beurteilung der Freiwilligkeit einer Einwilligung ist die subjektive Einschätzung des Betroffenen.

Nun haben Gerichte in Berlin[58] entschieden, dass bei Vorliegen einer Einwilligung des Betroffenen eine richterliche Anordnung der Maßnahme nicht mehr

schen Körpermaterials ist eine richterliche Anordnung der Maßnahme nicht erforderlich; die Erteilung einer solchen Anordnung wird daher von den Berliner Gerichten abgelehnt.

---

[57] Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999 zu DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen, vgl. Anlagenband „Dokumente zum Datenschutz 1999", S. 18

[58] AG Tiergarten, Beschluss vom 28. September 1999, Az.: 353 Gs 3388/99; LG Berlin, Beschluss vom 5. November 1999, Az.: 522 Qs 118/99

ergehen könne. Das haben wir zur Kenntnis genommen, auch wenn wir die rechtliche Begründung nicht teilen können. Um so wichtiger ist es dann, die Betroffenen umfassend entsprechend den datenschutzrechtlichen Vorschriften über die Einwilligung (§ 6 Abs. 3 bis 5 BlnDSG) auf den tiefen Eingriff in ihre Rechtsgüter aufzuklären. Wegen der datenschutzgerechten Gestaltung der Formulare sind wir mit den Senatsverwaltungen für Inneres und Justiz im Gespräch.

Bei molekulargenetischen Reihenuntersuchungen liegt die rechtsstaatliche Problematik in der faktischen Umkehr der Beweislast und in einer Durchbrechung der Unschuldsvermutung im Strafverfahren. Die Strafverfolgungsorgane müssen den Teilnehmern – soweit sie nicht Beschuldigten-Status haben – bis auf ganz allgemeine Kriterien wie vermutete Altersgruppe und Wohnort keine Tatnähe im Sinne eines Verdachtsgrades nachweisen. Vielmehr können sich die angesprochenen Personen veranlasst sehen, sich durch freiwillige Teilnahme am Reihentest aus dem Blickfeld der Ermittler zu bringen, um weitere polizeiliche und justizielle Maßnahmen abzuwenden. Viele Bürger nehmen nach einem spektakulären Verbrechen in ihrer Region offenbar gern an einem solchen Test teil, um die Polizei einem Aufklärungserfolg durch kriminaltechnischen Ausschluss der Nicht-Täter und damit der Eingrenzung weiterer Ermittlungen näher zu bringen. Eine Reihenuntersuchung verfolgt neben dieser Eingrenzungsfunktion auch das Ziel, dass der Täter an ihr teilnimmt und durch sie unmittelbar identifiziert wird. Die Strafverfolgungsbehörden schaffen mit dem Massen-DNA-Test eine Situation für den Täter, in der er sich aufgrund einer faktischen Drucksituation einer dem Geständnis gleichwertigen Selbstbelastung nicht mehr entziehen kann. Deshalb dürfen kriminaltechnische Reihentests nur bei herausragenden Fällen durchgeführt werden. Ihre Legitimation erhalten sie nur aufgrund des öffentlichen Interesses an der Aufklärung der Straftat – und nicht etwa aufgrund eines Interesses der Nicht-Täter an dem Nachweis, als Spurenverursacher ausgeschlossen zu werden.

Da mit den vorhandenen gesetzlichen Grundlagen DNA-Reihenuntersuchungen nicht gerechtfertigt werden können, sie andererseits aber im Einzelfall bereits heute – wie der zugrunde liegende Fall belegt – unverzichtbar sein können, müssen rechtsstaatliche Mindestanforderungen beachtet werden. Es wäre rechtsstaatlich nicht hinnehmbar, wenn – unabhängig von der Schwere der aufzuklärenden Tat und den sonstigen herkömmlichen Ermittlungsmöglichkeiten – immer häufiger von Massen-DNA-Tests Gebrauch gemacht würde, soweit es die Kostenbelastung für die Polizei zulässt. Die Aufforderung an unverdächtige Personen, sich selbst zu entlasten, darf nicht zu einem Standardfall der Strafermittlungen abschleifen.

Bei freiwilligen Massen-DNA-Tests ist die Einhaltung folgender Kriterien erforderlich:

- Massen-DNA-Tests stellen einen staatlichen Eingriff weit im Vorfeld eines Anfangsverdachtes dar. Sie können den Täter zu einer massiven, nur eingeschränkt freiwilligen Selbstbelastung veranlassen. Deshalb müssen sie die ultima ratio der strafprozessualen Ermittlungen bleiben. Es müssen erst alle in dem konkreten Fall einsetzbaren, gesetzlich vorgesehenen Ermittlungsinstrumente ausgeschöpft worden sein, die einen kleineren Kreis von Personen als den der potenziellen Teilnehmer eines Massen-DNA-Tests belasten.

- Die Ermittlungen müssen schwere Straftaten zum Gegenstand haben, in denen die Schutzgüter Leib und Leben verletzt oder zumindest gefährdet worden sind. Eine einfache Körperverletzung kann keine DNA-Reihenuntersuchung rechtfertigen. Der Katalog der strafprozessualen Rasterfahndung (§ 98 a StPO), einer im weitesten Sinn mit der DNA-Reihenuntersuchung vergleichbaren Maßnahme, kann als Vorbild dienen, enthält aber Straftaten, für die eine DNA-Untersuchung bei Nicht-Beschuldigten unverhältnismäßig wäre.

- Es muss aufgrund einer Fall-Analyse hinreichende Anhaltspunkte für die Eingrenzung des Teilnehmerkreises geben, die Massentests „ins Blaue hinein" ausschließen. Verhältnismäßig wäre ein Vorgehen in konzentrischen Kreisen, wonach Gruppen von Betroffenen je nach potenzieller Tatnähe gebildet und bei Erfolglosigkeit des Abgleichs die jeweils tatfernere Personengruppe einbezogen wird.

- Die Einwilligungsformulare und die hierzu gegebenen schriftlichen Erläuterungen zum Verfahren müssen sorgfältig gestaltet werden und die Freiwilligkeit der Teilnahme zweifelsfrei belegen. Gegenüber einer unmittelbaren, persönlichen Ansprache des Betroffenen ist die vorherige postalische Zusendung des Formulars erforderlich, damit die Betroffenen sich in Ruhe mit der Frage der Teilnahme befassen können.

- Die Daten dürfen nur streng zweckgebunden für den molekulargenetischen Abgleich mit der Täterspur in demselben Strafverfahren verwendet werden. Sie dürfen nicht mit der DNA-Analyse-Datei bei dem Bundeskriminalamt (BKA) abgeglichen oder gar in diese eingestellt werden und müssen spätestens mit der rechtskräftigen Verurteilung des Täters vernichtet werden. Eine Verwendung für die Aufklärung nachfolgender Verbrechen in demselben regionalen Bereich noch während dieser Aufbewahrungsdauer ist unzulässig. Auch die Regelungen zur zweckdurchbrechenden Nutzung von Daten aus Strafverfahren (§§ 474 ff. StPO) für andere repressive oder präventive Zwecke dürfen aus diesem Grund auf die DNA- und sonstigen Daten

der Teilnehmer der Reihenuntersuchung keine Anwendung finden.

- Große Bedeutung kommt den Maßnahmen zu, die gegenüber Verweigerern getroffen werden. Eine zwangsweise Anordnung der Abgabe einer Speichelprobe und deren molekulargenetische Untersuchung kommt nur gegenüber Personen mit Beschuldigten-Status in Betracht. Die Verweigerung des Einverständnisses darf nicht als verdachtsbegründend gewertet werden. Da dem Teilnehmerkreis der Reihenuntersuchung kein Beschuldigten-Status zuerkannt werden kann, verfügen Polizei und Staatsanwaltschaft über keine rechtliche Möglichkeit (§§ 81 c, 81 e, 81 f. StPO), das DNA-Profil der Verweigerer zu erlangen und abzugleichen; sie können lediglich Vorermittlungen zur Klärung, ob ein Anfangsverdacht vorliegt, durchführen, nicht jedoch Ermittlungen, die einen solchen Verdacht nach der StPO voraussetzen. Wenn eine Reihenuntersuchung tatsächlich als ultima ratio durchgeführt wird, wird sich ein Anfangsverdacht gegenüber Verweigerern allerdings in diesem Stadium vielfach kaum mehr begründen lassen. Das Vorgehen in konzentrischen Kreisen bedingt, dass erst die Frage der Maßnahmen gegenüber Verweigerern geprüft wird, bevor der nächste weitere Kreis von Teilnehmern des Speicheltestes angesprochen wird.

- Um eine gerichtliche und datenschutzrechtliche Nachprüfbarkeit zu ermöglichen, ob und mit welchen rechtlichen und tatsächlichen Erwägungen der dargestellten Vorgehensweise im konkreten Fall gefolgt wurde, sind die Verfahrensschritte in der Strafverfahrenakte hinreichend zu dokumentieren.

- Solange keine gesetzlichen Grundlagen für Reihenuntersuchungen vorhanden sind, sollte unsere Dienststelle – begleitend zur Durchführung eines Massen-DNA-Tests – über die beabsichtigten Verfahrensschritte unterrichtet werden.

Die Finanzierung für die Probenbestimmung muss feststehen.

Diese Kriterien wurden bei der ersten DNA-Reihenuntersuchung im Wesentlichen berücksichtigt. Insbesondere wurde nach umfangreichen Informationen über die Hintergründe und die weitere Vorgehensweise eine schriftliche Einwilligung eingeholt. Die Verarbeitung erfolgte streng zweckgebunden. Ein Abgleich mit der DNA-Analyse-Datei bei dem BKA wird nach Mitteilung der Polizei nicht durchgeführt. Ebenso werden die Daten – mit Ausnahme denen des Täters – nicht in die DNA-Analyse-Datei bei dem BKA eingestellt. Zum Zeitpunkt unserer Prüfung hatte noch keine Person die Mitwirkung an der DNA-Reihenuntersuchung verweigert.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

3.4 Vier Jahre IT-Sicherheitsrichtlinie und IT-Sicherheitsstandards in der Berliner Verwaltung

Der sichere Einsatz der Informationstechnik ist in den letzten Jahren ein Top-Thema der Fachpresse, aber auch von Schlagzeilen in den einschlägigen Rubriken der Tagespresse gewesen. Allenthalben werden Sicherheitslücken bei verbreiteter Standardsoftware aufgedeckt, liest man vom Durchbrechen von Sicherheitsschranken, ja sogar von Cyber-Terrorismus und Cyber-Krieg, wobei die Sicherheitslücken wichtigster Steuerungssysteme von Staat und Wirtschaft zu terroristischen oder kriegerischen Zwecken ausgenutzt werden könnten. Es ist unmöglich, das Angebot an Seminaren, Konferenzen, Workshops u.v.a.m., die sich mit dem Thema IT-Sicherheit im engeren und weiteren Sinne oder in Bezug auf eingeengte Fragestellungen oder bestimmte Produkte allein im deutschsprachigen Raum befassen, wahrzunehmen. Das Thema *IT-Sicherheit* ist zumindest ein großes Geschäft.

Eine von einer Fachzeitschrift und einer bekannten Unternehmensberatung im September 2002 veröffentlichte Studie zur Sicherheit der Computersysteme in deutschen Firmen zeigte auf, dass zwischen dem Konsens hinsichtlich der hohen Priorität der IT-Sicherheit und der Realität, die sich in den Maßnahmen zeigt, erhebliche Differenzen bestehen[59]. Die angeblich hohe Priorität der IT-Sicherheit erweist sich häufig als Lippenbekenntnis. Ein Drittel der befragten Unternehmen hatten in den 12 Monaten vor der Befragung keine Schritte zur Verbesserung der IT-Sicherheit unternommen. Bei 60% der Unternehmen waren die Budgets für IT-Sicherheit stagnierend oder rückläufig. Entsprechend sind die Folgen: 1,2 Millionen Tage sind die Computersysteme in deutsche Unternehmen im Jahre 2001 aufgrund von Angriffen auf die IT-Infrastruktur ausgefallen.

Lassen sich die erschreckenden Feststellungen auch auf die Berliner Verwaltung übertragen?

Seit Januar 1999 ist die Richtlinie zur Gewährleistung der notwendigen Sicherheit beim IT-Einsatz in der Berliner Verwaltung (*IT-Sicherheitsrichtlinie*)[60] mit den dazugehörigen IT-Sicherheitsstandards eine verbindliche Verwaltungsvorschrift und damit bindend für alle Senats- und Bezirksverwaltungen und deren nachgeordneten Behörden.

Eine wesentliche Vorgabe der IT-Sicherheitsrichtlinie ist die zwingende Erarbeitung und Umsetzung von Sicherheitskonzepten in den unterschiedlichen Berei-

Dem Senat ist bewusst, dass die Sicherheit des IT-Einsatzes in der Berliner Verwaltung noch weiter verbessert werden kann und muss. Die Umsetzung anforderungsgerechter Sicherheitsmaßnahmen ist ein ständiger Prozess, der durch eine entsprechende Erfolgs- und Qualitätskontrolle begleitet wird. Der Stand der Umsetzung wird u. a. durch den jährlichen IT-Sicherheitsbericht erfasst und analysiert.

Aus dem aktuellen IT-Sicherheitsbericht für das Jahr 2002 ergibt sich u. a., dass in den einzelnen Behörden nur in geringem Umfang schadensrelevante Sicher-

[59] „Blind oder blauäugig?"In: Informationweek 18/02, S. 22 ff.

[60] DBl. I 1999, S. 5; JB 1998, 2.2; JB 1999, 2.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

chen. Dazu zählen behördenbezogene, verfahrensspezifische und die zentrale Infrastruktur betreffende Sicherheitskonzepte. Die Methodik der Erarbeitung und Umsetzung von Sicherheitskonzepten hat sich bewährt, da aufgrund einer spezifischen Risikoanalyse die wesentlichen Gefahren und Risiken erkannt und durch geeignete Maßnahmen im Sicherheitskonzept beseitigt bzw. minimiert werden können. Nur anhand einer systematischen Risikoanalyse kann ermessen werden, welche technischen und organisatorischen Maßnahmen „für den angestrebten Schutzzweck angemessen" sind, wie in § 5 Abs. 1 BlnDSG verlangt wird.

Nach nunmehr vier Jahren sollten alle betroffenen Verwaltungen genügend Zeit gehabt haben, diese Vorgaben umzusetzen.

Die Praxis stellt sich Ende 2002 leider anders dar. Die IT-Sicherheitsrichtlinie und die IT-Sicherheitsstandards sind in wesentlichen Bereichen nur unzulänglich umgesetzt. Der nach der Sicherheitsrichtlinie jährlich zu erstellende IT-Sicherheitsbericht[61] weist für 2001 auf, dass ca. 40 % der betroffenen Verwaltungen nicht über ein behördenspezifisches Sicherheitskonzept verfügen. Bei den von uns durchgeführten Kontrollen wurde dieses Bild eindeutig bestätigt. Von acht kontrollierten Senats- und Bezirksverwaltungen verfügten sechs nicht über ein eigenes Sicherheitskonzept. Eine Bezirksverwaltung war gerade dabei, ein Sicherheitskonzept zu erarbeiten. Ein weiteres Sicherheitskonzept war aus dem Jahre 2000 und seit zwei Jahren nicht mehr fortgeschrieben. So mussten bei den Kontrollen Mängel festgestellt werden, die bei einer vollständigen Risikoanalyse und der Umsetzung eines darauf basierenden Sicherheitskonzeptes gar nicht aufgetreten wären.

Neben der Vorgabe der Erarbeitung und Umsetzung von Sicherheitskonzepten verlangen die IT-Sicherheitsrichtlinie bzw. die IT-Sicherheitsstandards ein Konzept zum „Schutz der Vertraulichkeit bei der Datenübertragung im Berliner Landesnetz". Dieses Konzept wurde Ende 2001 vom IT-KAB beschlossen und in die IT-Sicherheitsstandards integriert[62]. Es sieht innerhalb der zentralen IT-Infrastruktur (MAN) eine hardwarebasierte Leitungsverschlüsselung vor. Bei dieser Leitungsverschlüsselung werden die Daten beim Übergang von einem lokalen Netz (z. B. einer Bezirksverwaltung) in die zentrale IT-Infrastruktur (MAN) durch ein so genanntes Krypto-Gateway (Verschlüsselungsbox) verschlüsselt, so über das MAN übertragen und beim Übergang in das lokale Netz des Empfängers wieder durch ein Krypto-Gateway entschlüsselt.

Seit Jahren fordern wir die *Verschlüsselung* bei der

heitsvorfälle auftraten. Insofern lassen sich die angeführten Zahlen zu den in der Wirtschaft aufgetretenen Arbeitsausfällen auf Grund von Angriffen auf die IT-Infrastruktur nicht auf die Berliner Verwaltung übertragen.

Gleichwohl kommt der IT-Sicherheitsbericht zu dem Ergebnis, dass es gerade bei der Erstellung und Umsetzung der notwendigen IT-Sicherheitskonzepte noch weiterer Anstrengungen bedarf.

Dazu hat der IT-KAB auf seiner Sitzung am 28.11.02 u. a. die Entwicklung einer Modelllösung für behördliche Sicherheitskonzepte beschlossen.

Die Modelllösung soll die Vorgehensmethodik vereinfachen und konkretisieren sowie auf Basis gemeinsamer Risiken dazu konkrete, übergreifend anwendbare Sicherheitsmaßnahmen definieren.

Das Modellsicherheitskonzept wird derzeit ausgearbeitet. Dabei sollen bereits die jeweiligen Teilergebnisse schrittweise in den Behörden implementiert werden.

Die Nutzung des verschlüsselten Zugangs zum Berliner

[61] JB 1999, 2.2

[62] JB 2001, 3.6

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats
Übertragung personenbezogener Daten über das MAN[63], eine Forderung, die vom zentralen IT-Management und dem IT-Koordinierungs- und Beratungsgremium der Berliner Verwaltung (IT-KAB) stets unterstützt wurde. Seit April 2002 ist die Leitungsverschlüsselung verfügbar. Jedoch nehmen bisher nur wenige Behörden diesen Dienst des LIT in Anspruch. Dies bedeutet, dass immer noch wichtige Verfahren, wie z. B. das Haushaltsverfahren ProFISKAL, unverschlüsselt über das MAN betrieben werden, obwohl die Verschlüsselung durch die IT-Sicherheitsrichtlinie/-standards für alle Senats- und Bezirksverwaltungen und deren nachgeordneten Behörden vorgegeben ist. Diese leichtfertige Nutzung des Berliner Landesnetzes ist auch Gegenstand eines Beschlusses vom 26.11.2002 des Unterausschusses „Datenschutz" des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses von Berlin geworden. Der Beschluss lautet: „Der Senat wird aufgefordert, dafür zu sorgen, dass bei der Übertragung personenbezogener Daten über das Berliner Landesnetz oder über andere Übertragungswege zwischen unterschiedlichen Standorten der Verwaltung zur Gewährleistung ihrer Vertraulichkeit und Integrität (§ 5 Abs. 2 Nr. 1 und 2 Berliner Datenschutzgesetz) geeignete Verschlüsselungstechnik (z. B. die vom Landesbetrieb für Informationstechnik angebotenen Verschlüsselungssysteme) eingesetzt wird."	Landesnetz ist eine wichtige Maßnahme, um den erforderlichen Schutz der Vertraulichkeit übertragener Daten zu gewährleisten. Der IT-Sicherheitsbericht für das Jahr 2002 weist aus, dass der verschlüsselte Zugang derzeit von 9 Behörden genutzt wird. 12 Behörden planen die Nutzung für das Jahr 2003.
Besser sieht die Umsetzung der IT-Sicherheitsrichtlinie/-standards im Bereich der gestaffelten Firewalls und des Virenschutzes aus. Nach dem IT-Sicherheitsbericht 2001 verfügen 84 % der an das Berliner Landesnetz angeschlossenen lokalen Netze über ein Firewall-System zum MAN. Bei unseren Kontrollen mussten wir jedoch feststellen, dass die Firewalls teilweise völlig durchlässig konfiguriert werden müssen, da sonst bestimmte Verfahren nicht funktionsfähig sind. 93 % verfügen über ein dezentrales Virenschutzkonzept in den lokalen Verwaltungsnetzen. Hier wurden die erheblichen Gefahren, die mit der verstärkten E-Mail-Nutzung in der Verwaltung zusammenhängen, erkannt und durch geeignete Maßnahmen reduziert.	Die anforderungsgerechte und praxiswirksame Konfiguration von Firewalls sind ebenso wie die Durchführung von Notfallübungen Gegenstand der bereits erwähnten laufenden Aktivitäten zur Erstellung eines Modellsicherheitskonzeptes. Bei der Ausgestaltung von Notfallübungen müssen in jedem Fall die rechtlichen, organisatorischen und technischen Randbedingungen berücksichtigt werden.
Als Hauptargument für die Ignorierung der IT-Sicherheitsrichtlinie wird im Normalfall die finanzielle Situation der Verwaltungen angeführt. Sicherheit ist aber nicht umsonst zu haben. Die Durchführung einer Risikoanalyse und die Erstellung eines Sicherheitskonzeptes erfordern einen nicht unerheblichen Aufwand und sind damit, insbesondere bei Hinzuziehen von externem Sachverstand, mit Kosten verbunden. Die vom Bundesamt für Sicherheit in der Informationstechnik herausgegebenen „Hilfsmittel", das IT-Grundschutzhandbuch bzw. das IT-Sicherheitshandbuch, bilden jedoch eine hervorragende Grundlage, die man nur nutzen muss.	

[63] JB 1999, 4.8.1

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Ansonsten kann nur Überzeugungsarbeit helfen. Diese darf aber nicht mehr nur in Form von Worten oder Papieren bestehen. Den für die IT-Sicherheit in den jeweiligen Verwaltungen Verantwortlichen muss anschaulich gezeigt werden, wie angreifbar und verletzlich ihre Systeme sind. Dieses kann z. B. durch den Einsatz von Penetrationstests und gezielten Notfallübungen erreicht werden. Sinnvoll wäre eine „Spezialeinheit", die beim LIT angesiedelt sein könnte, die entweder unangekündigt oder auch angekündigt gezielte und gesteuerte Angriffe durchführt oder zumindest anschaulich simuliert.

Kontrollen von Bezirks- und Senatsverwaltungen

In diesem Jahr wurden acht Bezirks- und Senatsverwaltungen einer technisch-organisatorischen Kontrolle unterzogen um festzustellen, inwieweit die Regelungen der §§ 3 a und 5 BlnDSG und die Vorgaben der IT-Sicherheitsrichtlinie und der IT-Sicherheits-standards eingehalten werden.

Ein Schwerpunkt war die Sicherheit der installierten *Firewalls*. Wie bereits erwähnt, ist positiv anzumerken, dass die meisten kontrollierten Verwaltungen das Konzept der gestaffelten, dezentralisierten Firewalls umgesetzt haben. Dadurch wird das behördliche Netz gegenüber dem MAN abgeschirmt und dem Prinzip der informationellen Gewaltenteilung Sorge getragen. Um einen ausreichenden Schutz zu gewährleisten, reicht jedoch allein das Vorhandensein einer Firewall nicht aus. Wesentlich ist der inhaltliche Aufbau und die Administration dieser Schutzeinrichtung.

Entweder wird die Administration durch einen externen Dienstleister vorgenommen oder die eigene IT-Stelle mit der Administration beauftragt. Beide Lösungsansätze sind geeignet , wenn bestimmte Regeln bei der Administration Beachtung finden. Für den Betrieb der Firewall ist festzulegen:

- Anzahl der Firewalladministratoren und die Vertretungsregelungen;
- die Art, in welcher Weise die Administration (Fernwartung oder Konsole) und die damit verbundene Auswertung der Protokolle (Häufigkeit, Aufbewahrungsfristen, auswertende Personen) erfolgt;
- die Stelle, die festlegt, welche Dienste zugelassen werden sollen;
- ein Notfallplan, der die Vorgehensweise bei festgestellten Angriffen festlegt.

Die meisten Behörden, die die Firewall selbst administrieren, verfügen über ein solches Konzept.

Die im Bericht aufgeführten Anregungen zum Betrieb dezentraler Firewall und zum Zusammenhang von Virenschutz und Notfallkonzept werden ebenfalls bei der Erarbeitung des Modellsicherheitskonzeptes berücksichtigt.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Ein weiterer Schwerpunkt war die Umsetzung der dezentralen Virenschutzkontrolle in den Behörden. Noch vor wenigen Jahren wurde argumentiert, dass der zentrale Virenschutz am Übergangspunkt vom MAN zum Internet ausreichenden Schutz bietet[64]. Mittlerweile besteht aber Einigkeit darüber, dass ein Virenschutz vor Ort stattfinden muss. Auch die IT-Sicherheitsstandards enthalten ausführliche Vorgaben zum dezentralen Virenschutz.

Mittlerweile verfügt jede Verwaltung über Virenschutzsoftware. Obwohl die IT-Sicherheitsstandards klare Vorgaben machen, ist die Ausgestaltung jedoch sehr unterschiedlich. Nach den Standards sollen alle Dateiserver im Hintergrund überwacht werden. Wenn über ein Endgerät austauschbare Datenträger verarbeitet werden können oder wenn das Endgerät über einen Zugang zum Berliner Landesnetz oder zum Internet verfügt, ist immer eine Virenschutzsoftware zu installieren. Sollte der Zugang über einen Terminalserver realisiert sein, reicht jedoch ein Virenschutz auf dem Terminalserver aus. Das Endgerät muss dann nicht mehr zusätzlich mit einer entsprechenden Software ausgestattet sein.

Bei unseren Kontrollen mussten wir feststellen, dass die Erstellung und Fortschreibung eines Virenschutzkonzepts das einen Notfallplan berücksichtigt nur selten erfolgte. Darin ist festzulegen, wie im Falle eines Virenbefalls zu reagieren ist, wer zu benachrichtigen ist, was getan werden muss, um ein weiteres Ausbreiten zu verhindern, und wie das befallene System wieder in einen ordnungsgemäßen Zustand gesetzt werden kann. Auch hier gibt es trotz einiger Verbesserung noch großen Handlungsbedarf.

Vor allem im Bereich der Bezirksverwaltungen spielt die Sicherheit bei der Anbindung von Außenstellen eine wichtige Rolle. Meist erstreckt sich das bezirkliche Behördennetz über mehrere Standorte und muss damit mehrere (kleine) lokale Netze zu einem Netz zusammenführen. Erschwerend kommt hinzu, dass im Rahmen der Bezirksfusionen diverse Ämter und Abteilungen zusammengefasst oder auf unterschiedliche Standorte verteilt worden sind. Vor diesem Hintergrund kommt dem Problem der Sicherheit der Datenübertragung zwischen den lokalen Netzen der unterschiedlichen Standorte besondere Bedeutung zu.

§ 5 Abs. 2 Nr. 1 und 2 BlnDSG verpflichtet dazu, die Vertraulichkeit und Integrität der Daten zu gewährleisten, also zu verhindern, dass bei der Übertragung von personenbezogenen Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert,

Der Schutz der Vertraulichkeit übertragener Daten muss durch geeignete technisch-organisatorische Maßnahmen gesichert werden. Insbesondere bei der Übertragung zwischen einzelnen Standorten muss auf Basis der Risikoanalyse festgelegt werden, mit welchen Maßnahmen das bestehende Risiko auf ein akzeptables Maß verringert werden kann.

Dabei wird sich in vielen Fällen ein geeigneter Schutz nur durch eine Verschlüsselung erreichen lassen. Gleichwohl sollte jedoch grundsätzlich das Schutzziel (Schutz der Vertraulichkeit) und nicht eine mögliche technische Lösung (Verschlüsselung) Ausgangspunkt der Überlegungen zur Auswahl geeigneter Maßnahmen sein.

---

[64] vgl. JB 1999, 2.2

[65] JB 2001, 3.6

verändert oder gelöscht werden können. Dies kann entweder dadurch gewährleistet werden, dass ein Zugriff von Unbefugten auf die Kommunikationsleitungen verhindert wird, oder dadurch, dass die Daten bei der Übertragung durch geeignete Verfahren verschlüsselt werden. Der Schutz der Kommunikationsleitungen kann - wenn überhaupt - nur durch eine geeignete Verlegung in kontrollierbaren Gebäuden, Räumen oder Trassen realisiert werden. Wenn nicht sichergestellt werden kann, dass die Daten über kontrollierbare Leitungen (inkl. aller Netzknoten) fließen, ist eine Verschlüsselung notwendig. Dies gilt zumindest immer dann, wenn die Daten hausübergreifend fließen[65].

Wenn in einem Gebäude untergebrachten Amt eine strukturierte Verkabelung nach den in Berlin geltenden Verkabelungsvorschriften verwendet wird und die nach dem IT-Grundschutzhandbuch notwendigen Maßnahmen zur Verkabelung ergriffen wurden, kann innerhalb dieses lokalen Netzes auf eine Verschlüsselung verzichtet werden. Wenn jedoch eine Fernadministration eines Servers oder eine zentrale Datensicherung vom entfernten Rathaus aus erfolgt, so ist eine Verschlüsselung geboten.

Die meisten Bezirke realisieren den Zusammenschluss der einzelnen lokalen Netze zu einem bezirklichen Behördennetz über eigene für diesen Zweck gemietete Leitungen. Gelegentlich sind auch Richtfunkverbindungen über das IEEE 802.11b Protokoll realisiert[66]. In all diesen Fällen sind personenbezogene Daten bei der Übertragung zu verschlüsseln.

Bei den Kontrollen mussten wir jedoch feststellen, dass keine einzige Behörde für ihre Außenstellen eine Verschlüsselung vorgesehen hatte, obwohl in vielen Fällen eine Verschlüsselung der Daten für die Übertragung geboten wäre. Als Grund für die fehlende Verschlüsselung wurde immer das Fehlen von Haushaltsmitteln angegeben. Dieses Argument ist aber nicht ausreichend, um die Vernachlässigung gesetzlicher Vorschriften zu rechtfertigen.

4. Aus den Arbeitsgebieten

4.1 Sicherheit und Strafverfolgung

4.1.1 Rasterfahndung

Im letzten Jahresbericht haben wir bereits über die *Rasterfahndung* in Berlin nach dem 11. September 2001 berichtet[67]. Im Dezember 2002 wurde nun dem Präsidenten des Abgeordnetenhauses von Berlin der

Die Sachdarstellung des Berliner Datenschutzbeauftragten ist zutreffend.

Für die Bewertung der durchgeführten Maßnahmen ist

[66] JB 2001, 4.8.3

[67] JB 2001, 4.1.1

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

angekündigte „Sonderbericht über die Durchführung besonderer Formen des Datenabgleichs (Rasterfahndung)" übergeben. Die datenschutzrechtliche Überprüfung der Rasterfahndung hat gezeigt, wie schwierig die Anwendung der Rechtsgrundlagen für diese Art der Fahndung in der Praxis gewesen ist. Erst nach zahlreichen Anträgen des Polizeipräsidenten erging am 24. Oktober 2001 eine aus datenschutzrechtlicher Sicht ausreichende Anordnung der Rasterfahndung durch das Amtsgericht Tiergarten. Nachdem das Landgericht Berlin die Rasterfahndung am 15. Januar 2002 zunächst für unzulässig erklärt hatte[68], hob das Kammergericht Berlin in seiner Entscheidung vom 16. April 2002 die Entscheidung des Landgerichtes Berlin auf, da das Kammergericht eine gegenwärtige Gefahr zum Zeitpunkt der Rasterfahndung als gegeben angesehen hatte[69]. Das Kammergericht Berlin hat sich in seiner Entscheidung im Übrigen nur auf die richterliche Anordnung vom 24. Oktober 2001 bezogen und die vorangegangenen Beschlüsse des Amtsgerichtes Tiergarten als durch die letzte Anordnung aufgehoben bezeichnet, ohne die vorangegangenen Beschlüsse zu bewerten.

Nach dem Beschluss des Kammergerichts wurden die zunächst unterbrochenen Arbeiten fortgeführt. Anfang Juli war die Rasterfahndung selbst beendet; aus den angelieferten 58063 Datensätzen wurden schließlich die Daten von 114 Personen nach einer vorgegebenen Prioritätenliste ausgerastert. Am 12. Juli vernichtete der Polizeipräsident auf einer gemeinsamen Pressekonferenz mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit die CD-ROM mit allen gespeicherten Daten.

Zu den 114 Personen wurden eigene Ermittlungsakten angelegt, die zur Grundlage einer eingehenden Überprüfung gemacht wurden. Zum Zeitpunkt des Sonderberichts war uns von der Polizei mitgeteilt worden, dass auch diese Überprüfungen ergebnislos abgeschlossen seien. Aus diesem Grund forderten wir die Vernichtung der Akten, da alle Unterlagen, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind, unverzüglich zu vernichten sind (§ 47 Abs. 3 S. 1 ASOG).

Inzwischen hat uns der Polizeipräsident mitgeteilt, dass entgegen seiner vorherigen Aussage nur in bisher 17 Fällen die Bearbeitung der 114 Prüffälle aus der Rasterfahndung abgeschlossen sei. Auf der Grundlage dieses geänderten Sachverhalts ist die weitere Aufbewahrung der übrigen Prüffälle zulässig.

entscheidend, dass das Kammergericht die sog. Rasterfahndung in der Weise, wie sie von der Polizei durchgeführt wurde, für rechtmäßig erklärt hat.

Natürlich gab es bei der erstmaligen Anwendung des § 47 ASOG einige Anlaufschwierigkeiten bei allen Beteiligten. Weder Polizei noch der Berliner Beauftragte für Datenschutz und Informationsfreiheit, Gericht oder die Senatsverwaltung für Inneres hatten Erfahrungen mit der praktischen Durchführung einer Rasterfahndung, so dass Auslegungsdifferenzen oder unterschiedliche Auffassungen über den „richtigen" Ablauf der Maßnahme nicht verwundern können.

Im Ergebnis wird der Polizei im Sonderbericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit aber bescheinigt, die Rasterfahndung unter Wahrung der Verhältnismäßigkeit und datenschutzgerecht durchgeführt zu haben.

Aus dem Datenabgleich haben sich 114 sog. Positive Prüffälle ergeben. Die Bearbeitung dieser Prüffälle hat in keinem Fall Tatsachen erbracht, die die Prognose rechtfertigen würden, die betroffene Person werde Straftaten mit islamisch-terroristischem Hintergrund begehen.

17 Prüffälle hat die Polizei als endgültig erledigt abgeschlossen und die Akten vernichtet.

97 Prüffälle waren noch nicht endgültig abgeschlossen, weil hier noch die Möglichkeit bestand, dass sich aus dem Datenabgleich des BKA in der Verbunddatei „Schläfer" Erkenntnisse ergeben.

Dieser Datenabgleich beim BKA ist inzwischen abgeschlossen. Weitere Ermittlungsanhalte oder neue Erkenntnisse haben sich daraus nicht ergeben. Deshalb wurden zum 31. März 2003 sämtliche im Zusammenhang mit der Berliner Rasterfahndung stehenden per-

[68] Az.: 84 T 8/02

[69] Az.: 1 W 89-98/02

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats
	sonenbezogenen Unterlagen und Daten vernichtet oder deren Vernichtung beim BKA angewiesen. Es werden keine Akten mehr aufbewahrt und auch beim BKA sind die Daten aus der Berliner Rasterfahndung gelöscht worden.
Insgesamt hat die durchgeführte Rasterfahndung aus datenschutzrechtlicher Sicht die folgenden Mängel aufgewiesen:	Zu den vom Berliner Beauftragten für Datenschutz und Informationsfreiheit zusammenfassend aufgeführten „Mängeln“:
- Es fehlte vor und in der Regel auch während der Rasterfahndung an einer zeitnahen Unterrichtung des Berliner Beauftragten für Datenschutz und Informationsfreiheit (§ 47 Abs. 4 Satz 7 ASOG).	Der Vorwurf trifft nicht zu. Es gibt keine andere polizeiliche Maßnahme, bei der der Berliner Beauftragte für Datenschutz und Informationsfreiheit so intensiv informiert und konsultiert wurde, wie bei dieser Rasterfahndung. § 47 Abs. 4 letzter Satz legt nur fest, dass der Berliner Beauftragte für Datenschutz und Informationsfreiheit durch die Polizei über Maßnahmen der Rasterfahndung zu unterrichten ist. Über den Zeitpunkt der Unterrichtung sagt die Vorschrift nichts aus. Es bestand daher auch keine Verpflichtung, den Berliner Beauftragte für Datenschutz und Informationsfreiheit bereits vor der ersten Antragstellung zu informieren.
- Weder eine Risiko-Analyse noch ein Sicherheitskonzept sind für die Datei erstellt worden(§ 5 Abs. 3 BlnDSG).	Dies trifft zu. Allerdings muss die besondere Situation und der große Zeitdruck berücksichtigt werden, unter dem die Datei eingerichtet wurde. In dieser Situation wurden die Änderungen in § 5 Abs. 3 des Berliner Datenschutzgesetzes vom 30.07.2001 bei der Abfassung der Errichtungsanordnung nicht berücksichtigt. Das Verfahren bei der Erstellung von Risikoanalysen und Sicherheitskonzepten sollte grundsätzlich, d.h. unabhängig von der eilbedürftigen Errichtung dieser Datei, geklärt werden. Trotzdem hat der Berliner Beauftragte für Datenschutz und Informationsfreiheit auf Seite 42 seines Sonderberichts festgestellt, dass **die Polizei hinreichende Sicherheitsmaßnahmen getroffen hat, die teilweise über das allgemein übliche Maß hinausgingen!** In den kürzlich erlassenen neuen „Dateienrichtlinien“ haben wir geregelt, dass das Ergebnis einer Vorabkontrolle nach § 5 Abs. 3 BlnDSG als Anlage zu der Errichtungsanordnung zu nehmen ist. Damit haben wir eine Anregung des Berliner Beauftragte für Datenschutz und Informationsfreiheit aufgegriffen.
- Die Errichtungsanordnung ist trotz der Nachbesserungsaufforderungen mangelhaft geblieben (§ 49 ASOG i. V. m. § 19 Abs. 2 Nr. 10 BlnDSG).	Die Anordnung wurde mehrfach unter Berücksichtigung der Äußerungen des Berliner Beauftragten für Datenschutz und Informationsfreiheit überarbeitet und jeweils mit Zustimmung der Senatsverwaltung für Inneres erlassen. Teilweise bewertet die Senatsverwaltung für Inneres die Rechtslage etwas anders als der Berliner Beauftragte für Datenschutz und Informationsfreiheit. Außerdem hat die Senatsverwaltung für Inneres einige Grundsatzfragen zur Gestaltung von Errichtungsanordnungen, die sich nach der Änderung des Berliner Datenschutzgesetzes vom 30.07.2001 ergeben haben, nicht im Zusammenhang mit der Errichtung der

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

ohnehin zeitlich befristeten „Terrordatenbank“ erörtert, sondern durch die Neufassung der Dateienrichtlinien geklärt.

- Es wurden nach dem 11. September 2001 übereilt Daten erhoben auf der Grundlage eines vorläufigen Rasters, ohne dass die Voraussetzungen für ein Vorgehen auf der Grundlage von „Gefahr im Verzug” vorgelegen haben. Selbst wenn diese vorgelegen hätten, hätte es an der erforderlichen Anordnung gefehlt (§ 47 Abs. 4 Satz 1 bzw. 4 ASOG).

  Die Polizei hatte etwa eine Woche nach dem Anschlag bereits von einigen Stellen, unter anderem von der HU, die Übermittlung von Daten erbeten, bevor eine richterliche Anordnung vorlag. Dabei konnte die Formulierung des Anschreibens den unzutreffenden Eindruck vermitteln, es handele sich um Ermittlungen im Rahmen eines Verfahrens des Generalbundesanwalts. Diese Schreiben waren unglücklich formuliert. Auch hierbei darf aber nicht der besondere Druck vergessen werden, unter dem die Polizei zu dieser Zeit stand.

- Der erste richterliche Beschluss für die Durchführung der Rasterfahndung enthielt zu unbestimmte bzw. unverhältnismäßige Vorgaben für die Übermittlung personenbezogener Daten (es fehlte beispielsweise die Länderliste ...) (§ 47 Abs. 1, 2 Satz 1 i. V. m. § 9 Abs. 1 BlnDSG).

  Ein unabhängiges Gericht hat entschieden. Die gesamte Materie war für den Richter ebenso neu und unbekannt, wie für alle anderen Beteiligten auch. Das Kammergericht hat letztendlich die vom Amtsgericht getroffene Anordnung der Maßnahme bestätigt.

- Wegen der auf der Grundlage unterschiedlicher Beschlüsse übermittelten Daten gab es keinen einheitlichen Datenbestand. Bei der Speicherung der angelieferten Daten wurden bei Mehrfachübermittlungen alle übermittelten Daten in der „Terror-Datei” gespeichert, ohne dass die zuvor übermittelten Daten gelöscht worden wären (§ 9 Abs. 1 i. V. m. § 5 Abs. 2 Ziff. 2 BlnDSG).

  Aufgrund vor Anlaufschwierigkeiten, der großen angelieferten Datenmenge und der unterschiedlichen Qualität der angelieferten Daten ist bei Mehrfachübermittlungen eine Löschung des zuerst übermittelten Daten unterblieben. Die Polizei hat dies Problem erkannt, so dass es zu keinen nachteiligen Folgen für die betroffenen Personen oder negativen Einflüssen auf die Bewertung der einzelnen Prüffälle gekommen ist. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit stellt auf Seite 34 oben seines Sonderberichts fest, dass die Maßstäbe für die weiteren Aussortierungen ... **dem Datenschutz in besonderer Weise Rechnung trugen.**

Wir hoffen, dass unser Sonderbericht zur Rasterfahndung dazu beitragen wird, die Persönlichkeitsrechte unverdächtiger Personen, die in eine Rasterfahndung geraten, durch eine datenschutzgerechte Anwendung dieser Ermittlungsmethode zu stärken.

4.1.2 Polizeialltag

Videoüberwachung nach Polizeirecht

Der Senat hat einen Entwurf eines Gesetzes zur Änderung des Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG) in das Abgeordnetenhaus eingebracht, in dem eine Möglichkeit geschaffen werden sollte, gefährdete Objekte mit Videotechnik zu überwachen.

Vor dem Hintergrund vielfach erhobener und in anderen Ländern auch umgesetzter Forderungen nach der Einführung von Videoüberwachung im öffentlichen Raum ist zu begrüßen, dass sich die Regelung auf gefährdete Objekte beschränkt. Im Gegensatz zu Regelungen zur Videoüberwachung in den Polizeigesetzen

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

anderer Länder werden allerdings an die Straftaten, deren drohende Begehung die Videoüberwachung rechtfertigen soll, keine erhöhten Anforderungen gestellt. Jede Straftat soll die Videoüberwachung rechtfertigen.

Die allgemeinen Regelungen zur Videoüberwachung im neuen Datenschutzrecht (§§ 6 b BDSG, 31 b BlnDSG) sehen unterschiedliche Schwellen für die bloße Beobachtung und die Speicherung bzw. Aufzeichnung der Daten vor. Im vorliegenden Entwurf werden Übertragung zur Beobachtung und zur Aufzeichnung gleichbehandelt.

Im Gegensatz zu den allgemeinen Regelungen in Datenschutzgesetzen sah der Entwurf keine Information der Betroffenen vor, wenn durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet werden und gesetzliche Gründe dem nicht entgegenstehen. Der Entwurf lässt es zu, dass Videoaufzeichnungen über die zulässige Speicherungsdauer hinaus zur Aus- oder Fortbildung, zu statistischen Zwecken, im Interesse der betroffenen Person zur Behebung einer bestehenden Beweisnot oder zu wissenschaftlichen Zwecken sowie zur historischen Archivierung weiter genutzt werden dürfen. Bei den in Frage stehenden Aufzeichnungen spielen alle diese Zwecksetzungen keine Rolle. Vielmehr muss es dabei bleiben, dass die Aufzeichnungen vernichtet werden, soweit sie nicht zur Verfolgung von Straftaten benötigt werden.

Beide Mängel der Regelung wurden aufgrund unserer Stellungnahme beseitigt.

Dateienrichtlinien

Die Novellierung des Berliner Datenschutzgesetzes machte es erforderlich, dass die *Dateien-richtlinien* (Ausführungsvorschriften zu § 49 ASOG) angepasst werden mussten. Einvernehmen bestand mit der Senatsverwaltung für Inneres darin, dass nach dem ASOG für jede automatisierte Datei über personenbezogene Daten und solche nicht-automatisierten Dateien, aus denen personenbezogene Daten an andere Stellen übermittelt werden, jeweils eine Errichtungsanordnung zu erlassen ist. Das bedeutet, dass nicht nur die Polizeibehörde, sondern auch alle Ordnungsbehörden für diese Dateien mit personenbezogenen Daten Errichtungsanordnungen zu erlassen haben. Die alten Dateienrichtlinien waren zu eng, weil sie sich lediglich auf den Polizeipräsidenten in Berlin bezogen.

Darüber hinaus ist unsere Anregung aufgegriffen worden, die *Errichtungsanordnungen* über die behördlichen Datenschutzbeauftragten zu leiten. Diese Errichtungsanordnungen treten an die Stelle der Dateienübersicht. Auch unsere Empfehlung, die Ergebnisse der vom behördlichen Datenschutzbeauftragten unter bestimmten Voraussetzungen durchzuführenden Vorabkontrolle in die Errichtungsanordnung aufzunehmen,

Die Darstellung ist zutreffend.

Die neuen Dateienrichtlinien sind am 17. Februar 2003 in Kraft getreten; sie wurden im Amtsblatt für Berlin Nr. 10 vom 07. März 2003 auf Seite 820 veröffentlicht.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

wurde berücksichtigt.

Öffentlichkeitsfahndung im Internet

Auch in diesem Jahr kam es bei den Demonstrationen zum 1. Mai zu Ausschreitungen. Die Polizei hat ihre Videoaufzeichnungen, Fernsehaufnahmen und private Videobänder ausgewertet. Insgesamt wurden 53 Aufnahmen für die Öffentlichkeitsfahndung hergestellt. Diese Bilder sind in das Internet eingestellt worden.

Nach § 131 b Abs. 1 StPO ist die öffentliche Fahndung mit Bildern unbekannter Straftäter bei Straftaten von erheblicher Bedeutung zulässig, wenn die Feststellung der Identität des Straftäters auf anderem Wege erheblich weniger Erfolg verspräche oder wesentlich erschwert wäre.

Die Veröffentlichung von Abbildungen eines Beschuldigten, der einer Straftat von erheblicher Bedeutung verdächtig ist, ist zulässig, wenn die Aufklärung einer Straftat, insbesondere der Feststellung der Identität eines unbekannten Täters, auf andere Weise erheblich weniger Erfolg versprechend oder wesentlich erschwert wäre (§ 131 b Abs. 1 stop).

Die Verpflichtung der Staatsanwaltschaft, ihr bekannt gewordene Straftaten aufzuklären, verlangt, dass sie von den ihr gesetzlich zustehenden Kompetenzen im vorgesehenen Umfang Gebrauch macht. Sie kann als Ausfluss des Legalitätsgrundsatzes nicht auf die ihr zur Verfügung stehenden, erfolgsversprechenden Aufklärungsmöglichkeiten verzichten.

Straftaten von erheblicher Bedeutung sind:

- Verbrechen und
- Vergehen, die aufgrund ihrer Begehensweise, ihrer Dauer oder Schwere geeignet sind, den Rechtsfrieden besonders zu stören (§ 17 Abs. 3 ASOG)

Der Beschuldigte ist möglichst genau zu bezeichnen und – soweit erforderlich – zu beschreiben. Die Tat, derer er verdächtig ist, Ort und Zeit ihrer Begehung sowie Umstände, die für die Ergreifung von Bedeutung sein können, können angegeben werden. *Öffentlichkeitsfahndungen* dürfen nur durch den Richter, bei Gefahr im Verzug auch durch die Staatsanwaltschaft und ihre Hilfsbeamten angeordnet werden. Die richterliche Anordnung lag vor. Die andauernde Veröffentlichung in elektronischen Medien, also im Internet, ist damit grundsätzlich zulässig (§ 131 c Abs. 2 StPO).

Die Internet-Fahndung hat insgesamt 53 Verfahren betroffen. Unter den 53 Verfahren gab es mehrere Fälle, in denen es um Plünderungen i.S.d. §125a S.2 Nr.4 StGB ging. Der besonders schwere Fall des Landfriedensbruchs gem. § 125 a StGB ist eine Straftat von erheblicher Bedeutung im Sinne von § 131 b StPO; als Regelstrafrahmen ist daher eine Mindestfreiheitsstrafe von 6 Monaten vorgesehen.

Bei den neuen Regelungen zur Öffentlichkeitsfahndung ist der Verhältnismäßigkeitsgrundsatz zu berücksichtigen. Durch die Erörterung von Ermittlungsverfahren und die Einstellung von Bildern in den Publikationsorganen entsteht die Gefahr einer erheblichen Rufschädigung. Das gilt insbesondere für Unschuldige. Diese Gefahr ist bei der Qualität der Bilder von besonderer Bedeutung. Mit zunehmender Verbreitung des Internet gilt dies in wachsendem Maße auch für die Nutzung dieses elektronischen Mediums zu Fahndungszwecken. Die spätere Resozialisierung des Täters oder der Täterin kann durch unnötige Publizität des Falles schon vor der Fahndung erschwert werden. Eine Bloßstellung oder Schädigung der Tatverdächtigen muss nicht nur in deren Interesse, sondern auch im Interesse der Strafrechtspflege möglichst vermieden werden.

Da es sich bei § 125 a StGB um ein Regelbeispiel handelt, ist zwar immer im Rahmen des Gesamtgeschehens zu prüfen, ob das konkrete Tatbild die Indizwirkung des Regelbeispiels bestätigt bzw. Umstände vorliegen, die den Sachverhalt als atypische Fallkonstellation erscheinen lassen. Solche Anhaltspunkte haben sich weder für den Dezernenten der Staatsanwaltschaft noch für das Amtsgericht Tiergarten, welches in allen Fällen gemäß § 131 c StPO die Öffentlichkeitsfahndung angeordnet hat, ergeben.

Daher ist stets zu prüfen, ob den Tatverdächtigen oder anderen Betroffenen drohende Nachteile dadurch vermindert werden können, dass nur Medien von geringerer Breitenwirkung in Anspruch genommen werden,

dass andere Formen der Öffentlichkeitsfahndungen wie Plakate, Handzettel oder Lautsprecherdurchsagen gewählt werden oder dass die Fahndungshilfe örtlich oder in anderer Weise, etwa durch Verzicht auf die Verbreitung von Bildern der Gesuchten, beschränkt wird. Bei der Nutzung des Internet zu Fahndungszwecken ist außerdem zu berücksichtigen, dass die im Internet eingestellten Daten weltweit abrufbar sind. Sobald das Fahndungsziel erreicht ist oder die Ausschreibungsvoraussetzungen aus sonstigen Gründen nicht mehr vorliegen, ist die Nutzung des Internet zu Fahndungszwecken unverzüglich zu beenden.

Das Berliner Abgeordnetenhaus hat zur Sicherstellung der Verhältnismäßigkeit in einem Beschluss zu unserem Jahresbericht 1998[70] festgestellt, dass Öffentlichkeitsfahndungen im Internet eine noch stärkere Eingriffsintensität als herkömmliche Fahndungsmaßnahmen aufweisen. Dem Grundsatz der Verhältnismäßigkeit muss aus diesem Grund in besonderem Maße Rechnung getragen werden. Daher hat das Abgeordnetenhaus den Senat aufgefordert – wenn schon auf Personenfahndung im Internet als ultima ratio nicht verzichtet werden kann –, folgende Kriterien einzuhalten:

- Anordnung nur bei Schwerstkriminalität,
- Ergreifung erscheint auf andere Weise aussichtslos,
- Anordnung durch die Staatsanwaltschaft und
- Schaffung einer sicherheitstechnischen Infrastruktur, die die Unverfälschbarkeit der veröffentlichten Daten sicherstellt (Verwendung von digitalen Unterschriften und digitalen Wasserzeichen sowie Überprüfungsmöglichkeiten durch Internet-Benutzer) und Zugriffsschutzmechanismen vorsieht.

– Im vorliegenden Fall hatte die Ermittlungsgruppe Video der Polizei das jeweils beste Bild zu den Bildsequenzen der einzelnen Straftäter ausgesucht. Zusammen mit einem einheitlichen Vorblatt und einer Beschreibung des Geschehenablaufs wurden sie an die Staatsanwaltschaft übermittelt. Diese beantragte beim Amtsgericht Tiergarten eine Öffentlichkeitsfahndung (§§ 131 b, 131 c StPO), die in allen Fällen angeordnet wurde.

Auf Anweisung der Staatsanwaltschaft wurden daraufhin die Bilder aller Straftäter unabhängig von der einzelnen Straftat und der Bildqualität ins Internet eingestellt. Dies wurde damit begründet, dass in allen Fällen der Tatbestand des besonders schweren Landfriedensbruchs (§ 125 a StGB) erfüllt sei.

[70] Anlage 1 zum JB 2001

Wir haben Zweifel, ob der Verhältnismäßigkeitsgrundsatz in ausreichender Weise berücksichtigt wurde. Selbst wenn die vorgeworfenen Straftaten als „besonders schwerer Landfriedensbruch" zu werten sind, muss im Hinblick auf die Tatausführung unterschieden werden. Der Steinwurf auf einen Polizeibeamten – also auf eine Person – muss anders bewertet werden als der Diebstahl eines Sixpacks Bier aus dem Supermarkt. Es hätte also jeder Fall einzeln im Hinblick auf die Risiken des Internet geprüft werden müssen.

Die Staatsanwaltschaft hat demgegenüber auf das Strafmaß für „besonders schweren Landfriedensbruch" (sechs Monate bis zu zehn Jahren) hingewiesen. Sie hält dies für eine Straftat von erheblicher Bedeutung. Weil es sich in allen Fällen um die gleichen Delikte handelte, sieht die Staatsanwaltschaft keine Veranlassung für eine Differenzierung bei der Abwägung, ob die Öffentlichkeitsfahndung im Internet noch verhältnismäßig ist.

Einvernehmen bestand mit der Staatsanwaltschaft darüber, dass nicht aktenkundig gemacht wurde, dass die Fotos in das Internet eingestellt wurden. Ebenso ist den Vorgängen nicht zu entnehmen, wer die Anordnung getroffen hat. Die Staatsanwaltschaft hat eingeräumt, dass die Dokumentation unzureichend war. Sie hat zugesagt, dass Bilder von Personen, die sich gestellt haben oder die identifiziert wurden, unverzüglich aus dem Internet herausgenommen werden. Die gesamte Aktion der Öffentlichkeitsfahndung im Internet war ohnehin bis Ende des Jahres befristet. Diese Frist wurde allerdings nicht eingehalten.

Nicht beschuldigt und trotzdem im Polizeicomputer

Bei einem Verwaltungsstreitverfahren wegen einer Gefährderansprache zum 1. Mai ist einem Bürger ein Auszug aus den Personenerkenntnissen des Polizeilichen Staatsschutzes bekannt geworden. Dort konnte er lesen, dass er an einer zum Teil gewalttätig verlaufenen Demonstration in Sachsen teilgenommen hat und bei der Anfahrt zur Anti-JN-Demonstration in Frankfurt/Oder am Bahnhof mit einem „Schlagstock" angetroffen wurde. Er und andere „Linke" seien mit „Rechten" in Streit geraten und danach in einen Baumarkt geflohen, wo eine Verkäuferin mit Tränengas besprüht wurde. Der „Schlagstock" war ein ca. 40 Zentimeter langer Holzstock, an dem mit Reißzwecken provisorisch ein schwarz-rotes Tuch angebracht war. Bei der Auseinandersetzung in dem Baumarkt ließ sich der Sachverhalt nicht mehr klären, da die Beteiligten die Aussage verweigerten. Die Staatsanwaltschaft hat das Verfahren eingestellt.

Die Speicherung begründet die Polizei damit, dass bei der Demonstration in Sachsen eine Identitätsfeststellung durchgeführt wurde. Im Zuge der zum Teil gewalttätigen Demonstration wurden Straftaten began-

Der geschilderte Sachverhalt vermengt drei zeitlich verschiedene Vorgänge, die zu differenzieren sind:

- Die Teilnahme an einer zum Teil gewalttätig ver-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

gen, wobei kein konkreter Tatverdacht gegen den Bürger bestand. Die Polizei schließt allerdings nach der Einschätzung der Persönlichkeit des Bürgers nicht aus, dass er Straftaten begangen haben könnte und dabei unerkannt geblieben ist. Erkenntnisse zu bekannten gewalttätigen Straftätern, die der militanten linksextremistischen Szene zuzuordnen sind und aufgrund polizeilicher Maßnahmen zur Gefahrenabwehr gewonnen wurden, dienen der vorbeugenden Straftatenbekämpfung. Erkenntnisse über Reisebewegungen oder Personenbeziehungen im Zusammenhang mit Straftaten sollen zukünftige Ermittlungen fördern.
Wir haben die Auffassung vertreten, dass im Zusammenhang mit der *Demonstration* in Sachsen keine straf- oder polizeirechtlich relevanten Tatsachen geltend gemacht werden, die die Annahme rechtfertigen, dass der Bürger Straftaten begehen wird. Subjektive Vermutungen oder Befürchtungen ohne jeden Tatsachenbeleg sind hier nicht ausreichend. Mit der Begründung, dass der Bürger Straftaten begangen haben könnte und dabei unerkannt geblieben ist, ließe sich jede Datenspeicherung rechtfertigen.

Die Polizei hält die Speicherung der Daten gleichwohl für erforderlich.

laufenen Demonstration in Sachsen,

- das Angetroffenwerden im Vorfeld einer Demonstration mit einem Holzstock,

- sowie die geschilderte Auseinandersetzung in dem Baumarkt

–

In den Fällen zu 2. und 3. wurden gegen den Petenten Ermittlungsverfahren wegen Verdachts des Verstoßes gegen das Versammlungsgesetz bzw. wegen Verdachts der gefährlichen Körperverletzung geführt. Der Petent war somit in diesen beiden Fällen Beschuldigter in den jeweiligen Ermittlungsverfahren, so dass die Überschrift des Berichtsteils so nicht zutrifft.

Zwar wurden die Verfahren von der Staatsanwaltschaft eingestellt, weil dem Petenten die zur Last gelegten Vorwürfe nicht nachgewiesen werden konnten, dennoch blieb in beiden Fällen ein Resttatverdacht bestehen, der die weitere Datenspeicherung rechtfertigt. Hierbei ist eine Gesamtwürdigung der Person vorzunehmen, die der Berliner Beauftragte für Datenschutz und Informationsfreiheit außer Acht lässt:

Der Betroffene ist eine amtsbekannte Person aus dem gewalttätigen linksextremistischen Spektrum. Gegen ihn wurden im Zeitraum von 1994 bis 2000 **20 Ermittlungsverfahren** geführt, die im Zusammenhang mit seiner Zugehörigkeit zur linken Szene stehen.

Allein schon die Vielzahl der gegen den Betroffenen geführten Strafermittlungsverfahren sowie die Art und Ausführung der Taten als auch die Anbindung an die linksextremistische gewalttätige Szene begründen nach kriminalistischer und kriminologischer Erfahrung die Gefahr der Wiederholung von strafbaren Handlungen.

Vor diesem Hintergrund ist die Datenspeicherung zur vorbeugenden Bekämpfung von Straftaten zulässig.

Verbesserung bei den Aktenauskünften

Der Polizeipräsident hat in der Vergangenheit den Betroffenen bei Anträgen auf Auskunft über die zur Person gespeicherten Daten keine Mitteilung über die Empfänger von Datenübermittlungen und die Herkunft der Daten gemacht. So wurde beispielsweise den Rechtsanwälten von Globalisierungsgegnern die Auskunft darüber verweigert, woher die bei der Berliner Polizei vorliegenden Informationen über die Vorfälle in Göteborg (Schweden) stammen und was im Vorfeld an die schwedischen Behörden übermittelt wurde.

Der Polizeipräsident hat dies damit begründet, dass die Datenübermittlungen nicht vom *Auskunftsanspruch* umfasst werden (§ 50 ASOG). Er stützt das im Wesentlichen darauf, dass – entgegen der durch das ASOG suspendierten vergleichbaren Vorschrift im Berliner Datenschutzgesetz (§ 16 Abs. 1 BlnDSG) – dort nicht

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

ausdrücklich die Pflicht geregelt ist,

- den Zweck und die Rechtsgrundlage der Verarbeitung,

- die Herkunft der Daten und die Empfänger von Übermittlungen innerhalb der letzten zwei Jahre und

- den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten

darzulegen.

Diese Auffassung teilen wir nicht. Das Gesetz spricht hinsichtlich des Auskunftsrechtes zwar nur von „gespeicherten Daten"; eine Gefährdung besonderer Art besteht jedoch gerade bei der Übermittlung personenbezogener Daten mit anschließender weiterer Nutzung durch den Empfänger – unabhängig davon, ob die erhebende Stelle die Daten auch selbst gespeichert hat.

Der Begriff der „gespeicherten Daten" muss hier deshalb trotz des Wortlautes der Bestimmung dahingehend verstanden werden, dass die Ordnungsbehörden und die Polizei der betroffenen Person gerade auch über solche Daten Auskunft erteilen müssen, die sie an eine andere Stelle übermittelt haben. Wenn diese Behörden schon verpflichtet sind, Auskunft über die von ihnen selbst gespeicherten Daten zu erteilen, dann müssen sie es erst recht hinsichtlich solcher Daten sein, die sie an Dritte übermittelt haben.

Außerdem muss auch unter dem Aspekt der verfassungskonformen Auslegung wegen der Bedeutung des informationellen Selbstbestimmungsrechtes – vor allem im Rahmen automatisierter Datenverarbeitung – das Auskunftsrecht (§ 50 Abs. 1 Satz 1 ASOG) über den Wortlaut der Regelung hinaus auf die Phasen der Datenerhebung, -übermittlung und weiteren Nutzung ausgedehnt werden. Das Bundesverfassungsgericht hat im Volkszählungsurteil festgestellt, dass mit dem Recht auf informationelle Selbstbestimmung eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar wären, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Diesen Grundsätzen wäre nicht genügend Rechnung getragen, wenn das Auskunftsrecht des Betroffenen nur auf die Datenspeicherung beschränkt würde, zumal Einschränkungen dieses Rechtes nur im überwiegenden Allgemeininteresse, d. h. aus übergeordneten Individual- oder Gemeinschaftsinteressen, hinnehmbar sind.

Sollten im Einzelfall das öffentliche Interesse an der Geheimhaltung oder ein überwiegendes Geheimhaltungsinteresse eines Dritten an den Datenübermittlungen das schutzwürdige Interesse des Betroffenen an der Auskunft überwiegen, kann die Mitteilung darüber (§ 50 Abs. 2 ASOG) verweigert werden.

Der Senat teilt die Auffassung des Polizeipräsidenten in Berlin, dass § 50 ASOG von seinem insoweit eindeutigen Wortlaut her lediglich die Auskunft über die in Berliner Dateien gespeicherten Daten, nicht jedoch ihre Übermittlung an Dritte umfasst. § 16 BlnDSG, der eine solche Auskunftsverpflichtung festlegt, ist gemäß § 51 ASOG bei der Aufgabenerfüllung nach dem ASOG ausdrücklich suspendiert; insoweit hat die bereichsspezifische Regelung des § 50 ASOG, die bewusst nicht so weitreichend formuliert wurde wie der § 16 BlnDSG, Vorrang. Die Polizei ist somit grundsätzlich nicht verpflichtet, dem Auskunftsberechtigten mitzuteilen, an wen die Daten übermittelt, bzw. von wem die Daten empfangen wurden. Kriminalistischer Hintergrund hierzu ist die Verhinderung der gerade in den Fällen der Globalisierungsgegner deutlich gewordenen Ausforschungsversuche zu den Informationsbeziehungen der Polizeien. Andererseits ist die Polizei auch nicht gehindert, im Einzelfall – unbeschadet der Regelung des § 50 Abs. 2 ASOG - nach ihrem Ermessen auch über Datenübermittlungen Auskunft zu erteilen, wenn kriminalistische Erwägungen nicht dagegen sprechen. So wird in der polizeilichen Praxis auch verfahren.

Die internationale Zusammenarbeit ist im Bundeskriminalamtgesetz (BKAG) geregelt. Dem Bundeskriminalamt (BKA) obliegt der zur Verhütung oder Verfolgung von Straftaten erforderliche Dienstverkehr der Polizeien des Bundes und der Länder mit den Polizei- und Justizbehörden sowie sonstigen insoweit zuständigen öffentlichen Stellen anderer Staaten (§ 3 BKAG). Diese Vorschrift dürfte auch den Rechtsanwälten bekannt sein. Eine Offenlegung von Informationswegen können wir bei der klaren Rechtslage ebenso wenig erkennen wie einen Ausforschungsversuch.

Unabhängig davon hatte uns der Polizeipräsident in Berlin zu anderen Auskunftsersuchen Betroffener mitgeteilt, dass die Berliner Polizei im Vorfeld des EU-Gipfels in Göteborg keine personenbezogenen Daten nach Schweden übermittelt hat. Was daran geheimhaltungsbedürftig ist, blieb uns verschlossen.

Der Polizeipräsident hat schließlich seine Einwände fallen gelassen und eingewilligt, dass wir den Rechtsanwälten die Herkunft der Daten nennen.

In einem anderen Fall – die Verwendung eines Textbausteines lässt die Vermutung zu, dass in gleichgelagerten Fällen regelmäßig so verfahren wurde – hat die Polizei mitgeteilt, dass sich in den Kriminalakten Kopien der staatsanwaltschaftlichen Ermittlungsakten befinden. Über diese wird keine Auskunft erteilt, da ansonsten die strafprozessualen Vorschriften über das Akteneinsichtsrecht unterlaufen würden.

Diese Begründung ist unzutreffend. Es handelt sich beim Aktenrückhalt in der kriminalpolizeilichen Personenakte nicht mehr um Daten, die in den Anwendungsbereich der Strafprozessordnung (StPO) fallen. Die Polizei kann – soweit Bestimmungen der StPO oder anderer gesetzlicher Regelungen nicht entgegenstehen – personenbezogene Daten, die sie im Rahmen von strafrechtlichen Ermittlungen gewonnen hat, speichern, verändern und nutzen, soweit es zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten, erforderlich ist (§ 42 Abs. 3 ASOG). Die Polizei hat nach pflichtgemäßem Ermessen zu prüfen, welche Erkenntnisse aus den strafrechtlichen Ermittlungen für die Gefahrenabwehr nach Polizeirecht erforderlich ist. Somit stellt sich vielmehr die Frage, ob komplette Retente von Ermittlungsakten überhaupt zu diesem Zweck erforderlich sind.

Der Polizeipräsident hat eingeräumt, dass die von ihm gewählte Formulierung missverständlich ist, und hat sich unserer Auffassung angeschlossen.

Speicherung von Daten aus einem anderen Land

Einem Bürger sind die bei der Polizei zu seiner Person gespeicherten Daten bekannt geworden. So ist dort

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

unter anderem festgehalten, dass er an einer Veranstaltung in Fürstenwalde/Brandenburg teilgenommen hatte. Er wollte nun wissen, ob diese Speicherung überhaupt zulässig ist und woher die Daten stammen.

Die Berliner Bereitschaftspolizei war zur Unterstützung der brandenburgischen Polizeikräfte eingesetzt worden. Den Berliner Polizeibeamten waren mehrere an der Veranstaltung teilnehmende Personen von verschiedenen Einsätzen her persönlich bekannt. Die Beobachtungen sind in einem Bericht zusammengefasst und von der Bereitschaftspolizei dem Berliner Staatsschutz übermittelt worden. Dort werden personenbezogene Daten aus polizeilichen Aufklärungsberichten über Demonstrationen gespeichert, die entweder nicht friedlich verliefen oder bei denen aus polizeilicher Erfahrung und Prognose die Gefahr gewalttätiger Auseinandersetzungen zwischen „Rechten" und „Linken" oder „Linken" mit der Polizei – beispielsweise bei Anti-NPD-Demonstrationen – bestand. Die Erkenntnisse dienen sowohl der vorbeugenden Straftatenbekämpfung – beispielsweise für Gefährderansprachen – als auch der Dokumentation und späteren Auswertung der Ereignisse.

Die Darstellung ist zutreffend**.**

Nach Erörterung der Thematik im Unterausschuss „Recht und Verwaltung" des Arbeitskreises II „Innere Sicherheit" der ständigen Konferenz der Innenminister und –senatoren der Länder bestand einhellige Ansicht darüber, dass

- Befugnisnorm für die Erhebung personenbezogener Daten anlässlich von Demonstrationen (einschließlich „An- und Abströmphase") § 12 a i.V.m. § 19 a VersG ist,

- alle anlässlich des Einsatzes erhobenen Daten/Unterlagen nach Beendigung des Einsatzes der aktenführenden Dienststelle des unterstützten Bundeslandes zu übergeben sind. Dies kann mit dem Ersuchen verbunden werden, Daten an das unterstützende Bundesland zu übermitteln;

Berliner Polizeikräfte dürfen auf dem Hoheitsgebiet eines anderen Bundeslandes nur dann tätig werden, wenn es das jeweilige Landesrecht zulässt. Die im Land Brandenburg eingesetzten Berliner Polizeibeamten haben bei einem dortigen Einsatz die gleichen Befugnisse wie die Brandenburger Kollegen. Ihre Amtshandlungen gelten dann als Maßnahmen der Brandenburger Polizei. Die Brandenburger Polizei ist den Berliner Polizeikräften gegenüber weisungsbefugt. Die von Berliner Polizeikräften getroffenen Maßnahmen sind daher keine Berliner, sondern Brandenburger Amtshandlungen.

- die Erhebung von personenbezogenen Daten bei friedlich verlaufenden Demonstrationen nur in Ausnahmefällen (Vorliegen von Erkenntnissen über die Person des Teilnehmers, der in der Vergangenheit mehrfach als Störer in Erscheinung getreten ist, sowie von tatsächlichen Anhaltspunkten – polizeiliche Erfahrungswerte -, die erneutes Störerverhalten erwarten lassen) zulässig, die Speicherung dieser Daten über das Ende der Veranstaltung hinaus unzulässig ist. Eine „Mitnahme" (Datenübermittlung an die unterstützende Behörde) von personenbezogenen Daten aus diesen Anlässen ist somit grundsätzlich unzulässig;

Eine der Amtshandlungen war die Zusammenfassung der Aufklärungsergebnisse und die Übermittlung an den Berliner Staatsschutz. Ob die Erhebung der Daten erforderlich und die Datenübermittlung rechtmäßig war, hat der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg zu bewerten. Seine Prüfung ist noch nicht abgeschlossen. Wir haben allerdings Zweifel an der Erforderlichkeit und damit der Zulässigkeit der Erhebung der Daten über die Teilnehmer der offensichtlich friedlich verlaufenden Veranstaltung und der sich anschließenden Datenübermittlung. Offen ist in diesem Zusammenhang, ob die Brandenburger Polizei überhaupt Kenntnis von dieser Datenübermittlung hat.

- Unterstützungskräfte, die nach Maßgabe der Rechtsvorschriften des unterstützten Landes selbst personenbezogene Daten erheben, nur befugt sind, um Übermittlung zur Erfüllung eigener Aufgaben zu bitten, wenn die Voraussetzungen für die Datenerhebung auch nach eigenem Landesrecht vorgelegen hätten;

- vor der „Mitnahme" von personenbezogenen Daten die unterstützte Behörde in jedem Einzelfall das Übermittlungsersuchen nach ihrem Landesrecht prüfen muss; eine „Mitnahme" ohne ausdrückliches Einverständnis des ersuchten Landes ist nicht zulässig;

Die Senatsverwaltung für Inneres teilt unsere Rechtsauffassung, dass sich die Zulässigkeit der Datenerhebung und -übermittlung nach brandenburgischem Recht richtet und der Vorgang der Kontrollbe-

- die Speicherung und weitere Nutzung der übermittelten Daten sich nach den Rechtsvorschriften des unterstützenden Landes richtet und der Kontrolle des dortigen Landesdatenschutzbeauftragten unter-

fugnis des Datenschutzbeauftragten des Landes Brandenburg unterliegt. Dem hat sich auch der Unterausschuss „Recht und Verwaltung" des Arbeitskreises II „Innere Sicherheit" der Ständigen Konferenz der Innenminister und -senatoren der Länder angeschlossen. Die in Fürstenwalde über den Bürger erhobenen Daten wurden gelöscht.

Der Polizeipräsident in Berlin, der die Berichte bisher anlassbezogen abgelegt hat, wird künftig retrograd diese Unterlagen, die eine Vielzahl von personenbezogenen Daten unterschiedlicher Personen enthalten, nun personenbezogen in die Sammlung des Staatsschutzes einstellen. Dabei wird in jedem Einzelfall geprüft, ob zu dieser Person bereits Daten als Beschuldigter oder Tatverdächtiger beim Staatsschutz gespeichert sind; sofern dies nicht der Fall ist, werden keine weiteren Daten gespeichert.

Polizei übermittelt die Daten von NPD-Gegnern an die Partei

Der Presse war zu entnehmen, dass die Abteilung Staatsschutz des Landeskriminalamtes die Namen von 23 NPD-Gegnern an den Landesgeschäftsführer der Partei weitergegeben hat. Diese Personen sollen im September 2001 deren Wahlkampfplakate beschädigt haben.

Das Landeskriminalamt hat im September und Oktober 2001 in acht Fällen gegen 23 Personen wegen Sachbeschädigung (§ 303 StGB) an Wahlplakaten der NPD strafrechtliche Ermittlungen geführt. Die Datenübermittlung hat es damit gerechtfertigt, dass es sich dabei um ein Antragsdelikt handelt und der Geschädigte zur sachgemäßen Antragstellung in der Lage sein muss. Hierzu müsse er Tatsachen kennen, die einen Schluss auf die wesentlichen Tatumstände und den Täter zulassen. Mit dem in der Presse zitierten Schreiben sind die Verantwortlichen der NPD um Prüfung gebeten worden, ob sie einen Strafantrag gegen die aufgeführten Beschuldigten stellen wollen. Die Abwägung mit den schutzwürdigen Interessen der Betroffenen führte zu dem Ergebnis, dass lediglich Namen und Vornamen der Beschuldigten an die NPD weitergegeben wurden. Eine Dokumentation darüber erfolgte nicht.

Wir haben den Vorgang beanstandet. Grundsätzlich sollen bei Strafantragsdelikten bis zur Entscheidung, ob ein Strafantrag gestellt wird (Nr. 6 Abs. 1 Richtlinien für das Straf- und Bußgeldverfahren - RiStBV -), keine Ermittlungen geführt werden, es sei denn, ein Beweismittelverlust sei zu befürchten. Die Entscheidung, ob der Antragsberechtigte von der Straftat, dem Antragserfordernis und den Tatverdächtigen informiert wird, obliegt der Staatsanwaltschaft bei dem Landgericht Berlin (Nr. 6 Abs. 2 RiStBV), die bei ihrer Entscheidung zu berücksichtigen hat, ob ein öffentliches Interesse an der Strafverfolgung besteht.

liegt.

- Der Polizeipräsident in Berlin wurde gebeten, diese Grundsätze künftig zu beachten.

Es trifft zu, dass entsprechend der genannten Regelungen in den RiStBV (Nr. 6 Absatz 2) und in der StPO (§§ 406 e und 478) die Benachrichtigung des Antragsberechtigten über die Tat und ggfs. über den Tatverdächtigen grundsätzlich von der Staatsanwaltschaft vorzunehmen ist. Allerdings hatte der Berliner Beauftragte für Datenschutz und Informationsfreiheit zum Zeitpunkt der Berichtserstellung noch keine Kenntnis von der **Geschäftsanweisung LKA Nr. 1/2001 über die Bearbeitung von Delikten der Kleinkriminalität,** die das Vorgehen der Berliner Polizei im Rahmen der hier in Rede stehenden Bearbeitung von Antrags- und Privatklagedelikten verbindlich für alle Polizeivoll-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Die Tatsache, dass diese Benachrichtigung von der Staatsanwaltschaft vorzunehmen ist, korrespondiert mit den Vorschriften der §§ 406 e und 478 StPO, wonach über die Erteilung von Auskünften aus Ermittlungsakten die Staatsanwaltschaft entscheidet. Anhaltspunkte dafür, dass im hier konkret vorliegenden Fall oder auch durch eine generelle Absprache mit der Staatsanwaltschaft das Landeskriminalamt zur Übermittlung der Namen von Verdächtigen auf Grundlage des § 478 Abs. 3 StPO ermächtigt worden war, liegen nicht vor. Die von dem Polizeipräsidenten in Berlin vertretene Auffassung, dass auch bei einer Zeugenladung des Geschädigten durch die Polizei die Namen des Beschuldigten mitgeteilt werden, gibt im konkreten Fall keine Veranlassung, den Sachverhalt rechtlich anders zu bewerten, da nach den RiStBV bis zu der Entscheidung, ob ein Strafantrag gestellt werden soll, gerade grundsätzlich keine Ermittlungshandlungen vorgenommen werden sollen.

zugsbeamten regelt. Diese Geschäftsanweisung, die mit dem Generalstaatsanwalt bei dem Landgericht Berlin abgestimmt wurde, enthält u.a. die Ermächtigung der Polizei, die Verletzten/ Geschädigten u.a über Namen ggfs. ermittelter Beschuldigter zu benachrichtigen.

Die Geschäftsanweisung sieht die Belehrung des Verletzten/ Geschädigten über die Möglichkeit der Privatklage bzw. die Strafantragstellung vor. Diese Belehrung erfolgt durch die Aushändigung eines Schreibens bei der Anzeigeerstattung oder durch Zusendung dieses Schreibens an den Betroffenen. Bei dem standardisierten Schreiben handelt es sich aus arbeitsökonomischen Gründen um eine Durchschrift des beigefügten Strafanzeige-Vordrucks für Antrags- und Privatklagedelikte oder – im Falle der Verwendung eines anderen Strafanzeige-Vordrucks – das der Geschäftsanweisung als Anlage beigefügte Muster eines Belehrungsschreibens. Beide Schreiben sehen die Mitteilung des Namens eines ggfs. Ermittelten Beschuldigten an den Verletzten/ Geschädigten der Straftat vor. Mit dieser Mitteilung wird der Berechtigte in die Lage versetzt zu entscheiden, ob er Strafantrag stellen will, was in vielen Fällen maßgeblich auch von der Identität des Schädigers abhängt (so z.B. im Bereich der Antragsdelikte, die sich im familiären Bereich abspielen).

Der Anwendungsbereich und damit die beschriebene Verfahrensweise beschränkt sich auf Delikte der sog. Kleinkriminalität. Ausgeschlossen sind u.a. Ermittlungsvorgänge mit politischem, religiösem, rassistischem, fremdenfeindlichem oder sexuellen Bezug, für die insoweit keine staatsanwaltschaftliche Ermächtigung der Polizei zur Auskunftserteilung gegenüber dem Verletzten/ Geschädigten gegeben ist.

Im beanstandeten Fall ist die Geschäftsanweisung außer acht gelassen worden. Die Personendaten der Beschuldigten wären der NPD also bei Einhaltung der Vorschrift durch die Polizei nicht übermittelt worden; etwaige Auskünfte hätten allein durch die Staatsanwaltschaft erfolgen dürfen.

Die Senatsverwaltung für Justiz hat auf entsprechende Nachfrage erklärt, dass an dem bisherigen Verfahren auf der Grundlage der GA LKA Nr. 1/2001 festgehalten werden soll. Vor dem Hintergrund, dass diese Regelung in Übereinstimmung mit der Staatsanwaltschaft Berlin zustande gekommen ist und Einigkeit darin bestehe, dass der hier vorliegende Fall der Übermittlung von Namen von NPD-Gegnern an die Partei hiervon nicht umfasst war, hält sie eine Änderung der Geschäftsanweisung für nicht notwendig. Insbesondere böte die GA bei ihrer Einhaltung Gewähr dafür, dass in bedeutsamen Verfahren die Staatsanwaltschaft frühzeitig eingebunden werde und einzelfallbezogen über die Auskunftserteilung entscheide. Diese Auffassung wird von der Senatsverwaltung für Inneres geteilt. Gleichwohl wurde die Polizei nochmals auf die gebotene Einhaltung der bestehenden Vorschriften und die Be-

achtung der staatsanwaltlichen Befugnisse insbesondere in Fällen politisch motivierter Straftaten hingewiesen.

4.2 Ordnungsverwaltung

4.2.1 Melde- und Personenstandswesen

Meldegesetz – eine unendliche Geschichte

Wir haben in den letzten Jahren wiederholt darüber berichtet, dass Berlin, das im Jahr 1985 ein fortschrittliches *Meldegesetz* geschaffen hatte, seit Jahren das Schlusslicht in der Bundesrepublik bildet: Es sind bisher weder die Änderungen des Melderechtsrahmengesetzes von 1994 noch von 2000 oder 2002 in Landesrecht umgesetzt worden. Auch inzwischen drei Beschlüsse des Abgeordnetenhauses von Berlin, mit denen der Senat aufgefordert wurde, einen entsprechenden Gesetzentwurf vorzulegen, blieben bisher unbeachtet. Auf den vom Staatssekretär der Senatsverwaltung für Inneres im Unterausschuss „Datenschutz und Informationsfreiheit" des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses von Berlin am 11. Juni 2002 zugesagten Entwurf für den Herbst 2002 warten wir noch heute.

Alle Bundesländer – so auch Berlin – sind zurzeit dabei, die landesrechtlichen Regelungen für die Umsetzung der umfangreichen Novelle des Melderechtsrahmengesetzes aus dem Jahr 2002 zu erarbeiten, womit insbesondere die Nutzung moderner Informations- und Kommunikationstechnologien im Meldewesen verbunden sein wird. Um eine zielorientierte Umsetzung der rahmenrechtlichen Vorgaben in Landesrecht zu gewährleisten, wurde auf Bund-Länder-Ebene eine Projektgruppe zur Prüfung eingerichtet, welche rechtlichen und technischen Vorraussetzungen geschaffen werden müssen, damit Meldedaten mittels einer automatisierten Datenübertragung reibungslos zwischen den Meldebehörden ausgetauscht werden können, und in welcher Form es möglich ist, die elektronische Anmeldung und die Melderegisterauskunft über das Internet bei den Meldebehörden weitgehend einheitlich zu gestalten. Die in zwei Berichten erarbeiteten Empfehlungen der Projektgruppe werden von der Innenministerkonferenz des Bundes und der Länder auf ihrer nächsten Sitzung abschließend behandelt werden.

Die Projektgruppe hält es u.a. für notwendig, die technischen und rechtlichen Rahmenbedingungen für den im Meldewesen einzuführenden elektronischen Geschäftsverkehr in einem Musterentwurf für die Landesmeldegesetze zu formulieren, um damit den Ländern Gelegenheit zu geben, bundeseinheitlich die Bedingungen für diesen Geschäftsbereich festzulegen. Der Senat hält es für angezeigt, das Ergebnis dieses Prozesses im Rahmen des Berliner Landesrechts zu berücksichtigen und hält eine hieraus resultierende kurzzeitige weitere Verzögerung der Novellierung des Berliner Landesrechts für hinnehmbar.

Vorgriffsregelungen können Ärger bereiten

Die ledige Mutter eines nichtehelichen Kindes hat festgestellt, dass im Meldedatensatz des Sohnes Daten des nicht personensorgeberechtigten Vaters gespeichert waren, und wollte wissen, ob das zulässig ist.

Durch das 1. Gesetz zur Änderung des Melderechtsrahmengesetzes (1. MRRÄndG) 1994 wurde zugelassen, bei den Eltern die Daten ihrer Kinder bis zur Vollendung des 27. Lebensjahres und umgekehrt bei Personen bis zum vollendeten 27. Lebensjahr die Daten ihrer Eltern zu speichern. Damit wurde die Regelung

Die im Jahresbericht enthaltene Darstellung hinsichtlich der in Berlin praktizierten Vorgriffsregelung ist zutreffend.

Die im Jahr 1994 in Kraft getretene Neuregelung sollte die melderechtlichen Voraussetzungen für die Berück-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

ersetzt, nach der die Daten nur für die Zeit der gesetzlichen Vertretung gespeichert werden dürfen.

Die Regelungen des Melderechtsrahmengesetzes (MRRG) sind nicht unmittelbar anwendbar, sondern stellen eine Vorgabe für den Landesgesetzgeber für die Umsetzung in Landesrecht dar. Die Senatsverwaltung für Inneres hatte jedoch in einer Vorgriffsregelung zugelassen, bereits seit September 1996 so zu verfahren.

Die Rechtslage hat sich durch das 3. MRRÄndG 2002 wieder geändert: Es wird erneut auf den gesetzlichen Vertreter abgestellt. Somit entfällt die Grundlage für die Vorgriffsregelung. Aufgrund der Eingabe der Mutter wurden im Datensatz des Kindes die Angaben zum nicht personensorgeberechtigten Vater gelöscht. Durch die Vorgriffsregelung ist in einer Reihe von Datensätzen diese Verknüpfung zwischen Kind und nicht personensorgeberechtigtem Elternteil vorhanden. Die dadurch erforderlichen Datensatzänderungen zur Bereinigung des Melderegisters werden nach den Ausführungen des Landeseinwohneramtes einige Zeit in Anspruch nehmen.

Wir haben den Vorgang beanstandet. Die Meldebehörde speichert zur Erfüllung ihrer Aufgaben den gesetzlichen Vertreter (Vor- und Familienname(n), akademische Grade, Anschrift und Tag der Geburt) (§ 2 Abs. 1 Nr. 8 Meldegesetz (MeldeG)) sowie – korrespondierend dazu – im Datensatz der Eltern Vor- und Familienname(n), Tag der Geburt und Sterbetag ihrer minderjährigen Kinder (§ 2 Abs. 1 Nr. 15 MeldeG). Bei den Eltern ist nicht ausdrücklich das Personensorgerecht erwähnt; dies ergibt sich allerdings aus der Befugnis zur Speicherung im Datensatz des Kindes.

Damit durften im Datensatz des Kindes die Daten des nicht personensorgeberechtigten Vaters nicht gespeichert werden. Die Änderungen des MRRG sind dabei so lange unerheblich, bis sie in Landesrecht umgesetzt wurden.

sichtigung der vielfältigen Eltern-Kind-Beziehungen schaffen, die auch nach Vollendung des 18. Lebensjahres eines Kindes bestehen. Insbesondere sollte damit die Erteilung notwendiger Bescheinigungen für den Bereich der sozialen Sicherung (z.B. an die Zentralstelle für die Vergabe von Studienplätzen) erleichtert werden.

Die Senatsverwaltung für Inneres hielt eine vorgriffsweise Anwendung dieser Regelung für vertretbar, da die Neuregelung nach der Intention des Gesetzgebers eine Begünstigung für die zu registrierenden Einwohner bedeutete. Hinzu kam, dass mit der Vorgriffsregelung verhindert wurde, dass in diesem Bereich im Vergleich zu anderen Bundesländern, die diese Regelung bereits in Landesrecht umgesetzt hatten, unterschiedliche Datensätze entstanden, was anderenfalls bei Umzügen in andere Bundesländer zu Irritationen hätte führen können.

Nach dem Wortlaut der 1994 geschaffenen rahmenrechtlichen Regelung durften im Datensatz von Kindern bis zur Vollendung des 27. Lebensjahres „gesetzliche Vertreter, Eltern von Kindern“ gespeichert werden. Das Landeseinwohneramt Berlin hat als Berliner Meldebehörde im Zuge der vorgriffsweisen Anwendung die Formulierung „gesetzlicher Vertreter, Eltern von Kindern“ als Aufzählung interpretiert mit der Folge, dass auch Elternteile, die kein Personensorgerecht haben, im Datensatz der Kinder gespeichert werden. Diese Interpretation ist auch jedenfalls soweit zweifelsfrei richtig, als Eltern nicht mehr gesetzliche Vertreter ihrer Kinder sind, wenn diese das 18. Lebensjahr vollendet haben.

Mit der im letzten Jahr erneuten Änderung der rahmenrechtlichen Regelung ist klargestellt, dass nunmehr nur noch gesetzliche Vertreter gespeichert werden. Damit entfällt die Grundlage für die in Berlin praktizierte Vorgriffsregelung. Das Landeseinwohneramt wird die entsprechenden Datensätze automatisiert ändern bzw. die Änderungen „fortschreibend“, d.h. beim Zugriff auf den jeweiligen Datensatz, vornehmen.

Bei dem im Jahresbericht geschilderten Einzelfall wurde der Datensatz vom Landeseinwohneramt korrigiert

Und immer wieder Namensverwechslungen

Eine Bürgerin hat von Rechtsbeiständen eines Inkasso-Büros eine Mahnung erhalten, die auch einen „früheren Namen” enthielt. Die Bürgerin widersprach der Mahnung schriftlich und legte dar, dass sie nie diesen Namen getragen habe. Auch einen Vertrag mit dem Gläubiger habe sie nie abgeschlossen. Die Recherchen der Bürgerin haben weiterhin ergeben, dass weder

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Name noch Geburtsdatum oder Adresse der Gesuchten mit ihren eigenen Daten übereinstimmen.

Die Rechtsbeistände haben der Bürgerin mitgeteilt, dass es sich nach nochmaliger Prüfung der Unterlagen um eine Personenverwechslung gehandelt habe. Das ist zurückzuführen auf das Zusammenwirken eines Adressabgleichs mit der Deutschen Post Adress GmbH, die eine neue Anschrift der Schuldnerin – nämlich die der Bürgerin – mitteilte, und einer nicht eindeutigen Auskunft des Landeseinwohneramtes, da es konkrete Fragen zur Identitätsfeststellung mit einer erweiterten Melderegisterauskunft zur Person der Petentin beantwortet hat.

Die Rechtsbeistände haben uns ihr Schreiben an die Meldebehörde zur Verfügung gestellt, mit dem nachgefragt wurde, ob

- die Richtigkeit der ihnen bekannten Daten bestätigt werden kann,
- die gesuchte Person noch in Berlin gemeldet ist und
- eventuell weitere Alt-Anschriften bekannt sind.

– Als Nachweis des berechtigten Interesses war eine Kopie des Titels beigefügt. Das Landeseinwohneramt hat daraufhin Name, Vorname, Geburtsdatum, Anschrift, frühere Anschrift und die Tatsache, dass der frühere Name nicht im Datensatz der Bürgerin enthalten ist, mitgeteilt. Eine mit der Bürgerin namensgleiche Person – allerdings mit dem Geburtsdatum der Schuldnerin – konnte für die frühere Anschrift der Bürgerin nicht ermittelt werden.

Die von den Rechtsbeiständen gesuchte Person ist mit den aufgelieferten Daten nicht gefunden worden. Die aufgelieferten Daten stimmen lediglich hinsichtlich des Vornamens und der (früheren) Anschrift mit der erteilten Auskunft überein.

Die Meldebehörde darf Melderegisterauskünfte nur über bestimmte Einwohner erteilen (§ 28 Abs. 1 MeldeG). Nach der Geschäftsanweisung ist eine gesuchte Person erst dann hinreichend bestimmt, wenn nur eine Person im Melderegister gespeichert ist, auf die diese Merkmale zutreffen. Sofern die vorgegebenen Merkmale bis auf eine geringfügige Abweichung nur auf eine gespeicherte Person zutreffen, kann unter ausdrücklichem Hinweis auf die Abweichung Auskunft erteilt werden. Hier liegen allerdings keine geringfügigen Abweichungen vor; vielmehr unterscheiden sich Geburtsdatum und (frühere) Namen. Das sind so erhebliche Abweichungen, die dazu führen, dass keine Melderegisterauskunft erteilt werden darf. Wir haben den Vorgang beanstandet.

Der Senat schließt sich in dem im Jahresbericht geschilderten Einzelfall der Auffassung des Datenschutzbeauftragten an, dass eine Melderegisterauskunft nicht hätte erteilt werden dürfen, weil die Person mit den vorgegebenen Suchdaten nicht hinreichend bestimmt war.

Die Meldebehörde hat zugesagt, dass aufgrund dieses Vorfalles alle Mitarbeiterinnen und Mitarbeiter nochmals schriftlich und anlässlich von Dienstbesprechungen auch noch mündlich darauf hingewiesen werden, bei der Bearbeitung von Melderegisterauskünften genau auf die Vorgaben zu achten und eine Auskunft nur bei eindeutiger Personenbestimmung zu erteilen.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Warnmeldung wegen Scheinehe

Das Standesamt Steglitz-Zehlendorf hat den anderen elf Berliner Standesämtern sowie dem Standesamt der Stadt Frankfurt/Oder mitgeteilt, dass eine Eheschließung wegen Scheineheverdachtes abgelehnt wurde.

Diese Warnmeldung wird damit begründet, dass der Standesbeamte die Mitwirkung an der Eheschließung verweigern muss, wenn offenkundig ist, dass die Ehe aufhebbar wäre (§ 1314 BGB*)*. Bei einer Ablehnung werden Rundschreiben bzw. Mitteilungen an die Standesämter versandt, bei denen die Verlobten eine erneute Anmeldung versuchen könnten. Mit der Mitteilung des Verdachtes der *Scheinehe* solle darauf hingewiesen werden, dass die Ehe nur geschlossen wird, um für den ausländischen Verlobten auf diese Weise eine dauerhafte Aufenthaltsgenehmigung in der Bundesrepublik Deutschland zu erlangen. Die Versendung dieser Rundschreiben beruht auf einer gemeinsamen Absprache der Berliner Standesämter.

Das Standesamt hält die Übermittlung zur Abwehr erheblicher Nachteile für das Gemeinwohl für erforderlich (§ 14 Abs. 2 Nr. 6 BDSG). Dabei weist es darauf hin, dass in Einzelfällen die Verlobten trotz schriftlich erteilter Ablehnungen bei einem anderen Standesamt erschienen, um dort erneut die Eheschließung anzumelden. Die rechtliche Möglichkeit, über das zuständige Amtsgericht in das Anweisungsverfahren zu gehen, nutzten sie nicht, wodurch sich der Verdacht auf Scheinehe in diesem Einzelfall noch verstärkte.

Das Standesamt sieht allein in der Tatsache, dass dort an die 100 Meldungen eingegangen sind – überwiegend von anderen Standesämtern, aber auch von den Deutschen Botschaften in Ghana und Indien, der Präsidentin des Kammergerichtes und der Berliner Ausländerbehörde –, die Erforderlichkeit für einen Informationsaustausch dieser Behörde untereinander.

Wir haben den Vorgang beanstandet. Mit der Mitteilung werden personenbezogene Daten an die übrigen elf Berliner Standesämter und – offensichtlich wegen der Wohnung des Verlobten – an die Stadt Frankfurt/Oder übermittelt. Sofern Daten aufgrund einer Rechtsvorschrift des Bundes verarbeitet werden, ohne dass die Verarbeitung im Einzelnen geregelt ist, finden die §§ 13 bis 15 BDSG Anwendung (§ 6 Abs. 2 BlnDSG). Das BGB enthält keine ausreichenden Übermittlungsregelungen. Nach § 15 BDSG ist die Übermittlung personenbezogener Daten an öffentliche Stellen zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden.

Zum Zeitpunkt der Übermittlung steht nicht fest, ob

diese Informationen von einem der Empfänger für die ordnungsgemäße Aufgabenerfüllung jemals erforderlich sein werden. Es ist völlig offen, ob die Verlobten überhaupt nochmals bei einem Standesamt vorsprechen, um die Ehe zu schließen. Darüber hinaus ist offen, ob dann immer noch ein Aufhebungsgrund vorliegt. Davon hat sich im Übrigen der Standesbeamte, bei dem die Verlobten vorsprechen, dann durch eigene Feststellungen zu überzeugen. Somit ist im Ergebnis eine Warnmitteilung weder für das Bezirksamt Steglitz-Zehlendorf als übermittelnde Stelle noch für die Empfänger erforderlich. Sie sind darüber hinaus auch nicht geeignet. Durch einen Wohnortwechsel in den Zuständigkeitsbereich eines Standesamtes eines anderen Bundeslandes würden diese Meldungen keine Wirkung entfalten können.

Weiterhin liegen auch nicht die Voraussetzungen des § 14 Abs. 2 Nr. 6 BDSG vor. Die Übermittlung ist danach zulässig, wenn es zur Abwehr nicht nur von Nachteilen, sondern erheblichen Nachteilen für das Gemeinwohl erforderlich ist. Der Begriff darf bei verfassungskonformer Auslegung nicht allzu weit ausgelegt werden. Erhebliche Nachteile für das Gemeinwohl können dann vorliegen, wenn eine konkrete Gefahr für die Allgemeinheit, beispielsweise Katastrophenfälle, verhindert werden solle; denkbar wäre auch die Gefährdung wichtiger staatspolitischer Angelegen-heiten (beispielsweise Staatsbesuche, Staatsakte). Das ist hier nicht der Fall.

Ebenso wenig ist die Übermittlung zur Abwehr einer Gefahr für die öffentliche Sicherheit erforderlich. Nach allgemein verwendeter Definition ist die Gefahr eine Sachlage, die bei ungehindertem Ablauf des zu erwartenden Geschehens in überschaubarer Zukunft mit hinreichender Wahrscheinlichkeit zu einem Schaden für die öffentliche Sicherheit führen wird. Die Gefahr muss also unmittelbar drohen. Auch hier setzt das Gesetz eine erhöhte Schwelle. Sie betrifft hier nicht die Schwere des drohenden Schadens, sondern die Aktualität des drohenden Schadenseintritts. Anhaltspunkte dafür fehlen und sind auch nicht geltend gemacht worden.

Die Stellungnahme durch das Standesamt Steglitz-Zehlendorf steht noch aus.

4.2.2 Straßen- und Verkehrsverwaltung

Sammelanzeige über Verkehrsordnungswidrigkeiten in der Ermittlungsakte

Anlässlich einer Akteneinsicht zu einem Bußgeldverfahren stellte ein Rechtsanwalt fest, dass in der Ermittlungsakte seiner Mandantin eine Sammelanzeige über festgestellte Verkehrsordnungswidrigkeiten (Geschwindigkeitsüberschreitungen) abgelegt war. In dem Formblatt waren die Ergebnisse von Radarmessungen

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

eines ganzen Tages unter Angabe der Kfz-Kennzeichen der betroffenen Fahrzeuge dokumentiert.

In der Sammelanzeige waren nicht nur die Daten der Beschuldigten aufgeführt. Das Formblatt enthielt auch personenbezogene Daten weiterer Kfz-Halter, die nicht mit dem gegen die Beschuldigte geführten *Bußgeldverfahren* in Verbindung standen. Diese Daten waren für die Ermittlungen gegen die Beschuldigte nicht erforderlich; ihre Speicherung in der Ermittlungsakte zur Beschuldigten war unzulässig.

Durch unsere Nachfrage beim Polizeipräsidenten in Berlin wurde die fehlerhafte Bearbeitungsweise in der Akte bemerkt. In einer Dienstbesprechung wurde die Problematik dieses Falles aufgegriffen und alle MitarbeiterInnen wurden auf die Einhaltung der datenschutzrechtlichen Bestimmungen hingewiesen. Es wurde zugesagt, dass ab sofort die nicht erforderlichen Daten bei Kennzeichenanzeigen unkenntlich gemacht werden. Wir gehen davon aus, dass dies – entsprechend unserer Empfehlung – nachträglich auch in dem von uns überprüften Einzelfall geschehen ist.

Die nicht erforderlichen Daten in dem betreffenden Vorgang wurden unkenntlich gemacht.

Die (vergessene) Halterauskunft

Ein früherer Mitarbeiter einer Krankenkasse beschwerte sich darüber, dass das Landes-einwohneramt Berlin seinem ehemaligen Arbeitgeber bzw. dessen Rechtsvertreter Auskünfte aus dem Fahrzeugregister zu seiner Person bzw. zur Person seiner Ehefrau erteilt habe.

Die Kfz-Akten sind beim Landeseinwohneramt Berlin – Referat *Kraftfahrzeugzulassung* – auf Mikrofilmen abgelegt. Bei Bedarf – z. B. für eine Halterauskunft oder eine datenschutzrechtliche Überprüfung – werden die verfilmten Unterlagen und Dokumente ausgedruckt und zu einem (Loseblatt-)Vorgang zusammengeführt. In dem uns zur Prüfung vorgelegten Vorgang waren zwei Auskunftsvorgänge des Landeseinwohneramtes an den ehemaligen Arbeitgeber bzw. an den von diesem beauftragten Rechtsanwalt dokumentiert. Die Antragsteller hatten – unter Beifügung der Kopie einer vollstreckbaren Ausfertigung eines gegen den Petenten gerichteten Urteils des Arbeitsgerichtes Berlin – Auskunft darüber beantragt, ob der Petent bzw. dessen Ehefrau als Halter von Kraftfahrzeugen im Fahrzeugregister eingetragen sind. Die Auskunft wurde den Antragstellern – gestützt auf § 39 Abs. 3 Nr. 1 a StVG – erteilt.

Die Mikrofilm-Recherche ergab, dass die uns zur Prüfung vorgelegten (Papier-)Unterlagen unvollständig waren. Auf den Mikrofilmen war – neben den zwei bekannten Auskunftsvorgängen – ein weiterer Auskunftsvorgang dokumentiert, bei dem dem Rechtsbeistand des ehemaligen Arbeitgebers des Petenten – auf dessen erneute Anfrage – weitere Fahrzeugdaten mitgeteilt worden waren. Zur Erklärung dieses Umstandes

Im Rahmen der Wiederherstellung von auf Mikrofilm archivierten Halterauskünften zum Zweck der Akteneinsicht durch den Fahrzeughalter wurde eine Auskunft im Inhaltsverzeichnis der „Recherche Mikrofilm“ im örtlichen Fahrzeugregister übersehen. Es handelt sich um einen individuellen Fehler, nicht um einen Systemmangel. Bei der erfolgten Akteneinsicht ist dann festgestellt worden, dass die Halterauskunft gegenüber

verwies das Landeseinwohneramt darauf, dass es sich bei diesen Vorgängen um ein absolutes Massengeschäft handeln würde. Es sei zu vermuten, dass die weitere (vergessene) Auskunftserteilung bei der Auswertung des Mikrofilmes und der Zusammenstellung der Papierakte übersehen (Stichwort „menschliches Versagen") und nicht ausgedruckt worden sei. Die nachfolgenden Stellungnahmen – z. B. an den Berliner Beauftragten für Datenschutz und Informationsfreiheit – seien in Unkenntnis des auf Mikrofilm abgelegten Dokumentes gefertigt worden.

Nach § 39 Abs. 3 Nr. 1 a StVG dürfen Halter- und Fahrzeugdaten übermittelt werden, wenn der Empfänger glaubhaft macht, dass er die Daten zur Geltendmachung, Sicherung oder Vollstreckung von nicht mit der Teilnahme am Straßenverkehr im Zusammenhang stehenden öffentlich-rechtlichen Ansprüchen in Höhe von mindestens fünfhundert Euro benötigt. Das gegen den Petenten gerichtete Urteil des Arbeitsgerichtes Berlin hat keinen derartigen öffentlich-rechtlichen Anspruch des ehemaligen Arbeitgebers gegen den Petenten bzw. dessen Ehefrau begründet. Die Datenübermittlungen des Landeseinwohneramtes an den ehemaligen Arbeitgeber bzw. dessen Rechtsbeistand waren somit unzulässig.

Unabhängig davon sind technisch-organisatorische Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität). Die fehlerhafte Auswertung der Mikrofilme und unvollständige Zusammenstellung der (Papier-)Unterlagen entsprachen diesen Vorgaben nicht. Zur Vermeidung vergleichbarer Fälle in der Zukunft haben wir empfohlen, den Vorgang mit den zuständigen MitarbeiterInnen zu analysieren und diese auf die Einhaltung des Datenschutzes, insbesondere die Bedeutung der Datenintegrität, hinzuweisen.

Das (nicht) verjährte Verkehrsordnungswidrigkeitenverfahren

Ein Petent gab an, dass ihm eine Verkehrsordnungswidrigkeit zur Last gelegt werde. Obwohl die Tat bereits mehr als drei Monate zurückliegen würde, werde vom Polizeipräsidenten in Berlin gegen seine Person ermittelt. Insbesondere sei ihm angedroht worden, dass ein Abgleich mit den über seine Person im Personalausweisregister gespeicherten Daten vorgenommen würde, wenn er zu dem geladenen Termin nicht bei der Polizei erscheine.

Da es sich um ein Ordnungswidrigkeitenverfahren der Kreisstadt Herrenberg handelte, wurden die Ermittlungen zunächst von der dortigen Bußgeldstelle geführt. Das Kennzeichen des Tatfahrzeuges war auf eine Autovermietung zugelassen. Diese benannte den Petenten als den Fahrzeugführer zur Tatzeit. Da der Petent auf den ihm von der Bußgeldstelle in Herrenberg übersand-

der anfragenden Innungskrankenkasse irrtümlich erfolgte. Der gerügte Fehler wurde mit den Betroffenen ausgewertet und war auch Bestandteil einer Dienstbesprechung der Zulassungsbehörde auf Führungsebene.

ten Anhörungsbogen nicht geantwortet hatte, wurde der gesamte Vorgang für weitere Ermittlungen an den für seinen Wohnort zuständigen Abschnitt des Polizeipräsidenten in Berlin abgegeben. Erst nachdem dem Petenten von dort – unter Hinweis auf die Möglichkeit eines Daten-abgleiches mit dem Personalausweisregister – erneut Gelegenheit zur Äußerung eingeräumt worden war und dieser schriftlich mitgeteilt hatte, dass er zum geladenen Termin unter keinen Umständen erscheinen würde, wurden die Lichtbilder aus dem Personalausweisregister angefordert und mit den Tatfotos verglichen.

Die Erforderlichkeit von Datenerhebungen zur Feststellung des verantwortlichen Fahrers ist dann nicht gegeben, wenn eine *Verfolgungsverjährung* eingetreten ist. Die Verjährungsfrist beträgt nach § 26 Abs. 3 StVG drei Monate, solange weder ein Bußgeldbescheid ergangen noch öffentliche Klage erhoben worden ist. Im Fall des Petenten war die dreimonatige Frist des § 26 Abs. 3 StVG bereits abgelaufen, als er vom Polizeipräsidenten in Berlin mit der Bitte, sich zu dem Vorwurf zu äußern, angeschrieben wurde. Nach § 33 Abs. 1 Nr. 1 OWiG tritt jedoch eine Verjährungsunterbrechung ein, wenn dem Betroffenen bekannt gegeben worden ist, dass gegen ihn ein Ermittlungsverfahren geführt wird. Eine derartige Bekanntgabe liegt vor, wenn dem Betroffenen ein Anhörungsbogen mit konkreten Angaben zur Person und zum Tatvorwurf übersandt wird. Dem Petenten war bereits von der Bußgeldstelle der Kreisstadt Herrenberg ein derartiger Anhörungsbogen übersandt worden. Ihm war daher zu einem früheren Zeitpunkt – innerhalb der Verjährungsfrist – bereits bekannt, dass gegen seine Person ein Ermittlungsverfahren geführt wird. Da insofern keine Verfolgungsverjährung eingetreten war, war das Schreiben des Polizeipräsidenten in Berlin an den Petenten zur Feststellung des verantwortlichen Fahrers der Verkehrsordnungswidrigkeit erforderlich und nach § 18 Abs. 1 Satz 1 ASOG zulässig.

Auch der Abgleich des Tatfotos mit Lichtbildern des Petenten aus dem Pass- bzw. Personalausweisregister war datenschutzrechtlich nicht zu beanstanden. Personalausweis- bzw. Passbehörden dürfen Daten (z. B. Lichtbilder) aus dem Personalausweis- bzw. Passregister an andere Behörden übermitteln, wenn die Daten anders nicht oder nur mit unverhältnismäßigem Aufwand erhoben werden können (§ 2 b Nr. 3 Personalausweisgesetz bzw. § 22 Passgesetz). Daraus folgt, dass dem Betroffenen – vor einem Abgleich des Tatfotos mit den Lichtbildern aus dem Personalausweis- bzw. Passregister – zunächst die Möglichkeit einer Anhörung einzuräumen ist. Reagiert der Betroffene auf die Möglichkeit einer Anhörung nicht oder kommt er einer Vorladung unter gleichzeitigem Hinweis auf die Einsichtnahme in die Lichtbilder der Register – wie im vorliegenden Fall – nicht nach, darf ein Abgleich der Lichtbilder durch die Polizei vorgenommen werden.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

4.3 Justiz und Finanzen

4.3.1 Justiz

Beschwerde über Gerichtsvollzieher

Ein Bürger trat an uns mit der Beschwerde heran, ihm sei – entgegen einer vorherigen Absprache – eine Zahlungsaufforderung in einer Zwangsvollstreckungssache unkuvertiert in seinem Briefkasten durch den zuständigen Gerichtsvollzieher hinterlassen worden, so dass eine Hausbewohnerin, die einen Schlüssel zum Briefkasten hatte, nunmehr Kenntnis von der Zwangsvollstreckung erhalten habe.

Bei dem *Gerichtsvollzieher* handelt es sich um eine öffentliche Stelle, die bei Ausführung ihrer Aufträge an die Vorschriften des BlnDSG neben den speziellen Vorschriften für die Tätigkeit der Gerichtsvollzieher gebunden ist. Er hat Maßnahmen zu treffen, um den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung von Daten zu verhindern (§ 5 Abs. 4, Abs. 2 Nr. 1 BlnDSG). Aus den Vorschriften über die Tätigkeit des Gerichtsvollziehers ergibt sich, dass der Gerichtsvollzieher bei der Zwangsvollstreckung jede unnötige Schädigung oder Ehrenkränkung des Schuldners und die Erregung überflüssigen Aufsehens zu vermeiden hat (§ 104 Geschäftsanweisung für Gerichtsvollzieher). Darüber hinaus ist auch die Verwendung von Postkarten für den Gerichtsvollzieher nicht zulässig, soweit nichts anderes bestimmt ist oder Unzuträglichkeiten nicht zu besorgen sind (§ 53 der Gerichtsvollzieherordnung).

Auch die Tatsache, dass der Petent während der Dauer seiner Abwesenheit einer anderen Hausbewohnerin den Briefkastenschlüssel überlassen hatte, war weder ungewöhnlich noch konnte sie als Rechtfertigung für die Verwendung der unkuvertierten Nachricht herangezogen werden, da es sich bei der Angabe der konkreten Höhe der Verbindlichkeit im Zusammenhang mit der Zwangsvollstreckungssache und dem Namen der Vollstreckungsgläubiger um Daten handelt, deren Preisgabe zu einer Beschädigung des Ansehens des Schuldners führen konnte und deren Verwendung auf Postkarten daher sehr wohl unnötige Belastungen und Unzuträglichkeiten besorgen ließ.

Eine eingehende Stellungnahme zu dem geschilderten Fall ist nicht möglich, weil die näheren Umstände (z.B. eine vorherige Absprache) nicht bekannt sind. Dennoch sind die Berliner Gerichtsvollzieher auf die Beanstandung des Berliner Beauftragten für Datenschutz und Informationsfreiheit und auf die Einhaltung datenschutzrechtlicher Bestimmungen hingewiesen worden.

Dem Senat ist nicht bekannt, dass die nach § 53 Nr. 3 GVO grundsätzlich zulässige Verwendung von Postkarten durch die Gerichtsvollzieher bisher zu Unzuträglichkeiten geführt hat.

Einsichtnahme in die Prüfungsakte eines Mitprüflings

Ein Student der Rechtswissenschaft hatte bei dem Justizprüfungsamt den schriftlichen Teil seines Ersten Staatsexamens absolviert. Da es zu Unregelmäßigkeiten bei der Zuordnung einzelner Blätter zu den jeweiligen Examensarbeiten gekommen war und dem Petenten dadurch erhebliche Nachteile bei der Begutachtung seiner Examensarbeiten drohten, stellte er den Antrag

Die vom Berliner Beauftragten für Datenschutz und Informationsfreiheit vertretene Auffassung, das Justizprüfungsamt habe den Petenten bezüglich der Prüfungsakten seines Sitznachbarn weder als Betroffenen noch als Dritten im Sinne des § 17 Abs. 2 JAG angesehen, trifft nicht zu. Der Petent ist als Dritter angesehen worden. Es ging vielmehr um die Frage, ob der

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

auf Einsichtnahme in die Prüfungsakten seines Sitznachbarn. Dieses wurde ihm vom Justizprüfungsamt mit dem Hinweis auf § 17 Abs. 2 Gesetz über die juristische Ausbildung für das Land Berlin (JAG) und der Begründung verwehrt, die Prüfungsakten des Sitznachbarn beträfen nicht das Prüfungsverfahren des Petenten. Zugleich sei dieser aber auch nicht Dritter.

Nach § 17 Abs. 2 JAG wird dem Betroffenen Auskunft aus den *Prüfungsakten* auch nach Abschluss des Prüfungsverfahrens erteilt. In diesem Umfang wird auch Akteneinsicht gewährt. Dritten stehen diese Rechte gleichermaßen zu, jedoch nur mit schriftlichem Einverständnis des Betroffenen.

Die Rechtsauffassung des Justizprüfungsamtes, wonach der Petent bezüglich der Prüfungsakten seines Sitznachbarn weder Betroffener noch Dritter i. S. d. § 17 Abs. 2 JAG sei, konnten wir weder der Vorschrift entnehmen noch nachvollziehen. Soweit der Betroffene Einblick in seine Prüfungsunterlagen nimmt, ist er selbstverständlich nicht Dritter; wünscht er jedoch Einsichtnahme in Prüfungsakten seiner „Mitstreiter", so ist er Dritter, da sein Einsichtsbegehren ein fremdes Prüfungsverfahren betrifft. Schließlich macht es keinen Sinn, jedem x-beliebigen Bürger und gänzlich Unbeteiligten nach Einverständnis des Betroffenen ein Einsichtsrecht zu gewähren, Mitprüflingen dagegen nicht. Da der Gesetzgeber lediglich zwischen Betroffenem und Drittem unterscheidet, ist für die Konstruktion weiterer Interessenten insoweit kein Raum.

Daher war das Einverständnis des Betroffenen einzuholen.

Petent ein berechtigtes Interesse an dem Einholen des Einverständnisses seines Mitprüflings hatte. Dies ist verneint worden, weshalb auch das Einverständnis des Sitznachbarn nicht eingeholt wurde. Das Verwaltungsgericht hat die Rechtsauffassung des Justizprüfungsamtes bestätigt.

Beifügung von Stammblättern zur Gerichtsakte

Ein Bürger beschwerte sich darüber, dass die Geschäftsstellen beim Verwaltungsgericht Berlin automatisch bei Eingang eines Verfahrens der neu anzulegenden Akte eine Datenliste über vergangene abgeschlossene und noch laufende Verfahren mit inhaltlicher Kurzfassung zur Information der Richter beifügen. Dies verletze das Gebot der richterlichen Unvoreingenommenheit.

Bei der Prüfung haben wir festgestellt, dass der Richter bei Neuzugang bzw. Erstvorlage der Akte nicht automatisch einen Ausdruck über die anhängigen bzw. abgeschlossenen Verfahren des Klägers/Antragstellers erhält, sondern nur nach besonderer Aufforderung an die Geschäftsstelle. Die Entscheidung darüber ist hauptsächlich vom jeweils zugeordneten Sachgebiet abhängig und wird bei Spruchkörpern vom Vorsitzenden getroffen.

Das Stammblatt ermöglicht dem Richter, Doppelrechtshängigkeiten, Zuständigkeiten und Überschneidungen (§§ 81 ff. VwGO) zu prüfen. Die Stammblätter

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

werden nach Prüfung durch den Richter aus der Akte entfernt und in Sonderheften geführt. Verfahrensbeteiligte haben daher keine Möglichkeit, Einsicht in diese zu nehmen. Die im Stammblatt aufgeführten Verfahren können nicht vom Richter selbst mit Hilfe seines PCs aufgerufen werden; es bedarf vielmehr einer Anforderung an die jeweilige Geschäftsstelle. Die im Stammblatt enthaltenen Daten über Verfahren des Klägers/Antragstellers können für eine Prüfung prozessualer Fragen erforderlich sein. Zudem gebietet der Amtsermittlungsgrundsatz nicht nur eine intensive Auseinandersetzung mit dem gesamten Prozessmaterial, sondern darüber hinaus eine selbstständige Beschaffung prozessrelevanter Informationen durch den Richter. Dazu zählen auch Ergebnisse und Erwägungen aus bereits abgeschlossenen Verfahren, soweit sie der Richter als entscheidungserheblich bewertet. Insoweit sind die Anforderung und die Auswertung des Stammblattes durch die richterliche Unabhängigkeit gedeckt.

Gefangenenpersonalakte

Die Aufbewahrungsbestimmungen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden werden derzeit von den Justizministerien der Bundes und der Länder überarbeitet.

Hierfür sind die verschiedenen Themenkomplexe den einzelnen Bundesländern zur federführenden Bearbeitung zugewiesen worden. Berlin ist danach für den Themenkreis „Justizvollzugsbehörden" zuständig.
Seit Beginn des Jahres 2002 befinden wir uns mit der Senatsverwaltung für Justiz in Erörterungen über den Umgang mit *Gefangenenpersonalakten*. Nach dem Vorschlag der Senatsverwaltung für Justiz soll deren Aufbewahrungsfrist einheitlich zehn Jahre betragen. Unter diese Frist fallen sowohl nach bisher geltender als auch nach künftiger Rechtslage ebenfalls sensitive Daten der Strafgefangenen. Die von uns geforderte Anlegung von Sonderheften hat der Strafvollzugsausschuss unter Hinweis auf das Zusammenarbeitsgebot nach dem Strafvollzugsgesetz sowie aus Sicherheitsgründen abgelehnt.

Zu diesen Daten gehören

- Listen von Telefonverbindungsdaten,
- Aktenvermerke über Brief-, Telefon- und Besuchsüberwachungsmaßnahmen,
- sonstige Daten, die Dritte betreffen,
- erkennungsdienstliche Unterlagen (mit Lichtbildern und Beschreibungen von körperlichen Merkmalen),
- psychiatrische Gutachten und

Die Aussage, dass jedem Vollzugsbediensteten sämtliche Daten einschließlich der sensiblen Daten des Strafgefangenen jederzeit und uneingeschränkt zugänglich sind, ist nicht zutreffend.

Die Gefangenenpersonalakten werden in den Berliner Justizvollzugsanstalten entweder zentral in den Vollzugsgeschäftsstellen oder in den jeweiligen Teilanstalten oder Unterbringungsbereichen aufbewahrt.

Neben den Mitarbeitern, die dort ihren Dienst verrichten, haben grundsätzlich nur die Bediensten Zugriff auf die Akten, die diese für die Wahrnehmung ihrer obliegenden Aufgaben benötigen. Darüber hinaus besteht bei den nicht zu vermeidenden Übersendungen von Gefangenenpersonalakten in andere Bereiche der Anstalt (z. B. Anstaltsleitung etc.) für einige weitere Bedienstete die Möglichkeit eines Zugriffs auf die Akten.

Die in dem Jahresbericht aufgestellte Forderung, besonders sensible Unterlagen aus den Gefangenenpersonalakten in Sonderheften aufzubewahren und für diese Daten eine Aufbewahrungsfrist von einem Jahr festzulegen, ist weder praktikabel noch aus datenschutzrechtlichen Gründen geboten. Eine Aussonderung von bestimmten Daten widerspricht dem Grundsatz der Aktenvollständigkeit und vermindert die Übersichtlichkeit der Gefangenenpersonalakten. Eine entsprechende Regelung wurde demzufolge aus Sicherheitsgründen auf der 91. Sitzung des Strafvollzugsausschusses der Länder im Mai 2000 einstimmig abgelehnt.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

- Vermerke über interne Disziplinarmaßnahmen.

Bei psychiatrischen Gutachten und Therapieakten folgt dies bereits daraus, dass die darin enthaltenen Daten von der ärztlichen Schweigepflicht umfasst sind (§ 203 Abs. 1 Nrn. 1, 2 und 5 StGB). § 180 Abs. 8 Strafvollzugsgesetz (StVollzG) trägt der besonderen Schutzbedürftigkeit von Daten Dritter Rechnung und sieht eine restriktive Handhabung vor. Allein der Umstand, dass jedem Vollzugsbediensteten sämtliche Daten einschließlich der sensitiven Daten des Strafgefangenen jederzeit und uneingeschränkt zugänglich sind, verletzt ebenso wie deren zehnjährige Aufbewahrungsdauer das Persönlichkeitsrecht des Strafgefangenen.

Nach § 154 Abs. 1 StVollzG sollen alle im Vollzug Tätigen zusammenarbeiten und daran mitwirken, die Aufgaben des Vollzuges zu erfüllen. § 154 Abs. 2 StVollzG berücksichtigt, dass auch eine Zusammenarbeit mit Personen notwendig ist, die zwar nicht im Strafvollzug tätig sind, jedoch mit Gefangenen auch nach deren Entlassung zu tun haben.

Es ist kein Grund ersichtlich, weshalb diese Grundsätze durch die Führung eines Sonderhefts mit sensitiven Daten beeinträchtigt werden. Selbstverständlich können Vollzugsbedienstete, für die die Kenntnis dieser Daten erforderlich ist, die Sonderhefte einsehen (§ 183 Abs. 1 StVollzG).

Der Umfang des Einsichtrechtes wird durch Sonderhefte nicht eingeschränkt; vielmehr könnte ein solches Sonderheft gerade dazu beitragen, dass die Erforderlichkeit der Kenntnisnahme durch die Vollzugsbeamten von Fall zu Fall geprüft werden kann. Auch in der Zusammenarbeit mit anderen Stellen könnte die Anlage eines Sonderheftes Klarheit über die Sensitivität der Daten schaffen.

Sicherheitsaspekte stehen der Führung von Sonderheften ebenfalls nicht entgegeben. Zunächst kann nicht davon ausgegangen werden, dass alle sensitiver Daten besonders sicherheitsrelevant sind. Sollte die Kenntnis dieser Daten aus Gründen der Sicherheit erforderlich sein, so ist der Zugriff auf diese Sonderakten selbstverständlich aufgrund § 183 Abs. 1 StVollzG gewährleistet. Durch differenzierte Regelungen könnte sowohl den Belangen der Sicherheit als auch denen des Datenschutzes Rechnung getragen werden. So wäre es denkbar, dass bei dem konkreten Verdacht einer Gefahr für die Sicherheit das Sonderheft zu der Gefangenenpersonalakte geheftet wird.

Der Inhalt dieser Sonderhefte sollte gelöscht werden, wenn die Aufbewahrung dieser speziellen Daten nicht länger erforderlich ist. Eine Löschungsfrist von einem Jahr nach Ende der Strafhaft erscheint hier angemessen.

Der Hinweis, dass hinsichtlich der eingehenden Post für Untersuchungsgefangene eine einjährige Aufbewahrungsfrist besteht, trifft nicht zu. Gemäß Nr. 826 der Aufbewahrungsbestimmung sind lediglich die Begleitumschläge der eingehenden Briefe der Untersuchungsgefangenen nach einem Jahr zu vernichten.

Über die Aufbewahrungsdauer der eingehenden Post enthält die zitierte Vorschrift keine Aussage. Grund für eine frühzeitigere Aussonderung und Vernichtung der Begleitumschläge ist, dass diesen Umschlägen nur hinsichtlich des Eingangs und der Aushändigung der eingehende Post an den Untersuchungsgefangenen ein Beweiswert zukommt. Für eine eventuelle spätere Inhaftierung des Gefangenen haben diese Unterlagen keinen weiteren Nutzen. Ähnliches gilt hinsichtlich der ebenfalls in Nr. 826 der Aufbewahrungsbestimmungen aufgeführten Sprechscheine.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Bezüglich eingehender Briefe an Untersuchungsgefangene und in Bezug auf Sprechscheine sieht Nr. 826 der Aufbewahrungsbestimmungen die Möglichkeit der gesonderten Aufbewahrung sowie die kurze Aufbewahrungsfrist von einem Jahr vor. Hieraus kann abgeleitet werden, dass Daten, die aus der Überwachung des Briefverkehrs gewonnen werden, besonders sensitiv sind und deshalb ein besonderer Umgang mit ihnen zu gewährleisten ist. Insofern lässt sich der Schluss ziehen, dass diese Überlegung auch für die Überwachung des Briefverkehrs von Strafgefangenen gilt ebenso wie für die Überwachung von Telefonverbindungen und Besuchen, die ihrer Natur nach vergleichbar sind. Zu verweisen ist hier auf § 180 Abs. 8 StVollzG, der explizit eine Verwendungsbeschränkung für Daten regelt, die aus der Überwachung von Besuchen, Schriftwechsel oder Paketen bekannt geworden sind. Dies sollte sich auch auf die Aufbewahrung und Löschung auswirken.

4.3.2 Finanzen

Steuervergünstigungsabbaugesetz (StVerGAbG)

Am Ende des Jahres 2002 brachte die Bundesregierung den Entwurf für ein *Steuervergünstigungsabbaugesetz*[71] im Bundestag ein. Damit sollen nicht nur Steuervergünstigungen abgebaut werden, es sollen auch die Kontrollmöglichkeiten im Steuerbereich erheblich ausgeweitet werden.

Die vom Datenschutzbeauftragten kritisierten geplanten Änderungen hinsichtlich der Abschaffung des sogenannten Bankgeheimnisses (Streichung des § 30a AO) und der damit zusammenhängenden Änderungen (§ 194 (3) AO, § 23a EStG) sowie der Einfügung des § 139a AO durch das Steuervergünstigungsabbaugesetz (StVerGAbG) sind auf Empfehlung des Vermittlungsausschusses in seiner Sitzung am 09.04.2003 gestrichen worden. Diese geplanten Veränderungen sind in dem beschlossenen Steuervergünstigungsabbaugesetz nicht mehr enthalten.

Eine zentrale Vorschrift zum Steuergeheimnis, § 30a Abgabenordnung (AO), die das Vertrauensverhältnis des Bankkunden zu seiner Bank besonders schützt, soll ersatzlos gestrichen werden mit der Folge, dass die Finanzbehörden in Zukunft auch von den Banken umfassend Auskünfte erhalten können. Der Wegfall des § 30a AO ist die Voraussetzung dafür, dass mit dem Steuervergünstigungsabbaugesetz gleichzeitig neue Kontrollmitteilungen eingeführt werden können. So soll § 194 Abs. 3 AO dahin erweitert werden, dass in Zukunft Kontrollmitteilungen für alle Personen möglich sind, deren steuerliche Verhältnisse bei Außenprüfungen der Finanzbehörden auffallen. Neu ist auch eine Regelung im Einkommensteuergesetz (§ 23 a EStG), mit der eine Mitteilungspflicht für alle Kreditinstitute und andere Finanzdienstleister über alle Veräußerungs- und Termingeschäfte vorgesehen ist. Auch diese Mitteilungspflicht wäre ohne eine Abschaffung des § 30 a AO nicht möglich. Die Begründung für die Abschaffung des so genannten Bankgeheimnisses ist denkbar

[71] BT-Drs. 866/02

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

knapp, sie dient der Einführung der beiden genannten neuen Regelungen, „die bei einem Fortbestand des § 30a AO wirkungslos blieben".

Aus datenschutzrechtlicher Sicht vermissen wir hier eine Abwägung der Interessen des Bürgers, der Banken und des Staates. Inwieweit diese Maßnahme verhältnismäßig ist, bleibt offen. Auch mit der Frage des Rückwirkungsverbotes bei einem Wegfall des § 30 a AO hat sich die Bundesregierung in dem Gesetzesentwurf nicht befasst.

Eine weitere auch datenschutzrechtlich bedeutsame Änderung stellt die Einfügung des § 139 a AO dar. Danach sollen die bisher vergebenen Steuernummern durch ein neues bundeseinheitliches Identifikationsmerkmal ersetzt werden. Jeder Bundesbürger soll eine ihn lebenslang begleitende Steuernummer erhalten. Alles Nähere soll erst in einer Rechtsverordnung geregelt werden. Der Gesetzesbegründung lässt sich nicht entnehmen, warum das bundeseinheitliche Identifikationsmerkmal tatsächlich erforderlich ist. Datenschutzrechtlich bedenklich ist es, den Zweck dieses Merkmals und die Verwendung erst in einer Rechtsverordnung näher zu regeln. Dies entspricht nicht dem Grundsatz der Normenklarheit, auf den das Bundesverfassungsgericht im Volkszählungsurteil hingewiesen hat.

Fortsetzungsgeschichte Abgabenordnung

Zum Thema Novellierung der *Abgabenordnung*[72] durch die Aufnahme datenschutzrechtlicher Vorschriften gibt es in diesem Jahr nicht viel Neues zu berichten. Die Datenschutzbeauftragten des Bundes und der Länder haben dem Bundesfinanzministerium Vorschläge für eine Änderung der Abgabenordnung vorgelegt. Diese Vorschläge wurden im Herbst des Jahres 2002 erst einmal in einer Gemeinsamen Arbeitsgruppe mit Mitgliedern des Bundesfinanzministeriums, der Länderfinanzverwaltungen und der Datenschutzbeauftragten erörtert. Ziel ist es, einen Konsens herzustellen für eine Gesetzgebungsvorlage, die endlich die Aufnahme datenschutzrechtlicher Vorschriften in die Abgabenordnung regelt.

Die erste Sitzung der Koordinierungsrunde mit Vertretern der Datenschutzbeauftragten des Bundes und der Länder sowie der obersten Finanzbehörden der Länder unter Leitung des Bundesministeriums für Finanzen fand vom 30. September bis 1. Oktober 2002 in Bonn statt. Berlin war bei dieser Besprechung, die sich inhaltlich im Wesentlichen an den Vorschlägen des Bundesbeauftragten für den Datenschutz zur Änderung der Abgabenordnung unter datenschutzrechtlichen Gesichtspunkten orientierte, durch die Senatsverwaltung für Finanzen vertreten.

Es bestand Einvernehmen, dass ein Ziel der Koordinierungsrunde die Ausgestaltung der AO als bereichsspezifisch abschließende Datenschutzvorschrift sei, deren abschließender Regelungscharakter auch aus Sicht der Datenschutzbeauftragten dann keinen Raum mehr für eine subsidiäre Anwendung des BDSG lasse.
Berlin wird durch die Senatsverwaltung für Finanzen im Rahmen der nächsten Sitzungen daran weiterhin aktiv mitwirken.

Nachdem das Abgeordnetenhaus am 1. Juli 1999 aufgrund der Beschlussempfehlung des Ausschusses für

[72] JB 2001, 4.3.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Inneres, Sicherheit und Ordnung beschlossen hatte, dass der Senat aufgefordert wird, sich auf Bundesebene für die Aufnahme datenschutzrechtlicher Bestimmungen in die Abgabenordnung einzusetzen[73], hat sich die Senatsverwaltung für Finanzen als Vertreter der Länderfinanzverwaltungen an der ersten Arbeitssitzung der Koordinierungsrunde beteiligt. Wir hoffen, dass sie sich dort nachdrücklich für die Aufnahme datenschutzrechtlicher Vorschriften in die AO einsetzen wird.

Die neue Zeile „Eingetragene Lebenspartnerschaft" auf der Einkommensteuererklärung

Ein Bürger machte uns darauf aufmerksam, dass der Vordruck für die Einkommensteuererkärung 2001 eine neue Zeile enthielt. Auf dem Mantelbogen der Steuererklärung sollte angegeben werden, seit wann eine eingetragene Lebenspartnerschaft besteht. Nähere Angaben sollten auf einem gesonderten Blatt erfolgen.

Der Sachverhalt ist zutreffend und abschließend dargestellt.

Auch bei der Erhebung von Daten durch die Finanzbehörden gilt der Grundsatz, dass nur die Daten erhoben werden dürfen, die sich auf die Besteuerung der Einkünfte des Bürgers auswirken. Auf unsere Nachfrage bei der Senatsverwaltung für Finanzen teilte diese mit, dass das Eingabefeld „*Eingetragene Lebenspartnerschaft* seit dem" in den amtlichen Steuervordruck für das Jahr 2001 vorsorglich aufgenommen worden war, um steuerliche Änderungen berücksichtigen zu können, die durch ein angekündigtes Gesetz zur Ergänzung des Lebenspartnerschaftsgesetzes im Veranlagungsverfahren erwartet worden waren. Dieses Gesetz war jedoch nicht verabschiedet worden, so dass sich eine eingetragene Lebenspartnerschaft auf die Besteuerung der Lebenspartner bisher steuerlich nicht ausgewirkt hat. Die Erhebung der Daten war daher nicht erforderlich und unzulässig. Da der Steuervordruck für das Jahr 2001 bereits vollständig gedruckt war, war eine Änderung des Vordruckes für dieses Jahr nicht mehr möglich. Die Senatsverwaltung für Finanzen hat das Problem jedoch der Vordruckkommission „Einkommensteuer" vorgetragen, und diese hat die entsprechende Zeile im Entwurf für den Vordruck für das Jahr 2002 entfernt. Soweit Betroffene in dem Erklärungsvordruck für das Jahr 2001 nicht erforderliche Angaben zu einer eingetragenen Lebenspartnerschaft gemacht haben sollten, werden die Finanzämter diese Angaben nicht speichern.

Der verirrte Kraftfahrzeugsteuerzahlungshinweis

Ein Bürger beschwerte sich darüber, dass er vom Landeseinwohneramt – Referat Kraftfahrzeugzulassung – ein Schreiben mit der Aufforderung erhalten hatte, seine Kraftfahrzeugsteuer zu entrichten; ansonsten werde das Fahrzeug stillgelegt. Bei einer Nachfrage

Auf Beschwerde des Bürgers und die darauf erfolgte Nachfrage des Berliner Beauftragten für Datenschutz und Informationsfreiheit hin wurde dem Fall durch die zuständige Verwaltung nachgegangen und der Sachverhalt entsprechend der nebenstehenden Darstellung

[73] vgl. JB 1999, Anlage 2, S. 182

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

des Bürgers stellte sich heraus, dass der Zahlungshinweis für die Kfz-Steuer an eine ehemalige Urlaubsadresse gesandt worden war. Eine Nebenwohnung hatte der Bürger an diesem Ort nie angemeldet.

aufgeklärt.

1999 hatte der Petent seinen Urlaub in dem betreffenden Urlaubsort verbracht. Als das Finanzamt dem Bürger während des Urlaubes den Zahlungshinweis an seine Berliner Adresse sandte, versah die Deutsche Post AG den Brief mit dem Hinweis „Zur Zeit in ...” und schickte ihn an das Finanzamt zurück. Das Finanzamt interpretierte dies als dauerhafte neue Adresse und speicherte sie als *Zustelladresse*. In der Folgezeit sandte es die Zahlungshinweise immer an die Urlaubsadresse. Im Jahr 2000 war der Zahlungshinweis trotz Adressierung an die Urlaubsadresse nicht an das Finanzamt zurückgeschickt worden. Erst im Jahr 2001 wurde der Steuerbescheid von der Post mit dem Hinweis „Empfänger unter der angegebenen Anschrift nicht zu ermitteln” an das Finanzamt zurückgesandt. Nach einer Anfrage bei dem Einwohnermeldeamt des Urlaubsortes behandelte das Finanzamt den Verbleib des Steuerpflichtigen als „Unbekannt verzogen”.

Das Finanzamt hatte hier unzulässigerweise aufgrund des Hinweises der Deutschen Post AG „Zur Zeit in ...” die Urlaubsadresse des Bürgers als neue Zustelladresse gespeichert. Der Zufall wollte es, dass diese unzulässige Speicherung erst nach dem Zustellversuch im Jahr 2001 auffiel. Nachdem der Fall aufgeklärt war, hat das zuständige Finanzamt die gespeicherte falsche Adresse unverzüglich gelöscht. Der Fall diente als Anlass, die Mitarbeiterinnen und Mitarbeiter des Finanzamtes noch einmal auf die größtmögliche Sorgfalt – gerade auch bei der Speicherung neuer bzw. anderer Adressen – hinzuweisen.

Die Steuernummer auf der Rechnung – ein Freibrief beim Finanzamt?

Zahlreiche Bürger beschwerten sich über eine neue Regelung zur Bekämpfung des Umsatzsteuerbetruges: Der Gesetzgeber hat im Steuerverkürzungsbekämpfungsgesetz § 14 Abs. 1 a Umsatzsteuergesetz (UStG) so gefasst, dass der leistende Unternehmer in der Rechnung die ihm vom Finanzamt erteilte Steuernummer anzugeben hat. Die Betroffenen befürchten, dass mit Hilfe der Steuernummer Auskünfte beim Finanzamt zu ihrer Person eingeholt werden können.

Die Berliner Finanzämter sind nochmals ausdrücklich instruiert worden, telefonische Auskünfte über vom Steuergeheimnis geschützte Verhältnisse nur nach der nebenstehend dargestellten Verfahrensweise zu erteilen.

Zu der generellen Problematik der gesetzlich geforderten Angabe der Steuernummer auf Rechnungen ist darauf hinzuweisen, dass ab dem 1.1.2004 die Vorgaben der EU-Richtlinie 2001/115/EG vom 20.12.2001 über die mehrwertsteuerlichen Anforderungen an die Rechnungsstellung in das nationale Umsatzsteuerrecht übernommen werden müssen. Hiernach ist in den Rechnungen grundsätzlich die Umsatzsteuer-Identifikationsnummer (USt-IdNr.) des leistenden Unternehmers anzugeben. Durch eine Optionsregelung ist es den Mitgliedstaaten jedoch möglich, von den Steuerpflichtigen die Angabe der Steuernummer neben

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

der USt-IdNr. bzw. anstatt der USt-IdNr. (außer bei innergemeinschaftlichen Umsätzen) obligatorisch zu verlangen.

Seit dem 1. Juli 2002 ist wegen dieser Rechtsgrundlage die *Steuernummer* anzugeben. Dabei handelt es sich um die von dem zuständigen Finanzamt zugeteilte Steuernummer. Die Steuernummer dient dem Finanzamt als Ordnungsmerkmal. Der Aufbau der Steuernummer ist nicht gesetzlich geregelt, sondern wurde von den Finanzbehörden bundeseinheitlich festgelegt. Aus datenschutzrechtlicher Sicht wäre der Zwang zur Offenbarung der Steuernummer dann problematisch, wenn die Finanzämter allein auf der Grundlage der Nennung der Steuernummer Auskünfte zu den Steuerpflichtigen erteilen würden.

Hierzu hat uns die Senatsverwaltung für Finanzen mitgeteilt, dass die Mitarbeiter der Finanzämter weder in der Vergangenheit berechtigt gewesen waren noch in der Zukunft berechtigt sind, bei Nennung der Steuernummer am Telefon Auskunft zu dem Steuerfall zu erteilen. Nur dann, wenn einem Mitarbeiter des Finanzamtes der Anrufende aufgrund der Stimme aus vorangegangenen Gesprächen persönlich bekannt sei, sei er berechtigt, ihm eine Auskunft zu der Steuernummer zu erteilen. Ansonsten hat durch den Mitarbeiter immer eine Überprüfung der Auskunftsberechtigung durch einen Rückruf zu erfolgen. Diese Verfahrensweise ist aus datenschutzrechtlicher Sicht nicht zu beanstanden.

Änderung des Kraftfahrzeugsteuergesetzes

Auf Initiative der Bundesländer wurde das Kraftfahrzeugsteuergesetz dahingehend geändert, dass die Zulassungsstelle bei der Anmeldung eines Kraftfahrzeuges den Fahrzeugschein erst aushändigen darf, wenn nachgewiesen ist, dass den Vorschriften über die *Kraftfahrzeugsteuer* genügt ist (§ 13). Hierzu dürfen die Landesregierungen die Aushändigung des Fahrzeugscheines durch Rechtsverordnung davon abhängig machen, dass die Kraftfahrzeugsteuer für den ersten Zeitraum entrichtet ist oder eine Einzugsermächtigung erteilt wird oder eine Bescheinigung vorgelegt wird, dass das Finanzamt wegen einer erheblichen Härte für den Fahrzeughalter darauf verzichtet (Erstversteuerungsverfahren).

Die 2002 in Kraft getretenen Änderungen des Kraftfahrzeugsteuergesetzes sind im Wesentlichen zutreffend dargestellt:

Nach dem neuen § 13 können die Landesregierungen die Aushändigung des Fahrzeugscheines durch Rechtsverordnung davon abhängig machen, dass

- die Kraftfahrzeugsteuer für den ersten Zeitraum entrichtet bzw. eine Einzugsermächtigung erteilt worden ist, oder

- für die KFZ-Steuer eine Einzugsermächtigung erteilt worden ist bzw. eine Bescheinigung vorgelegt wird, nach der das Finanzamt auf die Einzugsermächtigung wegen einer erheblichen Härte für den Fahrzeughalter (z.B. kein Konto bei einem deutschen Geldinstitut) verzichtet;

  und

- keine KFZ-Steuerrückstände für den Fahrzeughalter bestehen.

- Nach der Berliner Rechtsverordnung vom 27.07.02 ergänzt durch die Verordnung vom 26.11.02 darf in

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Berlin die Zulassungsbehörde den Fahrzeugschein erst aushändigen, wenn die Kraftfahrzeugsteuer für den ersten Zeitraum entrichtet bzw. eine Einzugsermächtigung erteilt worden ist und wenn die Zulassungsbehörde festgestellt hat, dass der Fahrzeughalter keine KFZ-Steuerrückstände hat.

Durch Rechtsverordnung darf auch geregelt werden, dass die Aushändigung des Fahrzeugscheines davon abhängig gemacht wird, dass keine Kraftfahrzeugsteuer-Rückstände bestehen. Zu diesem Zweck dürfen die Finanzämter den Zulassungsstellen Auskünfte über Kraftfahrzeugsteuer-Rückstände des Fahrzeughalters erteilen. Die Zulassungsstellen werden insoweit als Landesfinanzbehörden tätig. Wird das Fahrzeug nicht durch den Fahrzeughalter selbst zugelassen, muss derjenige, der das Fahrzeug zulässt, eine Einverständniserklärung des Steuerpflichtigen mit der Bekanntgabe seiner kraftfahrzeugsteuerlichen Verhältnisse an ihn vorlegen können.

Die Regelungen sollen dazu dienen, die fristgerechte Zahlung der Kraftfahrzeugsteuer sicherzustellen. Der Fahrzeughalter behält die Wahlmöglichkeit, selbst zu entscheiden, ob er der Zulassungsstelle Kontendaten übermitteln will, indem er die Kraftfahrzeugsteuer vor einer An- bzw. Ummeldung eines Kraftfahrzeuges entrichtet.

KfZ-Erstversteuerungsverfahren – auf die Datensicherheit kommt es nicht an

Das Landeseinwohneramt unterrichtete uns bereits 2001 über die Ergänzung des Verfahrens KVA (KfZ-Wesen), mit der die Erstversteuerung durchgeführt werden soll (Erstversteuerungsverfahren – EVV). Rechtsgrundlage für das Verfahren ist die „Verordnung über die Mitwirkung der Zulassungsbehörde bei der Verwaltung der Kraftfahrzeugsteuer" vom 27. Juli 2001[74], die am 1. Januar 2003 in Kraft getreten ist.

In unserer ersten Reaktion haben wir darauf hingewiesen, dass die Zulassungsbehörde im Zusammenhang mit dem EVV-Verfahren als Landesfinanzbehörde tätig wird und diese Tätigkeit damit dem Steuergeheimnis nach § 30 Abgabenordnung unterliegt.

Wir wiesen darauf hin, dass vor der Entscheidung über diese wesentliche Änderung des KVA-Verfahrens nach § 5 Abs. 3 Satz 1 BlnDSG die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzepts zu ermitteln sind. Bei Verfahren, die dem Steuergeheimnis unterliegen, gehört dazu nach Satz 2 auch eine Vorabkontrolle hinsichtlich möglicher Ge-

[74] GVBl. S. 320

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

fahren für das Recht auf informationelle Selbstbestimmung. Die Durchführung dieser Vorabkontrolle ist Aufgabe des behördlichen Datenschutzbeauftragten (§ 19 a Abs. 1 Satz 3 Nr. 1 BlnDSG).

Nunmehr haben wir festgestellt, dass das EVV-Verfahren pünktlich zum 2. Januar 2003 in den Echtbetrieb gegangen ist, ohne dass eine Risikoanalyse vorgenommen, ein Sicherheitskonzept erarbeitet und demzufolge auch umgesetzt und keine Vorabkontrolle durchgeführt wurde. Die Vorabkontrolle wäre ohne Risikoanalyse und Sicherheitskonzept auch nicht möglich gewesen.

Wir haben förmlich beanstandet, dass damit wider besseres Wissen das Erstversteuerungsverfahren in Betrieb genommen wurde, ohne dass die Vorschriften von § 5 Abs. 3 BlnDSG Beachtung gefunden hätten. Offensichtlich kommt es dem Landeseinwohneramt in dieser Anwendung, in der mit personenbezogenen Daten und erheblichen Geldsummen umgegangen wird, auf den Datenschutz und die Sicherheit der Datenverarbeitung nicht so genau an.

Der Senat hat die erforderlichen Vorkehrungen zur Gewährleistung des Datenschutzes rechtzeitig getroffen. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit wurde frühzeitig beteiligt und die Risikoanalyse sowie ein Sicherheitskonzept vor der Inbetriebnahme des Kfz-Erstversteuerungsverfahren erstellt. Auch die Vorabkontrolle durch den behördlichen Datenschutzbeauftragten wurde rechtzeitig eingeleitet. Durch ein Büroversehen des Landeseinwohneramtes waren die entsprechenden Unterlagen nur an den behördlichen Datenschutzbeauftragten des Landeseinwohneramtes und nicht auch an den Berliner Beauftragten für Datenschutz und Informationsfreiheit gesandt worden. Dies ist inzwischen nachgeholt worden.

4.4 Sozialordnung

4.4.1 Personaldatenschutz

Arbeitnehmerdatenschutzgesetz

Geradezu obligatorisch ist mittlerweile ein Hinweis auf die Notwendigkeit eines *Arbeitnehmerdatenschutzgesetzes*. Diese mittlerweile über zehn Jahre alte Forderung, den Datenschutz im Arbeitsverhältnis durch ein eigenständiges Gesetz zu stärken und für die Praxis übersichtlich und leicht anwendbar zu machen, hat an Aktualität nicht verloren. Datenschutzrechtliche Verstöße im Arbeitsverhältnis beruhen häufig nicht auf der Ignoranz oder gar Böswilligkeit der Arbeitgeber, sondern sind immer wieder auf die Unübersichtlichkeit der gesetzlichen Regelungen und einschlägigen arbeitsgerichtlichen Rechtsprechung zurückzuführen, die es insbesondere kleineren Unternehmen unnötig erschwert, die rechtlichen Vorgaben in der täglichen Arbeit umzusetzen. Es ist daher zu begrüßen, dass Bündnis90/Die Grünen und SPD im Koalitionsvertrag vereinbart haben, den Schutz der Daten der Arbeitnehmerinnen und Arbeitnehmer in einem eigenen Gesetz zu verankern[75].

Die im Jahresbericht 2002 enthaltene Forderung nach der Kodifizierung spezieller Vorgaben zum Arbeitnehmerdatenschutz in einem eigenständigen Arbeitnehmerdatenschutzgesetz ist auch aus arbeitsrechtlicher Sicht unterstützenswert. Sowohl die allgemeinen Regelungen des Bundesdatenschutzgesetzes als auch die mit Blick auf den Datenschutz nutzbaren betriebsverfassungsrechtlichen Beteiligungsrechte (z.B. § 87 Abs. 1 Nr. 6 BetrVG bezüglich technischer Einrichtungen, die dazu geeignet sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen und zu diesem Zweck Daten sammeln bzw. speichern oder das in § 94 Abs. 1 Satz 1 BetrVG enthaltene Zustimmungserfordernis für Personalfragebögen) sind zu rudimentär und unspezifisch, um den Besonderheiten des Arbeitnehmerdatenschutzes angemessen gerecht zu werden. Ziel dieser Maßnahme muss jedoch sein, praxistaugliche, übersichtliche und leicht anwendbare Vorgaben für die Rechtsanwender auf betrieblicher Ebene zu schaffen, die noch genügend Raum für spezifische Lösungen durch Tarifverträge oder durch Betriebsvereinbarungen lassen.

Unbedingt zu vermeiden ist in diesem Zusammenhang eine Überreglementierung, die einen durch klarstel-

[75] Koalitionsvertrag vom 16. Oktober 2002: „Erneuerung-Gerechtigkeit-Nachhaltigkeit", Kapitel VIII: „Sicherheit, Toleranz und Demokratie; Demokratische Beteiligungsrechte und Datenschutz"

lende Kodifizierung entstehenden Entlastungseffekt für die Rechtsanwender auf der einen Seite durch zu weitreichende Regularien auf der anderen Seite wieder konterkariert. Nötig – aber auch ausreichend – erscheint insofern lediglich eine Ergänzung der bereits existierenden allgemeinen Grundsätze und Generalklauseln des Datenschutzrechts um unabdingbar notwendige für das Arbeitsverhältnis zu beachtende Spezifika.

Nachdem derzeit nicht absehbar ist, wann und mit welchem Ergebnis die auf europäischer Ebene seitens der Kommission verfolgten Bestrebungen zur Schaffung spezieller Gemeinschaftsvorschriften für den Arbeitnehmerdatenschutz abgeschlossen sein werden, sollte mit der Schaffung eigener nationaler Vorgaben nicht länger gewartet werden. Die Ankündigung in der Koalitionsvereinbarung der die Bundesregierung tragenden Parteien ist daher auch aus arbeitsrechtlicher Sicht zu begrüßen.

Internet und E-Mail am Arbeitsplatz

Für immer mehr Arbeitnehmerinnen und Arbeitnehmer gehört der Einsatz moderner Telekommunikationsmittel zum beruflichen Alltag. Arbeitsabläufe werden beschleunigt und vereinfacht, Informationsressourcen für berufliche, aber auch private Zwecke erweitert und Fähigkeiten des Einzelnen im Umgang mit Informations- und Kommunikationstechnik vervollkommnet. In dem Maße aber, in dem der Einsatz moderner Telekommunikationstechnik im Arbeitsumfeld zunimmt, wachsen auch die Gefahren für die informationelle Selbstbestimmung der Arbeitnehmer. Surfen im Internet oder Versenden einer E-Mail hinterlässt Datenspuren in den Netzen. Je mehr Arbeitnehmerinnen und Arbeitnehmer auf die Nutzung von E-Mail und Internet während ihrer Arbeit angewiesen sind, umso leichter wird es für Vorgesetzte und Arbeitgeber, durch die Auswertung von protokollierten Verbindungs-, Nutzungs- oder sogar Inhaltsdaten umfassend die Leistung und das Verhalten ihrer Mitarbeiter zu kontrollieren. Datenschutz- und Arbeitsrecht müssen daher für einen Ausgleich zwischen den legitimen Direktions- und Kontrollrechten der Arbeitgeber auf der einen Seite und dem verfassungsrechtlich gebotenen Schutz der informationellen Selbstbestimmung der Arbeitnehmer auf der anderen sorgen.

Die rechtlichen Rahmenbedingungen zur Nutzung von Informations- und Kommunikationstechnik am Arbeitsplatz sind – insbesondere für diejenigen, die sich im Alltag damit ausein-ander zu setzen haben, also die Arbeitgeber und Arbeitnehmer – schwer zu fassen. Ob allein die allgemeinen Datenschutzgesetze oder aber auch Bestimmungen des Telekommunikationsrechts zum Tragen kommen, kann nur anhand des konkreten Einsatzes von IuK-Technik und des Umfangs der den Arbeitnehmern eingeräumten Nutzungsrechte bestimmt werden.

Die Datenschutzgruppe nach Art. 29 der Europäischen Datenschutzrichtlinie hat zu der Problematik ein Arbeitspapier erarbeitet[76]. Auch hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hierzu auf ihrer 63.-Sitzung im März 2002 eine Entschließung verabschiedet[77], die die datenschutzrechtlichen Grundsätze beim Einsatz von E-Mail und Internet am Arbeitsplatz kurz skizziert. Begleitet wurde diese von einer detaillierteren Orientierungshilfe[78], die der Arbeitskreis „Medien“ der Konferenz verfasst hatte.

Protokolldaten, die aus Gründen des Datenschutzes, der Datensicherheit oder des ordnungsgemäßen Betriebs des Datenverarbeitungsverfahrens gespeichert werden, unterliegen – unabhängig von der Frage, ob die E-Mail- und Internetnutzung im geringen Umfang auch für private Zwecke erlaubt ist – einer strikten Zweckbindung: Sie dürfen zur Leistungs- und Verhaltenskontrolle der Mitarbeiter nicht verwendet werden. Angesichts der für Laien nur schwer durchschaubaren Datenverarbeitungsprozesse müssen die Arbeitnehmer über ihre Nutzungsbefugnisse, über etwaige Kontrollfunktionen des Verfahrens, über Protokollierungen und über Verfahren zur Klärung eines begründeten Verdachts der missbräuchlichen Nutzung von Internet oder E-Mail umfassend informiert werden (Transparenz der Datenverarbeitung). Und nicht zuletzt weist die Konferenz darauf hin, dass private E-Mails als elektronische Post dem Telekommunikationsgeheimnis unterliegen, dessen Adressat auch jeder Arbeitgeber ist.

Um Unsicherheiten der Beschäftigten im Umgang mit E-Mail und Internet zu minimieren und Konflikte von vornherein zu vermeiden, raten wir jeder verantwortlichen Stelle, die Verfahren in Betriebs- bzw. Dienstvereinbarungen zwischen der Unternehmens- oder Behördenleitung auf der einen Seite und der Mitarbeitervertretung auf der anderen klar zu regeln. Insbesondere sollte darin festgehalten werden, welche Arten von Daten zu welchen Zwecken, mit Hilfe welcher Verfahren verarbeitet und wie lange sie gespeichert werden. Geregelt werden sollte auch, wie bei einem Missbrauchsverdacht einzelfallbezogene Überprüfungen – regelmäßig unter Beteiligung der Mitarbeitervertretung und des betrieblichen/behördlichen Datenschutzbeauftragten sowie Information der Betroffenen – durchgeführt werden können. Ebenso wichtig sind Vertretungsregelungen für den Fall der Abwesenheit eines Mitarbeiters. So kann eingehende elektronische Post an einen zuvor festgelegten Kollegen elektronisch weitergeleitet werden oder – zur Vermeidung, dass dieser

[76] vgl. 4.7.2

[77] Datenschutzgerechte Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2002”, S. 11

[78] Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz, vgl. Anlagenband, a. a. O., S. 21

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

private E-Mails des Abwesenden zur Kenntnis nimmt – der Absender automatisch auf die Abwesenheit des eigentlichen Empfängers hingewiesen werden, verbunden mit dem Angebot, sich mit seinem Anliegen an einen benannten Vertreter zu wenden. Empfehlenswert sind überdies Notfallregelungen für Zugriffe auf Postfächer von Mitarbeitern, die nicht erreichbar sind.

Die *Internet-Dienstvereinbarung* der Berliner Verwaltung, auf die der letzte Jahresbericht detailliert einging, deren Abschluss zum Zeitpunkt der Erstellung aber nur angekündigt werden konnte, trat am 21. Februar 2002 in Kraft. Damit verfügt der öffentliche Dienst des Landes Berlin nunmehr über ein Regelungswerk, das die Rahmenbedingungen der Nutzung von Internet und E-Mail am Arbeitsplatz nachvollziehbar absteckt. Auch wenn die Vereinbarung auf die besonderen Gegebenheiten der Berliner Verwaltung zugeschnitten ist, kann sie in einzelnen Punkten durchaus als Vorlage für Betriebs- oder Dienstvereinbarungen in anderen Bereichen dienen.

Die vom Berliner Beauftragten für Datenschutz und Informationsfreiheit gemachten Ausführungen bzgl. notwendiger Regelungen bei der Nutzung des Internet sind in der mit Datum vom 21.02.2002 mit dem Hauptpersonalrat abgeschlossenen Internet-Dienstvereinbarung der Berliner Verwaltung berücksichtigt. Die Vereinbarung entstand in enger Abstimmung mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit.

Der Senat begrüßt, dass der Berliner Beauftragten für Datenschutz und Informationsfreiheit diese Vereinbarung als Vorlage für entsprechend Vereinbarungen in anderen Bereichen ansieht.

Heimliches Mithören von Telefonaten in Call-Centern

Bereits in den vergangenen Jahren hat uns wiederholt das unbemerkte Ab- und Mithören von Telefonaten in *Call-Centern* und Unternehmen der Markt- und Meinungsforschung beschäftigt. Betreiber von Call-Centern verstehen die Überwachung von Telefonaten als Instrument der Qualitätssicherung. Soweit diese Maßnahmen mit Kenntnis der Beschäftigten in jedem Einzelfall geschehen, wird das Direktions- und Kontrollrecht des Arbeitgebers in zulässiger Weise wahrgenommen. Werden aber Telefonate der Mitarbeiter ohne vorherige Anmeldung und durch diese unbemerkt abgehört oder mitgeschnitten, liegt ein schwerwiegender Eingriff in ihr Persönlichkeitsrecht vor. Zur Klärung der Rechtslage in diesem Bereich haben wir den Arbeitnehmerdatenschutzexperten Prof. Dr. Peter Wedde um die Erstellung eines Gutachtens gebeten, dessen Ergebnis unsere rechtliche Auffassung bestätigte:

Das heimliche Ab- und Mithören von Telefonaten greift in das Recht am eigenen Wort des Betroffenen ein, welches als Ausprägung des grundrechtlichen Persönlichkeitsschutzes anerkannt ist. Es ist daher auch im Bereich von Call-Centern und in Unternehmen der Markt- und Meinungsforschung grundsätzlich unzulässig.

Zwar können Eingriffe in verfassungsrechtlich geschützte Bereiche auf eine Einwilligung des Betroffenen gestützt werden, wenn dabei der Verhältnismäßigkeitsgrundsatz gewahrt bleibt. Dies ist aber nicht der Fall, wenn Maßnahmen zu einer lückenlosen Leistungs- und Verhaltenskontrolle führen oder führen können. Eine solche Kontrollmöglichkeit besteht bei

Verfahren, die ein unbemerktes Ab- und Mithören vorsehen. Daher können sie weder durch allgemeine Regelungen in individuell abgeschlossenen Arbeitsverträgen noch durch kollektivrechtliche Vereinbarungen auf betrieblicher oder tariflicher Ebene legitimiert werden.

Ein Ab- und Mithören von Telefonaten ist somit nur aufgrund einer auf den konkreten Einzelfall bezogenen freiwilligen Einwilligung des Beschäftigten zulässig. Dies könnte beispielsweise während der Einarbeitungsphase zur Verbesserung der Qualität der telefonischen Beratung der Fall sein.

Nur im konkreten Ausnahmefall wäre auch bei einer unbemerkten Ab- oder Mithörmaßnahme die Verhältnismäßigkeit gewahrt, wenn beispielsweise der begründete Verdacht gegenüber einem einzelnen Mitarbeiter besteht, er begehe im Rahmen seiner telefonischen Aktivitäten strafbare Handlungen.

Das Ergebnis unserer Prüfung in den das Gutachten auslösenden Einzelfällen steht noch aus. Überdies streben wir an, über die betroffenen Unternehmensverbände eine einheitliche, datenschutzgerechte Verfahrensweise in Call-Centern und Unternehmen der Markt- und Meinungsforschung herbeizuführen.

Personalakten

Ein vom Land Berlin gekündigter Angestellter beschwerte sich darüber, dass eine Berliner Behörde in einem Kündigungsschutzprozess dem das Land vertretenden Rechtsanwalt seine vollständige Personalakte übersandt hatte. Die betreffende Behörde vertrat die Auffassung, dass dieses Verfahren in der Regel erforderlich sei, da häufig nicht abgeschätzt werden könne, welche Umstände des Beschäftigungsverhältnisses in der Gerichtsverhandlung von Relevanz sein können.

Die Übersendung der gesamten *Personalakte* an einen Rechtsanwalt ist aus datenschutzrechtlicher Sicht grundsätzlich unzulässig. Wir verkennen nicht, dass im Interesse einer effektiven Vertretung des Landes Berlin der betreffende Rechtsanwalt umfassend über die Hintergründe der Kündigung und des Arbeitsverhältnisses informiert sein muss. Allerdings kann nicht darauf verzichtet werden, dass durch die jeweilige Verwaltung vor Herausgabe der Personalakte eine Prüfung erfolgt, welche Aktenteile für die Untermauerung der dem Kündigungsschutzprozess zugrunde liegenden Kündigungsgründe nicht von Relevanz sind. Ein besonderes Augenmerk ist hierbei auf die Teile der Personalakte zu richten, die besonders sensitive Daten, beispielsweise Angaben über die Gesundheit der oder des Betroffenen, beinhalten. Soweit sie – was der Regelfall sein dürfte – für die Prozessführung nicht von Belang sind, müssen diese Teile der Akte vor einer Übersendung an den Rechtsanwalt herausgenommen werden. Hinnehmbar ist, dass trotz dieser vorherigen Prüfung einzelne

Der Senat teilt die Auffassung des Berliner Beauftragten für Datenschutz und Informationsfreiheit zur Frage der Übersendung von Personalakten von Angestellten des Landes Berlin an einen Rechtsanwalt.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Dokumente an den Rechtsanwalt übersandt werden, deren Relevanz für den Prozess sich nach eingehender Prüfung durch den in Arbeitsgerichtsprozessen erfahrenen Fachanwalt nicht bestätigt.

Eine Petentin hatte sich im Sommer 2001 für eine Tätigkeit als Angestellte einer Behörde beworben. Bei einer Nachfrage, warum ihre Bewerbung nicht erfolgreich war, wurde auf längere Fehlzeiten aus Krankheitsgründen verwiesen, die in ihrer Personalakte zu einer Ausbildungszeit, welche sie im Jahre 1993 abbrechen musste, gespeichert gewesen seien.

Für die Speicherung von Fehlzeiten aus Krankheitsgründen sieht das Landesbeamtengesetz (LBG) klare Fristen vor, die analog auch für die *Personalaktenführung* von Angestellten gelten. Nach § 56 f. Abs. 3 LBG sind Unterlagen über Erkrankungen fünf Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, aufzubewahren und nach Abs. 4 mit Ablauf der Aufbewahrungsfrist zu vernichten. Im Falle der Petentin hätten die Angaben über Fehlzeiten aus Krankheitsgründen also mit Ablauf des Jahres 1998 gelöscht werden müssen. Bei einer Prüfung des Sachverhalts stellte sich heraus, dass diese Löschung tatsächlich stattgefunden hatte. Bei den in Rede stehenden Unterlagen handelte es sich um die Ergebnisse einer von der Behörde angeordneten amtsärztlichen Untersuchung, die Grundlage der Entscheidung zur Entlassung der Petentin aus dem Ausbildungsverhältnis war. Ihre Speicherung war zulässig, da sie obligatorischer Teil der Personalakte sind. Hierzu gehören nämlich auch Unterlagen, die die Art und Weise erhellen, in der die jeweilige Entscheidung vorbereitet worden ist, oder die Aufschluss über die Gesichtspunkte und Erwägungen geben, die für die einzelne das Dienstverhältnis berührende Maßnahme oder dafür, dass sie unterblieben ist, maßgebend waren[79]. Die Aktenführung der Behörde war daher nicht zu beanstanden.

Bei der Prüfung dieser Eingabe befassten wir uns auch generell mit der Speicherung von krankheitsbedingten Fehlzeiten in der Berliner Verwaltung. Dabei mussten wir feststellen, dass für die fristgemäße Löschung der Fehlzeiten von Beschäftigten nur unzureichende Vorkehrungen getroffen worden sind, mithin diese Fristen häufig überschritten werden. Den Personalakten wird generell ein Personalblatt vorangestellt, auf welchem fortlaufend die Zeiträume von Erkrankungen der Beschäftigten eingetragen werden. Die entsprechenden Vorgaben wurden durch Rundschreiben der Senatsverwaltung für Inneres den Behörden bekannt gemacht. Hinweise auf Löschungspflichten hinsichtlich dieser Eintragungen enthielten diese Rundschreiben nicht. Dies führte dazu, dass Fehlzeiten über Jahre gespeichert blieben und für Einsichtnehmende jederzeit die

Die Aufbewahrungsfristen für Personalakten der Beamtinnen und Beamten ist in § 56 f LBG geregelt. Nach § 56 f Abs. 2 Satz 1 LBG sind Unterlagen u.a. über Erkrankungen fünf Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, aufzubewahren. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit problematisiert die Führung von Aktenvorblättern für Personalakten der Beamtinnen und Beamten, auf denen die Fehlzeiten chronologisch ohne vorgesehene Löschungsfristen vermerkt werden, als mit dem Gesetz nicht vereinbar. Der Senat teilt diese Ansicht nicht:

Die datenmäßige Erfassung von Krankheitszeiten auf Aktenvorblättern erfüllt nicht den Unterlagenbegriff im Sinne von § 56 f Abs. 2 Satz 1 LBG; insoweit

[79] BVerwGE 15, 3 (12 ff.); 67, 300 (302)

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Krankheitszeiten der Beschäftigten auch aus lang zurückliegenden Zeiträumen ersichtlich waren. Wir haben die Senatsverwaltung für Inneres aufgefordert, dafür Sorge zu tragen, dass künftig in allen Berliner Verwaltungen die Daten zu Erkrankungen unter Berücksichtigung von § 57 f. LBG nach Ablauf der Fünfjahresfrist gelöscht werden.

unterliegen die Personalaktenvorblätter nicht der gesetzlich geregelten Aufbewahrungsfrist von fünf Jahren. Anders als die Erkrankungsanzeigen, die nach der Fünfjahresfrist des § 56 f Abs. 2 Satz 1 LBG zu entfernen sind, lässt die schlichte Auflistung der Fehlzeiten im Aktenvorblatt keinen Rückschluss auf die Art der Erkrankung zu, wie es z.B. durch die Angabe des Arztes und der ärztlichen Fachrichtung auf der Erkrankungsanzeige der Fall ist. Zudem ist die Kenntnis von Fehlzeiten über einen längeren Zeitraum wesentlich im Hinblick auf die Einleitung eines Verfahrens zur Zurruhesetzung wegen Dienstunfähigkeit nach §§ 77, 78 LBG. Abschließend sei darauf hingewiesen, dass die kürzeren Aufbewahrungsfristen des § 56 f Abs. 2 Satz 1 LBG der Verwaltungsvereinfachung und nicht dem Schutz des Rechts auf informationelle Selbstbestimmung der Beamten dienen.

Die „Handakte" eines Petenten, die bei seiner Dienststelle geführt wird, enthielt u. a. medizinische Gutachten des Betriebsarztes, Beurteilungen von Vorgesetzten und Unterlagen über einen zurückliegenden Arbeitsrechtsstreit.

Das Führen einer *Nebenakte* zur Personalakte (häufig auch als Handakte bezeichnet) ist nach § 56 Abs. 2 Satz 3 LBG zulässig, wenn die personenverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist, ihre Aufgabenerfüllung aber das Bereithalten bestimmter Personalaktendaten erforderlich macht. Dieser Grundsatz gilt auch für Außenstellen einer Behörde, wenn diese selbst Aufgaben der Personalverwaltung wahrnehmen und hierfür das Führen einer Nebenakte zwingend erforderlich ist. Für die Aufgabenerfüllung erforderliche Unterlagen dürfen nur dann in die Nebenakte aufgenommen werden, wenn sie im Original oder als Kopie in der Grund- bzw. Teilpersonalakte enthalten sind. Somit kann die Nebenakte nur spiegelbildlich Teile der eigentlichen Grundakte wiedergeben, nie jedoch selbständig einen Bereich des Beschäftigungsverhältnisses dokumentieren. Eine Prüfung der Eingabe durch den behördlichen Datenschutzbeauftragten, an den sich der Petent ebenfalls gewandt hatte, ergab, dass die Nebenakte Dokumente enthielt, die für die Aufgabenerfüllung der Außenstelle nicht erforderlich waren (wie medizinische Gutachten, die ohnehin auch innerhalb der Personalakte besonders geschützt werden müssen, und Angaben zu einem früheren Arbeitsrechtsstreit). Überdies befanden sich dort auch Unterlagen, die generell nicht in einer Personalakte hätten abgelegt werden dürfen. Die Prüfung hat zur Bereinigung der Akte geführt.

Die Eingabe betraf einen Missstand, der in der betreffenden Behörde, die von der Natur der Sache her in großem Umfang mit Nebenakten arbeitet, nicht auf die Personalakte des Petenten beschränkt ist. Der behördliche Datenschutzbeauftragte hatte daher eine Dienstanweisung der Behördenleitung angekündigt, die die Grundsätze zum Führen von Nebenakten regeln sollte.

Trotz einer Mahnung auch unsererseits ist bis heute eine solche Dienstanweisung nicht erlassen worden.

Mitarbeiter eines Unternehmens beschwerten sich bei uns darüber, dass in den in ihrem Betrieb öffentlich ausliegenden Wählerlisten zur Betriebsratswahl hinter dem jeweiligen Namen auch die Geburtsdaten der Betroffenen aufgeführt wurden.

Nach der Wahlordnung zum Betriebsverfassungsgesetz hat zwar der Wahlvorstand eine Liste mit allen wahlberechtigten Betriebsangehörigen zu führen, in der auch das Geburtsdatum der Wähler verzeichnet ist. Diese ausführliche Liste soll aber nur dem Wahlvorstand selbst zur Verfügung stehen, der über die ordnungsgemäße Durchführung der Wahl zu wachen hat. Das Geburtsdatum ermöglicht es ihm, die Wahlberechtigung nach § 7 BetrVG (18 Jahre) festzustellen sowie – bei Namensgleichheit in größeren Unternehmen – die jeweiligen Wähler genau zu identifizieren. Im Betrieb öffentlich auszulegen ist nach § 2 Abs. 4 der Wahlordnung zum Betriebsverfassungsgesetz jedoch nicht dieses Original, sondern ein Abdruck der Wählerliste, der die Geburtsdaten aus Gründen des Persönlichkeitsschutzes der Betroffenen nicht enthalten soll. Bestehen Zweifel an der Wahlberechtigung nach § 7 BetrVG eines in der Liste aufgeführten Beschäftigten, so kann der Wahlvorstand um Überprüfung gebeten werden.

Erkenne dich Selbst mit Hilfe deines Arbeitgebers

Ein Unternehmen hatte seinen Mitarbeitern aufgegeben, einen siebzig Punkte umfassenden Fragebogen zur Analyse des Persönlichkeitstyps auszufüllen. Die Analyse kam geradezu unverfänglich daher: „Welcher Typ sind Sie? Lernen Sie Ihr Strickmuster besser kennen. Was sind die Vorzüge Ihres Musters? Wofür ist es besonders geeignet? Wir arbeiten in unserem Personalentwicklungsteam seit Jahren mit dem folgenden typologischen Fragebogen. (...) Bei diesem Fragebogen gibt es keine Verlierer. Jeder erfährt seine persönliche Stärken. Das ist das Reizvolle daran. Sie können also spontan und ohne Furcht vor unangenehmen Enthüllungen Ihre Kreuze setzen: Es gibt kein falsch oder richtig. Je offener Sie antworten, desto klarer ist das Bild, das Sie von Ihren eigenen Stärken bekommen."

Das *Personalentwicklungsteam* interessierte sich dann vor allem dafür, ob die Probanden bei geselligen Anlässen möglichst viele Leute kennen lernen wollen oder sich lieber auf einige Bekannte konzentrieren, ob sie, was andere betrifft, in ihrem Kollegen-/Bekanntenkreis eher auf dem Laufenden oder nicht auf dem neuesten Stand seien. Beantwortet werden sollte auch die Frage, ob man sich nach einem Kauf wohler fühle, oder aber wenn der Kauf noch bevorsteht. Auch für die Auffassung zur perfekten Beziehung interessierten sich die Personalentwickler. So sollten die Probanden angeben, ob sie es bevorzugen, dass in einer Beziehung die meisten Angelegenheiten klar geregelt sind oder sie

eher den Umständen entsprechend behandelt werden sollten.

Eine Mitarbeiterin bezweifelte, dass ihr Arbeitgeber die Beantwortung dieses Fragebogens von ihr verlangen könne. Sie lag mit ihren Zweifeln richtig: Die Verarbeitung personenbezogener Daten im Arbeitsverhältnis, also innerhalb eines Vertragsverhältnisses, ist nur unter den Voraussetzungen des § 28 Abs. 1 Nr. 1 BDSG zulässig (bei sensitiven Daten § 28 Abs. 6 Nr. 3 BDSG). Danach muss die konkrete Datenverarbeitung erforderlich sein, um den Zweck des Arbeitsverhältnisses zu erfüllen. Angaben zu persönlichen Vorlieben und Ansichten zur Kindererziehung oder zur perfekten Partnerschaft spielen für das Arbeitsverhältnis keine Rolle und gehen somit den Arbeitgeber auch nichts an. Genauso wenig ist ein Personalentwicklungsteam legitimiert, in der Privatsphäre der Belegschaft herumzuschnüffeln. Überdies kann vor „Persönlichkeitsanalysen" innerhalb eines Beschäftigungsverhältnisses nur gewarnt werden. So unverfänglich die einzelnen Fragen erscheinen mögen; in ihrer Gesamtheit vermögen sie häufig mehr auszusagen, als einem lieb ist – selbst wenn man meint, man habe nichts zu verbergen.

4.4.2 Gesundheitswesen

Anforderungen an Medizinnetze

Im letzten Jahr haben wir uns schwerpunktmäßig mit der *Telemedizin* auseinandergesetzt, dabei Berliner Projekte vorgestellt und bundesweite Entwicklungen diskutiert, die auch im Zusammenhang mit den komplizierten Bemühungen um die Gesundheitsreform stehen[80].

In der Zwischenzeit hat eine gemeinsame Arbeitsgruppe der Arbeitskreise Gesundheit/Soziales und Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ein Arbeitspapier „Datenschutz und Telemedizin – Anforderungen an Medizinnetze" erarbeitet, welches sowohl die rechtlichen Voraussetzungen und Grundlagen als auch die technischen Anforderungen zur Gewährleistung des im Bereich der ärztlichen Schweigepflicht gebotenen hohen Sicherheitsniveaus zusammenfasst.

Die einrichtungsübergreifende elektronische Kommunikation soll in der Gesundheitsversorgung die Kommunikation zwischen den Institutionen fördern und die Leistungsprozesse verbessern. Telemedizin soll zur Verbesserung der Heilungschancen für die Patienten und gleichzeitig zur Kosteneinsparung führen.

Auch bei telemedizinischen Anwendungen ist die ärztliche Schweigepflicht zu gewährleisten, d. h., es ist

[80] JB 2001, 3.4

sicherzustellen, dass die Rechtsgrundlage zur Weitergabe von Patientendaten auch dann auf deren informierter und explizit zum Ausdruck gebrachter Einwilligung beruht, wenn die Daten über Netze transportiert und in entfernten Systemen gespeichert und ausgewertet werden. Gleiches gilt für die Dokumentationspflichten des Arztes, die Wahrung der Informationsrechte der Patienten und die Beachtung der in den Ländern unterschiedlichen Regelungen zur Zulässigkeit der Auftragsdatenverarbeitung.

Das Arbeitspapier geht dabei von vier Grundszenarien für die Datenhaltung aus, die in reiner Form oder kombiniert alle Modelle für die Datenhaltung beschreiben können: Dezentrale, zentrale, verteilte Datenhaltung sowie die dezentrale Datenhaltung mit zentraler Komponente. Für diese unterschiedlichen Grundszenarien werden die Verteilung der datenschutzrechtlichen Verantwortung, die Realisierung der Patienteneinwilligung sowie die Wirkung auf den Beschlagnahmeschutz der Patientendaten beschrieben.

Neben den rechtlichen Rahmenbedingungen für telemedizinische Anwendungen sind grundlegende Sicherheitsanforderungen zu betrachten. Dabei handelt es sich um

- die *Vertraulichkeit* der Daten, die sowohl auf den Übertragungswegen als auch bei der Speicherung in den beteiligten Datenverarbeitungssystemen nur durch starke *Verschlüsselungsverfahren* sichergestellt werden kann;

- die *Authentizität* bzw. Zurechenbarkeit der Daten, also die Feststellbarkeit des Urhebers bzw. Verantwortlichen für patientenbezogene Daten, der Auslöser bzw. Verantwortlichen von Verarbeitungsvorgängen mittels *elektronischer Signatur und elektronischen Zeitstempels;*

- die *Integrität* der Daten, die verlangt, dass die personenbezogenen Daten in allen Phasen der Verarbeitung unversehrt, vollständig, gültig und widerspruchsfrei bleiben, ebenfalls durch die *elektronische Signatur*;

- die *Verfügbarkeit* der Daten und darin impliziert der zur ordnungsgemäßen Verarbeitung notwendigen Hard- und Softwarekomponenten durch *hochverfügbare Systemauslegung* und *Backup-Verfahren*;

- die *Revisionsfähigkeit* der Verarbeitungsprozesse als Ausprägung der ärztlichen Dokumentationspflicht, so dass festgestellt werden kann, wer wann welche patientenbezogenen Daten wie verarbeitet, durch *elektronische Signatur und Protokollierung*;

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

- die *Validität* der Daten, d. h. ihre aktuelle Bereitstellung in einer für den Nutzungszweck angemessenen Qualität (z. B. Auflösung und Farbechtheit von Bilddaten) durch *Standardisierung* der für die Validität relevanten Systemkomponenten im Hinblick auf ihre Qualitätsansprüche;

- die *Rechtssicherheit*, also die Beweiskräftigkeit der Nachweise für die Verarbeitungsvorgänge und deren Ergebnisse, durch die *qualifizierte elektronische Signatur*;

- die *Nicht-Abstreitbarkeit von Datenübermittlungen* durch den Empfänger durch *Quittungsverfahren* unter Verwendung elektronischer Signaturen;

- die *Nutzungsfestlegung*, also die Bestimmung des Nutzerkreises, abgestufter Nutzungsrechte und von Nutzungsausschlüssen, durch *systemweite Berechtigungskonzepte und Zugriffskontrollmechanismen*.

Als Beispiele für telemedizinische Konzepte beschreibt das Papier das System zur patientenbegleitenden Dokumentation (PaDok) des Fraunhofer-Instituts für Biomedizinische Technik, mit dem ein Großteil der alltäglichen Kommunikation von Leistungserbringern im Gesundheitswesen unter Beachtung der meisten oben genannten Anforderungen erfüllt wird, sowie die Konzepte zur Elektronischen Patientenakte (EPA), die auch in der Diskussion zur Reform des Gesundheitswesens eine Rolle spielen. Diese Konzepte gehen einheitlich von einer Kombination aus einer Chipkarte mit Schlüsselfunktion und einem gesicherten Zugang an pseudonymisierte Daten aus. Sie variieren in der Frage des Ortes der Speicherung: Entweder enthält die Patientenchipkarte selbst die Patientendaten oder die Chipkarte erschließt den Zugriff auf anderweitig gespeicherte Daten.

Überprüfung der Arbeitsunfähigkeit

Eine Krankenkasse versandte Fragebögen an die Vertragsärzte arbeitsunfähig geschriebener Patienten, mit deren Hilfe Daten über die Krankheit des Versicherten, über deren bisherigen Verlauf, über die Schwere der Krankheit, den Behandlungsplan, die verabreichten Medikamente, die Herkunft der Krankheit, die stufenweise Wiedereingliederung und eine Prognose für den weiteren Verlauf erhoben werden sollten. Nach Auffassung der Krankenkasse seien die Vertragsärzte zu solchen Angaben verpflichtet.

Die Krankenkasse begründete dies mit der Regelung in § 36 Abs. 2 *Bundesmantelvertrag Ärzte* (BMV-Ä). Nach dieser Regelung sei ein Vertragsarzt befugt und verpflichtet, die zur Durchführung der Aufgaben der

Die Auffassung des Berliner Beauftragten für Datenschutz und Informationsfreiheit wird geteilt. Der Medizinische Dienst der Krankenkassen hat gemäß § 275 Abs. 1 Ziffer 3 SGB V die Arbeitsunfähigkeit zu überprüfen. Sowohl die Krankenkasse als auch die Kassenärztliche Vereinigung Berlin wurden entsprechend unterrichtet.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Krankenkassen erforderlichen Informationen (Auskünfte, Bescheinigungen, Zeugnisse, Berichte und Gutachten) auf Verlangen der Krankenkassen zu übermitteln. Der Bundesmantelvertrag kann sich jedoch nur auf das Verhältnis zwischen den Vertragsärzten und den Krankenkassen beziehen. Er kann keine Eingriffsbefugnisse gegenüber Patienten schaffen.

Wie sich aus § 36 Abs. 2 BMV-Ä in Verbindung mit der Vordruckvereinbarung zu dieser Regelung ergibt, sind für die Erteilung von Auskünften einheitliche Vordrucke zu verwenden. Reichen die Vordrucke zur Klärung des Sachverhaltes nicht aus oder liegen keine Vordrucke vor, dürfen Krankenkassen die benötigten Informationen zwar ausnahmsweise auch auf nicht vereinbarten Vordrucken anfordern. Dabei ist allerdings anzugeben, nach welcher Bestimmung des Sozialgesetzbuches (SGB) oder welchen anderen Regelungen die Übermittlung der Information zulässig ist.

Nach den dortigen Regelungen ist die Arbeitsunfähigkeit vom Medizinischen Dienst der Krankenkassen (MDK) zu überprüfen und nicht durch Befragung bei den behandelnden Ärzten. Der MDK ist nach § 275 Abs. 1 Ziff. 3 SGB V zur Begutachtung im Auftrag der Krankenkassen verpflichtet, woraus sich zwar weitgehende Informationspflichten des MDK gegenüber den Krankenkassen ergeben. Die behandelnden Ärzte sind jedoch nur dem MDK gegenüber verpflichtet, Informationen über die Ursachen und Ausmaß der Arbeitsunfähigkeit im Rahmen des versicherungsrechtlichen Leistungsverhältnisses zu erteilen (vgl. § 276 Abs. 4 und 5 SGB V).

Die Jagd nach Blaumachern

Wegen einer in der Öffentlichkeit zu erwartenden großen Resonanz wollte ein Fernsehsender über die „Jagd auf die Blaumacher", d. h. zu Unrecht arbeitsunfähig geschriebene Erkrankte, berichten. Er trat an eine gesetzliche Krankenkasse mit der Bitte heran, Berater von arbeitsunfähig geschriebenen Versicherten mit einem Kamerateam begleiten zu dürfen. Nach Angabe der Krankenkasse wurde versucht, vier Patienten in Begleitung des Kamerateams aufzusuchen. Von den vier Versicherten wurde nur eine Person angetroffen. Das Kamerateam wurde von der Krankenkasse mit der Patientenadresse versorgt und darüber informiert, dass es sich um Patienten handele, die von einem Arzt krankgeschrieben worden waren, der wegen der Vielzahl erstellter Arbeitsunfähigkeitsbescheinigungen auffällig geworden war. Es bestünden Zweifel, ob die Arbeitsunfähigkeit richtig diagnostiziert worden sei. Eine Mitarbeiterin der Krankenkasse habe das Kamerateam dann mit zur Wohnung genommen, an der Wohnungstür geklingelt und sich und ihr Anliegen der arbeitsunfähigen Person vorgestellt. Vor weiteren Fragen habe sie auf das Kamerateam verwiesen, das zu diesem Zeitpunkt noch nicht filmte, und gefragt, ob das Gespräch aufgenommen werden dürfe. Dem habe

Die Überprüfung einer Krankschreibung ist verbindlich geregelt und die gesetzlichen Krankenkassen müssen den im 275 SGB V vorgeschriebenen Weg einhalten. Es ist unzulässig, die Anschrift und den Status „arbeitsunfähig" ohne vorherige Einwilligung des jeweiligen Versicherten an Fernsehsender oder sonstige Dritte zu übermitteln. Diese Rechtslage wurde der Kasse mit der Bitte um Beachtung mitgeteilt.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

die versicherte Person zugestimmt. Erst dann wurde das Gespräch aufgezeichnet, allerdings nicht gesendet.

Von der Krankenkasse wurde mitgeteilt, dass sie von dem Hausbesuch in Begleitung des Kamerateams unterrichtet gewesen sei und ihn unter der Bedingung genehmigt habe, dass die Aufzeichnung durch das Kamerateam nur mit Zustimmung der betroffenen Person stattfinden dürfe.

Die Überprüfung der *Arbeitsunfähigkeit* erfolgt nach § 275 Abs. 1 Ziff. 3 SGB V, der die Krankenkassen verpflichtet, bei Zweifeln eine gutachterliche Stellungnahme des Medizinischen Dienstes einzuholen. Krankenkassen können zwar im Rahmen ihrer Aufgabenerfüllung ihren Versicherten bei anhaltender Arbeitsunfähigkeit Beratung und Betreuung anbieten. Dazu mögen auch Hausbesuche unter geeigneten Umständen in Betracht kommen. Es mag auch sachlich gerechtfertigt sein, dass bei einem auffällig gewordenen Arzt in verstärktem Maße arbeitsunfähige Patienten angesprochen werden.

Nach § 35 SGB I hat aber jeder Anspruch darauf, dass seine Sozialdaten von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt oder gar übermittelt werden (Sozialgeheimnis). Das Sozialgeheimnis erlaubt es nicht, Daten von Versicherten (Sozialdaten) an Fernsehsender zu übermitteln. Genau dies war nach Darstellung der Krankenversicherung allerdings geschehen.

Zwar verwies die Krankenkasse darauf, dass die zu Hause angetroffene Person sich mit den Dreharbeiten einverstanden erklärt habe. Dies kann jedoch die zuvor unzulässig erfolgte Übermittlung der Anschriften und des Gesundheitsstatus „Arbeitsunfähig" nicht heilen.

Ende eines Konflikts

Das Bundessozialgericht hat einen Schlussstrich unter eine jahrelange Auseinandersetzung zwischen Krankenkassen und Krankenhäusern gezogen. Es ging um die Anforderung der *Krankenhausentlassungsberichte* bei den Krankenhäusern. Die Krankenkassen wollten die Wirtschaftlichkeit und Angemessenheit der Krankenhausaufenthaltsdauer überprüfen. Um die Krankenhäuser zur Offenbarung dieser Informationen zu zwingen, wurde in Tausenden von Behandlungsfällen die Zahlung verweigert[81].

Das Bundessozialgericht hat nunmehr[82] Klarheit geschaffen. Es verweist auf die Informationsbefugnisse der Krankenkassen nach § 100 Abs. 1 Satz 1 Nr. 1 Satz 3 SGB X. Danach sind die Krankenhäuser zwar ver-

Die zuständige Senatsverwaltung hat den landesweiten Berliner Kassen mitgeteilt, unverzüglich die Konsequenzen aus der genannten Entscheidung des Bundessozialgerichts vom 23. Juli 2002 zu ziehen und medizinische Unterlagen von den Krankenhäusern nur noch dem Medizinischen Dienst der Krankenkassen zu übermitteln.

[81] JB 2001, 4.4.2

[82] Urteil vom 23. Juli 2002, Az.: B 3 KR 64/01 R

pflichtet, im Einzelfall den Krankenkassen auf Verlangen Auskunft zu erteilen, soweit es für die Durchführung ihrer Aufgaben nach dem SGB erforderlich und gesetzlich zugelassen ist. Die Übermittlung von Behandlungsunterlagen wird nach Auffassung des Gerichts hiervon aber nicht erfasst. Denn der Begriff „Auskunft" ist bereits seinem Wortsinn nach etwas anderes als „die Herausgabe der Unterlagen". Dies zeige auch die Regelung des § 276 Abs. 1 Satz 1 SGB V, wonach die Krankenkassen verpflichtet sind, dem MDK für die Beratung und Begutachtung erforderliche Unterlagen vorzulegen und Auskünfte zu erteilen. Eine Vorschrift, die eine Übermittlung der Behandlungsunterlagen an die Krankenkassen ausdrücklich vorschreibt, sei nicht ersichtlich.

§ 301 SGB V stelle aus datenschutzrechtlichen Gründen abschließend auf, welche Angaben den Krankenkassen bei der Krankenhausbehandlung ihrer Versicherten zu übermitteln sind. Dazu gehören die Stammdaten der Versicherten, die Institutionskennzeichen von Krankenkasse und Krankenhaus, Detaildaten über Aufnahme, Verlegung, Art der Behandlung und Entlassung einschließlich der Angabe des einweisenden Arztes mit Einweisungsdiagnose, Aufnahmediagnose und Änderung von Diagnosen, die medizinische Begründung für die Verlängerung der Verweildauer sowie Datum und Art der durchgeführten Operationen und Prozeduren – nicht aber die Behandlungsunterlagen der Versicherten, die in § 301 SGB V keine Erwähnung finden.

Auch wir hatten der Arbeitsgemeinschaft der Krankenkassen empfohlen, auf die Anforderung des Krankenhausentlassungsberichtes zu verzichten, weil der Wortlaut des SGB, die „Aushändigung von Behandlungsunterlagen" nicht vorsieht. Wir gehen davon aus, dass nach dieser Entscheidung die Informationsflüsse zwischen Krankenkassen und Krankenhäusern geklärt sind und zu keinen Reibungsverlusten mehr führen.

Der Schadensgutachter oder: „Klein ist die Welt!"

Nach einem Unfall erteilte ein Petent eine Entbindung von der ärztlichen Schweigepflicht für die Schadensregelung durch die gegnerische Versicherung. Die Stellungnahmen der behandelnden Ärzte gefielen dem Sachbearbeiter dieser Versicherung offenbar nicht. Ohne den Petenten zu befragen, übermittelte er die ärztlichen Stellungnahmen mit persönlichen und medizinischen Daten, Arztrechnungen und dem Kfz-Unfallgutachten sowie Teilen der Korrespondenz an einen Gutachter. Dieser Gutachter war, so wollte es der überraschende Zufall, der Ausbilder des Betroffenen.

Nachdem wir unsere Bedenken vorgebracht haben, hat sich die Versicherung bereit erklärt, ein Verfahren einzuführen, bei dem vom Anspruchsteller erst die Zustimmung für ein *Fremdgutachten* eingeholt werden

soll, bevor die Unterlagen mit den ärztlichen Daten an den Gutachter geschickt werden. Verbunden mit einer erweiterten Schweigepflichtentbindung soll dem Anspruchsteller eine Liste mit mehreren infrage kommenden Gutachtern übersandt werden, zu denen er im Einzellfall seine Ablehnung erklären könne. Wenn er alle vorgeschlagenen Gutachter ablehne, müsse er allerdings mit der Ablehnung seines Anspruchs seitens der Versicherung rechnen.

Dies kann zwar gravierende Verfahrensänderungen nach sich ziehen, die im Einzelnen noch von dem Unternehmen und im Gespräch mit dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) bedacht werden müssen. Jedoch scheint hier ein interessanter Weg zur Verbesserung der informationsrechtlichen Situation von Unfallopfern bei der Schadensregulierung gangbar zu werden. Dass der zunächst angeschriebene Gutachter hier ausgerechnet ein Ausbilder des Unfallopfers war, kommentierte die Versicherung mit den Worten: „Hierfür können wir uns nur entschuldigen."

Wechsel des Betriebsarztes

Ein Berliner Gesundheitsamt beabsichtigte einen neuen Betriebsarzt zu bestellen. Um die Patientenakten durch den Nachfolger weiterführen zu können, wurde von den Beschäftigten eine Schweigepflichtentbindung zugunsten des neuen, namentlich bestimmten Betriebsarztes eingeholt. Das Landesamt für Arbeitsschutz, Gesundheitsschutz und technische Sicherheit hat auf Anfrage des Gesundheitsamtes empfohlen, pragmatisch zu verfahren und die Mitarbeiter des Bezirksamtes über die Erfordernisse und Prozeduren der arbeitsmedizinischen Vorsorge, den Betreuungswechsel und die Übergabe der medizinischen Unterlagen mit einem Hinweis auf ein Widerspruchsrecht gegen die Übergabe zu informieren.

Die Annahme, dass der Arbeitgeber seiner Verantwortung für Sicherheit und Gesundheitsschutz der Beschäftigten bei der Arbeit (die sich im übrigen nicht aus dem ASiG, sondern aus dem Arbeitsschutzgesetz - ArbSchG - ergibt) nicht nachkommen könne, wenn er nicht über die betriebsärztlichen Unterlagen verfüge, ist irrig. Über die Maßnahmen des Arbeitsschutzes hat der Arbeitgeber auf Grund der Beurteilung der Arbeitsbedingungen zu entscheiden (§ 5 ArbSchG). Hat der Arbeitgeber infolge des Ergebnisses der Beurteilung der Arbeitsbedingungen arbeitsmedizinische Untersuchungen **zu veranlassen**(z.B. nach § 15 BiostoffV), **anzubieten** (z. B. nach § 6 BildscharbV) oder **zu ermöglichen** (z.B. nach § 6 ArbZG), so sind nicht die im Rahmen dieser Untersuchungen ermittelten Befunde, sondern allenfalls die vom Arzt auszustellende „ärztliche Bescheinigung", die lediglich eine Aussage enthält, ob gesundheitliche Bedenken gegen die Ausübung einer speziellen Tätigkeit bestehen oder nicht, für die Arbeitsschutzentscheidungen des Arbeitgebers relevant.

Bei einem Großteil der arbeitsmedizinischen Untersuchungen steht dem Arbeitgeber jedoch keine solche ärztliche Bescheinigung zu, ihre Ausstellung ist z.T. explizit ausgeschlossen (z.B. Untersuchungen nach § 15 Abs. 2 BiostoffV).

D.h.: ein Großteil der arbeitsmedizinischen Untersuchungen sind vom Gesetzgeber bewusst so konzipiert, dass sie ausschließlich der Beratung des Beschäftigten, nicht als Entscheidungshilfe für den Arbeitgeber dienen. Die Frage des Informationstransfers zwischen Arzt und Arbeitgeber auf eine Frage der berufsrechtlichen Verschwiegenheitspflicht des Arztes zu reduzie-

Das Arbeitssicherheitsgesetz sieht die betriebliche Sicherheit als Aufgabe des Arbeitgebers an. Die Bereitstellung einer betriebsärztlichen Einrichtung ist eine gesetzliche Pflichtaufgabe des Arbeitgebers. Der *Betriebsärztliche Dienst* ist von einem Arzt wahrzunehmen, der der ärztlichen Berufsordnung unterliegt. Er ist zur Verschwiegenheit und zur Führung von Aufzeichnungen verpflichtet, die zehn Jahre aufzubewahren sind. Bei Veräußerung einer Privatpraxis eines frei niedergelassenen Arztes kann die Patientendokumentation zwar nur an den Praxisnachfolger übergeben werden, soweit die Zustimmung der Patienten dafür eingeholt werden konnte. Die betriebliche Sicherheit ist jedoch eine arbeitsrechtliche Pflicht des Arbeitgebers. Der Arzt wird im Auftrag des Arbeitgebers tätig. Der Arbeitgeber kann diese Aufgaben auch auf einen externen Betriebsärztlichen Dienst verlagern. Auch ein externer Betriebsärztlicher Dienst unterliegt der ärztlichen Schweigepflicht, was praktisch bedeutet, dass der Arbeitgeber auf diese ärztlichen Unterlagen keinen Zugriff nehmen darf. Nur wenn der Dienst nicht „ärztlich" tätig geworden ist, z. B. bei arbeitsergonomischen Untersuchungen der Betriebsräume, kann der Arbeitgeber diese Unterlagen einsehen.

ren, geht insoweit fehl und vermag Missverständnisse zu erzeugen.

Bereits aus der jeweiligen gesetzlichen Zweckbestimmung der Untersuchungen selbst ergibt sich, dass die ermittelten Befunde für den Arbeitgeber irrelevant sind. Arbeitsmedizinische Untersuchungen sind spezialrechtlich geregelt und enthalten klare Regelungen zum Verbleib der ärztlichen Unterlagen: in die Verantwortung genommen wird allein und ausschließlich der Arzt. Er hat die Gesundheitsakte zu führen, in gehörige Obhut zu nehmen und ggf. an andere Ärzte oder an die Behörde - nicht jedoch an den Arbeitgeber - weiterzugeben. Er würde eine Ordnungswidrigkeit begehen, wenn er die von ihm z. B. nach StrlSchV oder RöV zu führende Gesundheitsakte nicht bis zum 75. Lebensjahr des Untersuchten aufbewahrt, diese nicht spätestens 95 Jahre nach der Geburt des Untersuchten vernichtet, oder wenn er sie nicht unverzüglich auf Anforderung des nachuntersuchenden Arztes diesem übergibt. Es zeigt sich also, dass es nicht der Arbeitgeber ist, der seine Pflichten nicht erfüllen kann, wenn er nicht über die Akten verfügt, sondern dass der Arzt über die Akten verfügen muss, um seinen gesetzlichen Pflichten nachzukommen.

Zusammenfassend ist festzustellen:

Die ärztlichen Unterlagen, die im Zusammenhang mit arbeitsmedizinischen Vorsorgeuntersuchungen angelegt werden, sind vom Arzt so zu verwahren, zur Verfügung zu halten und weiterzugeben, wie es in den betreffenden Rechtsvorschriften vorgesehen ist. Existieren für bestimmte Untersuchungsarten keine präzisen Vorgaben, ist das ärztliche Berufsrecht anzuwenden.

geber Zugriff nehmen. Wurde er jedoch gegenüber Mitarbeitern arbeitsmedizinisch tätig, unterliegt er der ärztlichen Schweigepflicht. Wenn der Betriebsarzt wechselt, verbleiben die patientenbezogenen Unterlagen gleichwohl institutionell im Betriebsärztlichen Dienst des Arbeitgebers. Sie können nicht von dem „abgehenden Arzt" mitgenommen werden. Der Arbeitgeber könnte sonst seine gesetzlichen Verpflichtungen nach dem Arbeitssicherheitsgesetz nicht mehr erfüllen. Denn die Unterlagen werden vom nachfolgenden Arzt benötigt. Die ärztliche Schweigepflicht schützt also die Mitarbeiter nach innen, institutionell handelt es sich aber um betriebliche Daten des Arbeitgebers.

Fund von Akten mit personenbezogenen Daten in einer Papiertonne

Der Hausmeister einer Berliner Wohnsiedlung teilte uns mit, dass er in einer blauen Papiertonne eine größere Menge von Akten mit personenbezogenen Daten (vorwiegend von Ärzten) gefunden habe. Das Aktenmaterial lag in losen Bündeln obenauf in der Tonne. Als personenbezogene Daten wurden vorwiegend solche von so genannten „Prüfärzten" gefunden, die im Rahmen der klinischen Forschung zur Wirksamkeit von Medikamenten an den Studien verschiedener Pharmaunternehmen beteiligt waren (Adresslisten, „Rekrutierungslisten", Einschätzungen von Ärzten hinsichtlich ihrer Geeignetheit für Studien, Honorarvereinbarungen). Patientendaten erschienen in den reichlich gefundenen Prüfberichten in (schwach) anonymisierter Form (Initialen, Geburtsdaten). Daneben fanden sich Schreiben, Faxe und E-Mails aus dem normalen Geschäftsverkehr.

Nachdem alle relevanten Akten sichergestellt waren und gerade in das Auto geladen werden sollten, kam eine junge Frau auf uns zu, die sich uns gegenüber als „Entsorgerin" der Akten offenbarte. Offenbar war sie sich ihres nicht korrekten Handelns bewusst geworden, denn sie legitimierte sich sofort und gab bereitwillig Auskunft.

Sie war gerade im Umzug begriffen und wollte die Unterlagen, die einer Freundin gehörten, entsorgen. Sie hatte der Freundin einen Gefallen erweisen wollen, die das Aktenmaterial nicht mehr benötigte, und hatte es daher mitgenommen, um es in die Papiertonne in ihrem Wohnbereich zu werfen. Ihre Freundin war in der klinischen Forschung im Auftrag von verschiedenen Pharmaunternehmen beschäftigt gewesen, war nunmehr aber bei einer anderen Firma angestellt und benötigte daher die Unterlagen, die ihre ehemaligen Auftraggeber betrafen, nicht mehr.

Die Frau wurde darauf hingewiesen, dass ihr „Freundschaftsdienst" einen Verstoß gegen datenschutzrechtliche Bestimmungen darstellte, da sie bei der Entsorgung der Daten, zu der sie wegen der Bitte der Freundin befugt war, die Vertraulichkeit der Daten nicht sicher-

gestellt hatte.

Die Akten wurden wieder an die Frau mit der Auflage zurückgegeben, ein Aktenvernichtungsunternehmen mit der datenschutzgerechten Entsorgung zu beauftragen und uns das Vernichtungszertifikat vorzulegen. Der Nachweis der ordnungsgemäßen Vernichtung wurde schließlich erbracht.

Sorgloser Umgang mit medizinischen Daten

Ein Berliner Arzt übersandte per Telefax seine ärztlichen Stellungnahmen regelmäßig an ein Berliner Kreditinstitut, bis uns das Kreditinstitut davon in Kenntnis setzte und wir an die Ärztekammer appellierten, ihre Kammermitglieder zu verstärkter Aufmerksamkeit aufzurufen. Das Kreditinstitut hatte leider eine ähnliche Telefaxnummer wie die Barmer Ersatzkasse, an die sich der Arzt eigentlich wenden wollte.

Von einer Krankenkasse wurde ein für den Medizinischen Dienst gedachtes Formular an einen Versicherten übersandt und diesem der Name, die Krankenversicherungsnummer, Geburtsdatum und Arbeitsunfähigkeit eines anderen Versicherten bekannt gegeben. Es handelte sich nach Bekundung der Krankenkasse um einen Vordruck, der ausschließlich behandelnden Ärzten versandt und durch ein EDV-gestütztes Formularsystem zugeordnet werde. Leider war das System am fraglichen Tag nicht funktionsfähig. Die für den Vorgang zuständige Mitarbeiterin habe den Vordruck kopiert, jedoch die darauf enthaltenen Daten unzureichend ausgestrichen und falsch einkuvertiert.

Ein Berliner Krankenhaus überließ die ärztliche Abrechnung einem Inkassounternehmen, vergaß aber den Patienten vorher um Zustimmung zu ersuchen. Um weiterem Ärger aus dem Wege zu gehen, verzichtete das Krankenhaus auf die Forderung; es wählte damit eine zwar kundenfreundliche, jedoch nicht ganz billige Lösung zur Beseitigung des datenschutzrechtlichen Problems. Die unzulässig übermittelten Daten wurden zurückgeholt und vernichtet.

Diese Beispiele zeigen, dass auch nach vielen Bemühungen um die Verbesserung des Datenschutzes gerade im Gesundheitswesen leichtfertig mit Gesundheitsdaten umgegangen wird, obwohl sie besonders schutzwürdig sind[83].

4.4.3 Sozial- und Jugendverwaltung

Fragen, Fragen über Fragen

Immer wieder mussten wir Fragebögen für Leistungs-

[83] vgl. 3.1

empfänger mit der Begründung bemängeln, hier würde zu viel Privates über Ausländer gefragt. Es sollten u. a. Fragen zum Reiseweg, zur Religion, zur Vermögenslage, zur Bezahlung der Reisekosten, zu beteiligten Schlepperorganisationen usw. beantwortet werden.

Die Einreisemotivation ist das entscheidende Kriterium für die Leistungsbemessung nach §§ 1 und 1 a AsylbLG. Das Oberverwaltungsgericht von Berlin verlangt eine „substanziierte und substanzreiche" Schilderung der Einreiseumstände, also eine ausführliche, natürlich wahrheitsgemäße Schilderung der Reiseumstände, die in sich schlüssig zu sein hat und den wirklichen Lebensumständen entsprechen muss. Die Fragebögen hatten jedoch den gravierenden Mangel, dass sie diese Anforderungen nicht hinreichend deutlich herausstellten und keinen Hinweis auf die Rechtsgrundlagen enthielten, aufgrund derer die Fragen gestellt werden. Deshalb blieb der Sinn vieler Fragen oft unverständlich und erregte bei den Helferorganisationen Unwillen und Unverständnis. Diesem Mangel wurde mit einem Formulierungsvorschlag abgeholfen, der die Rechtsgrundlage und die Bedeutung der Fragen besser vermittelt.

Spätwirkungen von Misshandlungstraumata

Eine mittlerweile volljährige Petentin schrieb: „Schon im Kleinkindalter wurde ich sexuell missbraucht, was sich später im Alter von 13 Jahren mit der ersten Vergewaltigung fortsetzte; ein solcher ‚Faden' zieht sich durch das ganze Leben." Aufgrund dieser Geschehnisse sei sie psychotherapeutisch behandlungsbedürftig und benötige eine Kostenübernahme. Sie habe eine multiple Persönlichkeitsstörung und befinde sich therapeutisch in einem akuten Stadium. Zur Kostenübernahme und auch für ein Gelingen der persönlichen Verarbeitung ihres früheren Leidensweges möchte sie in die Dokumentation des Jugendamts während ihrer Kindheit zu diesen Vorfällen Einsicht nehmen. Die Nachfrage bei ihrem Jugendamt ergab, dass die Akten bereits vernichtet waren. Die Petentin bittet um Prüfung der Aufbewahrungsfristen.

Die Aufbewahrungsfristen für Akten des *Jugendamts* sind in Ausführungsvorschriften[84] geregelt. Nach diesen Vorschriften beginnt die Aufbewahrungsfrist mit dem Jahr, das auf das Jahr folgt, in dem der Minderjährige volljährig geworden ist. Bei Akten mit Geldverkehr beträgt die Aufbewahrungsfrist zehn Jahre, ohne Geldverkehr fünf Jahre. Unter dem Begriff Geldverkehr werden Einnahmen und Ausgaben hinsichtlich des Unterhaltsanspruchs des Kindes verstanden. Erheblich längere Aufbewahrungsfristen – 30 Jahre – gibt es nur, sofern die Vermögenssorge dem Jugendamt übertragen So bedauerlich es für die Petentin auch ist, dass ihr die Unterlagen durch das Jugendamt nicht mehr vorgelegt werden konnten, müssen Altakten, die nicht von besonderem Interesse sind und deshalb dem Landesarchiv zur Verfügung zu stellen sind, nach angemessener Frist vernichtet werden. Die in der AV Vorm geregelten Fristen haben sich bewährt. Auch eine Vereinheitlichung der Frist auf zehn Jahre ab Volljährigkeit hätte im vorliegenden Fall, in dem die Vernichtung erst nach 23 Jahren durchgeführt worden ist, den Sachverhalt nicht im Sinne der Petentin positiv verändert."

[84] Ausführungsvorschriften für Vormundschaften, Pflegschaften, Beistandschaften für Kinder und Jugendliche – Vormundschaftsvorschriften (AV Vorm) vom 18. September 1989, Dienstblatt IV Nr. 1, S. 8

worden war oder das Jugendamt das Kind im Adoptionsverfahren gesetzlich vertreten hat.

Das Jugendamt hat zwar eingeräumt, dass ein Mitarbeiter als Pfleger für die Petentin bestellt war. Jedoch war der Wirkungskreis dieser Pflegschaft nicht auf den Geldverkehr bezogen. Deshalb hätten in diesem Fall entsprechend den Ausführungsvorschriften die Unterlagen im Jahre 1982 vernichtet werden können; ausweislich des Mündelregisters wurden sie im Jahre 2000 vernichtet. Das Jugendamt war sehr bemüht, die vorhandenen Möglichkeiten einer Einsichtsnahme in frühere Unterlagen zu unterstützen. Es sei jedoch davon auszugehen, dass Akten des Sozialpädagogischen Dienstes, des Pflegekinderwesens oder über frühere Heimpflege nicht mehr vorhanden seien, denn es gäbe keine landeseinheitlichen Regelungen zur Aufbewahrungsfrist sozialpädago-gischer Betreuungsunterlagen.

Dies wurde auch in einer interdisziplinären Arbeitsgruppe erörtert, in der engagierte Mitarbeiterinnen und Mitarbeiter der Berliner Verwaltung und freier Träger zur Verbesserung des Schutzes von gefährdeten Kindern vor sexuellem Missbrauch und Misshandlung zusammenarbeiten (Kindernotdienst, Jugendamt, Polizei, Staatsanwaltschaft, schulpsychologischer Dienst, Wildwasser, Landesjugendamt und der Sozial- und Gesundheitsreferent unserer Behörde). Dort wurde eine fachlich und therapeutisch gut fundierte Regelung der Aufbewahrungsfristen von derartigen Betreuungsunterlagen für dringend erforderlich gehalten.

Das besondere Interesse dieser Arbeitsgruppe gilt den datenschutzrechtlichen Fragestellungen bei Kindesmisshandlung und Missbrauch. Sie erarbeitet einen Leitfaden für Praktiker, der vom Landesjugendamt den einschlägigen Einrichtungen zur Verbesserung ihrer Arbeitsweise zur Verfügung gestellt werden soll. Wir haben unter unserer datenschutzrechtlichen Aufgabenstellung mitgearbeitet und unterstützen das Vorhaben, um Verunsicherungen durch das Datenschutzrecht mit Aufklärung zu begegnen.

Geldeintreibung als Auftragsdatenverarbeitung im Sozialbereich?

Eine Berliner Rechtsanwaltsfirma bot diversen Sozialstadträten Berliner Bezirke die Übernahme von Dienstleistungen an, die in den Sozialämtern viele Mitarbeiter mit Arbeiten binden, die außerhalb ihres eigentlichen Aufgabenbereichs liegen und die als lästige „Kiepen-Arbeit" empfunden werden. Dabei handelt es sich um die Einziehung von Geldansprüchen der Sozial- und Jugendämter (z. B. Einziehung übergegangener Ansprüche nach dem Bundessozialhilfegesetz, Vorauszahlungen auf Kindesunterhalt). Eventuellen datenschutzrechtlichen Bedenken gegen die für dieses Outsourcing erforderliche Bereitstellung der personenbezogenen Sozialdaten glaubte die Firma dadurch entkräften zu können, dass sie die Tätigkeit als Datenver-

Bei der Geltendmachung und Durchsetzung von Unterhaltsansprüchen nach dem BSHG handelt es sich um eine hoheitliche Aufgabe, welche nicht im Wege der Auftragsvergabe nach § 80 SGB X vollständig an Rechtsanwaltskanzleien übertragen werden kann. Vielmehr handelt es sich hierbei um eine klare Aufgabenübertragung, welche - neben den datenschutzrechtlichen Aspekten - auch aus anderen rechtlichen Gründen für bedenklich gehalten wird. Materiell-rechtliche Entscheidungen über eine Inanspruchnahme zu Unterhaltsleistungen (z.B. Härtefallprüfungen) sind durch den Träger der Sozialhilfe zu treffen. Denkbar ist es jedoch - wie bereits auch in der Vergangenheit üblich - einzelne Umsetzungsakte, wie z.B. die Prozessführung,

arbeitung im Auftrag einordnete, so dass keine Übermittlung der Daten im rechtlichen Sinne vorläge.

Die Leistungsbeschreibung der *Rechtsanwaltsfirma* ging weit über darüber hinaus, was unter Datenverarbeitung im Auftrag nach § 80 SGB X verstanden werden kann. Datenverarbeitung im Auftrag liegt nur dann vor, wenn sich der Auftrag auf die Erhebung, Verarbeitung (= Speichern, Verändern, Übermitteln, Sperren und Löschen) und Nutzung von Daten beschränkt (§§ 80 Abs. 1 Satz 1 i. V. m. 67 Abs. 5-7 SGB X). Dies darf ein privater Auftragnehmer nach § 11 Abs. 3 BDSG nur im Rahmen der Weisungen des Auftraggebers tun. Die datenschutzrechtliche Verantwortung für die Verarbeitung bleibt im vollen Umfang beim Auftraggeber.

Die Leistungsbeschreibung sah jedoch nach Übergabe der Leistungsakte die Erstellung von Auskunftsersuchen, die Androhung und Festsetzung von Zwangsmitteln, die Erstellung von Bescheiden, die Überwachung des Zahlungsverkehrs, die Bearbeitung von Widersprüchen, die Anordnung der sofortigen Vollziehung, die Durchsetzung von Forderungen, die Bearbeitung von Stundungen, die Führung des verwaltungsgerichtlichen Schriftverkehrs und vieles andere mehr vor. Hier bestehen also auch außerhalb der Phasen der Erhebung, Verarbeitung und Nutzung von Daten Entscheidungsbefugnisse und weisungsunabhängige Sachentscheidungskompetenzen, für die auch der juristische Sachverstand eingebracht wird. Der Auftrag betrifft also nicht die Datenverarbeitung im engeren Sinne, sondern das Inkasso von finanziellen Ansprüchen der Sozialbehörde in umfassender Form. Die in diesem Rahmen stattfindende Datenverarbeitung dient diesem Zweck und erfolgt damit unter eigener datenschutzrechtlicher Verantwortung der Auftragnehmers.

Sofern die Firma personenbezogene Sozialdaten des Sozialamtes erhalten würde, würde dies daher nicht im Rahmen der Bereitstellung für eine Auftrags*daten*verarbeitung erfolgen, sondern zur Durchführung einer darüber hinausgehenden Aufgabe im Rahmen einer Aufgabenübertragung. Es handelt sich daher um eine Datenübermittlung, die nach § 67 d SGB X nur zulässig ist, soweit eine gesetzliche Übermittlungsbefugnis nach §§ 68 bis 77 SGB X oder nach einer anderen Rechtsvorschrift im SGB vorliegt.

Da wir eine solche Rechtsgrundlage für die Übermittlung an die Rechtsanwaltsfirma nicht erkennen konnten, rieten wir von dieser Form des Outsourcings ab.

Sozialdaten – Steht die technische Sicherheit noch auf einer guten BASIS?

Das 1994 auf der Grundlage der Standardsoftware ProSOZ eingeführte IT-Verfahren *BASIS I* wird in unterschiedlichen Varianten seit vielen Jahren für die Bearbeitung von Sozial- und Jugendhilfeangelegenhei-

im Wege des Outsourcing durch Rechtsanwaltskanzleien erledigen zu lassen.

ten in den Bezirken und dem Landesamt für Gesundheit und Soziales eingesetzt und hat inzwischen diverse Versionen erlebt. Wir haben uns in unseren Jahresberichten wiederholt zu dem Verfahren geäußert. Die in der Einführungsphase für die Sicherheit der damaligen Versionen des Verfahrens vorgesehene Konzeption haben wir akzeptiert.

Bereits im Jahresbericht 1999[85] haben wir über das Ergebnis von Kontrollen in den Bezirken im laufenden Echtbetrieb berichtet, bei denen erhebliche Sicherheitsmängel festgestellt wurden. Die Mängel waren auf die unzureichende Umsetzung der von der Basis-Geschäftsstelle herausgegebenen Anweisungen zur Wahrung der IT-Sicherheit des Verfahrens zurückzuführen.

Mittlerweile haben sich die Rahmenbedingen für den Einsatz des Verfahrens gewandelt. Bei den Kontrollen zeichnete sich die Entwicklung dahin ab, dass das veraltete Betriebssystem MS-DOS, mit dem noch keine parallele Abarbeitung vom Programmcode (Multitasking) möglich war, durch Betriebssysteme mit graphischen Benutzeroberflächen (Windows 3.x) abgelöst wurde. Inzwischen ist der Einsatz von graphisch orientierten 32-Bit-Betriebssystemen (Windows NT 4) auch bei BASIS I fast obligatorisch.

Mit der Einführung neuer Betriebssysteme entstanden aber auch neue Risiken, die bei der ursprünglichen Sicherheitskonzeption noch nicht bedacht werden konnten. 1999 zeichnete sich ab, dass die Änderung des systemtechnischen Unterbaus erhebliche Mängel in der Sicherheit nach sich zog.

Die gravierendste Schwachstelle des Verfahrens ermöglicht jedem Mitarbeiter, der Zugriff auf BASIS hat, die Einsichtnahme und Manipulation von Daten, die nicht in seinem Zuständigkeitsbereich liegen. In einer so genannten 16-Bit-Umgebung (MS-DOS in Verbindung mit Windows 3.x) konnten noch technische Maßnahmen getroffen werden, die einen solchen Zugriff unterbinden können. Für den Einsatz von 32-Bit-Betriebssystemen fehlt ein zufriedenstellender Lösungsansatz.

Unseren Bedenken wurde mit dem Argument begegnet, dass eine Umstellung auf 32-Bit-Systeme nur im Zusammenhang mit der Ablösung des Verfahrens BASIS I durch das zu diesem Zeitpunkt noch in Entwicklung befindliche Projekt BASIS 3000 (BASIS II) erfolgen würde. Bei BASIS 3000 sollte es sich um ein Verfahren auf Grundlage einer Client-Server-Architektur handeln. In einer solchen Architektur stellt der Rechner des Sachbearbeiters (Client) Anfragen an einen Server und erhält nach erfolgter Berechtigungsprüfung Antworten. Ein direkter Zugriff auf die Daten durch den

[85] JB 1999, 4.4.3

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Nutzer ist nicht notwendig und kann somit auch unterbunden werden. Das auf dem Client eingesetzte Betriebssystem ist eher nebensächlich. Es bedarf nur eines so genannten Frontend-Programms, das Anfragen an den Server schickt und die entsprechenden Antworten für den Nutzer aufbereitet. Der Vorteil aus sicherheitstechnischer Sicht ist die speziell definierte Schnittstelle, die die Kontrolle der Kommunikation von und zum Server vereinfacht.

Nach dem Scheitern des Projekts BASIS 3000 wurde kurzfristig nach einer neuen Lösung gesucht, weil die technische Unterstützung für das inzwischen veraltete Betriebssystem MS-DOS und das Verfahren selbst durch die jeweiligen Hersteller eingestellt werden sollte. Als Zwischenlösung, die bis zur Entwicklung eines Nachfolgeverfahrens eingesetzt werden soll, wurde das Programm ProSOZ für Windows eingeführt. Hierbei handelt es sich um eine Weiterentwicklung des alten Programms ProSOZ für DOS für das 16-Bit-Betriebssystem Windows 3.x. Aus sicherheitstechnischer Sicht wurde lediglich die Oberflächengestaltung modernisiert. Die Kernstruktur des Programms wurde nicht geändert, so dass die Sicherheitsprobleme der alten DOS-Version in diesem Fall fortbestehen, jedoch wie auch bei DOS durch technische Maßnahmen neutralisiert werden können.

Da inzwischen auch die technische Unterstützung für Windows 3.x ausläuft und auf 32-Bit-Betriebsysteme umgestellt werden muss, wurde mittlerweile eine entsprechende Version von ProSOZ entwickelt. Aber auch hier ist bei der Weiterentwicklung der ursprüngliche Programmkern verwendet worden, so dass die Sicherheitsprobleme weiter Bestand haben. Unter Windows NT 4 können diese Probleme aber nicht mehr mit technischen Maßnahmen entschärft werden.

Die Umgehung des Problems durch den Verzicht auf den Einsatz von 32-Bit-Technologie ist jetzt nicht mehr möglich. Spätestens jetzt ist wichtig und seit der Novellierung des Berliner Datenschutzgesetzes von 2001 auch durch § 5 Abs. 3 gesetzlich vorgeschrieben, das Sicherheitskonzept für BASIS I an die neuen Gegebenheiten anzupassen bzw. neu zu entwickeln.

Die Bedenken des Berliner Beauftragten für Datenschutz und Informationsfreiheit zur Sicherheit von PROSOZ/S für Windows werden von der zuständigen Senatsverwaltung für Gesundheit, Soziales und Verbraucherschutz geteilt. Diese hat daher bereits im vergangenen Jahr die BASIS-Geschäftsstelle aufgefordert gemeinsam mit den Bezirksämtern die lokalen Sicherheitskonzepte weiterzuentwickeln. Mit der Umstellung auf PROSOZ/S für Windows, insbesondere in der 32-bit-Version, haben nunmehr die Bezirksämter eine aktuelle Risikoanalyse und ein Sicherheitskonzept in Auftrag gegeben. Diese Risikoanalyse und das Sicherheitskonzept werden auch maßgeblich die Anforderungen bestimmen, die bei einem Vergabeverfahren für ein modernes Sozialhilfesoftwaresystem für das Land Berlin zu stellen sind. Die BASIS-Geschäftsstelle beauftragte am 18. Dezember 2002 im Einvernehmen mit den Amtsleitern Soziales der Bezirksämter den LIT mit der Durchführung eines entsprechenden Projektes. Nach der Projektplanung wird das neue Sicherheitskonzept noch in diesem Jahr umgesetzt.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Wird es versäumt, die technische Sicherheit auf den gebotenen Stand zu heben, drohen erhebliche Risiken für die Vertraulichkeit, Integrität und Verfügbarkeit für die in BASIS I zu verarbeitenden Daten, die als Sozialdaten einen besonderen Schutz der Vertraulichkeit und als Grundlage für finanzielle Leistungen in Milliardenhöhe auch besonderen Schutz der Integrität beanspruchen.

Es ist daher wichtig, die bevorstehende Umstellung nicht im „Hauruckverfahren" nur unter dem Aspekt der allgemeinen Praxistauglichkeit durchzuführen, sondern der Verfahrenssicherheit den Stellenwert einzuräumen, der beim Umgang mit solchen Sozialdaten notwendig und gesetzlich vorgeschrieben ist.

4.4.4 Bauen, Wohnen und Umwelt

Zweckentfremdung von Wohnraum

Mit Urteil vom 13. Juni 2002 hat das Oberverwaltungsgericht Berlin ein Zweckentfremdungsverbot von Wohnraum in Berlin aus verfassungsrechtlichen Gründen abgelehnt und die entsprechende Zweckentfremdungsverbot-Verordnung rückwirkend (ab 1. September 2000) außer Kraft gesetzt. Das Land Berlin hat gegen diese Entscheidung Rechtsmittel eingelegt. Mit einer abschließenden Entscheidung des Bundesverwaltungsgerichtes ist im Frühjahr 2003 zu rechnen.-

Sollte die Entscheidung des Oberverwaltungsgerichtes Berlin rechtskräftig werden, hätte dies zur Folge, dass die *Zweckentfremdungsverbot*-Verordnung aufzuheben wäre. Wir haben die Senatsverwaltung für Stadtentwicklung vor diesem Hintergrund darauf hingewiesen, dass nach § 9 Abs. 1 BlnDSG die Verarbeitung von personenbezogenen Daten nur zulässig ist, wenn sie zur Erfüllung der durch Gesetz der Daten verarbeitenden Stelle zugewiesenen Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist. Eine derartige Erforderlichkeit ist – angesichts des Urteils des Oberverwaltungsgerichtes Berlin – für die Verarbeitung von personenbezogenen Daten zur Bekämpfung der Zweckentfremdung von Wohnraum derzeit nicht mehr gegeben.

Die Senatsverwaltung für Stadtentwicklung hat entsprechend reagiert und in Abstimmung mit den Bezirken veranlasst, dass bis auf weiteres alle entsprechenden Antragsverfahren bei den bezirklichen Wohnungsämtern ruhen und bei bestandskräftigen Bescheiden ab 1. Juli 2002 die Einziehung der festgesetzten Ausgleichszahlungen ausgesetzt wird.

Inzwischen hat das Bundesverwaltungsgericht die Beschwerde gegen die Nichtzulassung der Revision gegen die Urteile des OVG vom 13. Juni 2002 zurückgewiesen. Damit ist die Entscheidung des OVG Berlin rechtskräftig, wonach die 2. Zweckentfremdungsverbot-Verordnung (2. ZwVbVO) automatisch zum 1. September 2000 außer Kraft getreten ist.

Da es sich bei der Entscheidung um eine „Indizienentscheidung" im Rahmen von fünf Einzelfällen handelt, die noch keine Allgemeinverbindlichkeit entfaltet, müssen nunmehr

- das Zweckentfremdungsbeseitigungsgesetz vom 8. März 1990 (GVBl. S. 627)

sowie auch

– die 2. Zweckentfremdungsverbot-Verordnung vom 15. März 1994 (GVBl. S. 91), zuletzt geändert durch Verordnung vom 6. November 2001 (GVBl. S. 581)

–

aufgehoben werden.

Trotz der nunmehr anstehenden Aufhebung des Zweckentfremdungsbeseitigungsgesetzes sowie auch der 2. Zweckentfremdungsverbot-Verordnung sind zur Abwicklung anhängiger Fälle (z. B.: Einstellung von

ruhenden Verfahren oder Zahlungsvorgängen, Antragstellungen von bisher vom Zweckentfremdungsverbot Betroffener) von den Wohnungsämtern bisher erfasste Daten bis zum endgültigen Abschluss der Verfahren zu verwenden.

Der abwesende Hauswart

Ein Mieter beschwerte sich bei seiner Wohnungsbaugesellschaft darüber, dass er mehrfach vergeblich versucht habe, den für seinen Wohnblock zuständigen Hauswart zu erreichen. Er habe daher darum gebeten, dass ihm die Abwesenheitszeiten des Hauswartes vom Vermieter mitgeteilt werden. Dieser habe die Auskünfte unter Hinweis auf den Datenschutz verweigert.

Die Übermittlung derartiger Daten durch die Wohnungsbaugesellschaft an Dritte ist nur zulässig, soweit es zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat (§ 28 Abs. 3 Nr. 1 BDSG).

Die Tätigkeit eines Hauswartes besteht darin, die Funktionsfähigkeit der gemieteten Wohnung zu kontrollieren und gegebenenfalls durch kleinere Reparaturen bzw. Dienstleistungen wiederherzustellen. Als Vertreter des Vermieters ist er Ansprechpartner für den Mieter, um Beeinträchtigungen der Mietsache selbst auszuräumen bzw. dies zu veranlassen. Insofern hat der Mieter ein berechtigtes Interesse daran, die Abwesenheitszeiten des Hauswartes bzw. die Zeiten, in denen dieser durch einen Dritten vertreten wird, zu erfahren. Das berechtigte Interesse des Mieters erstreckt sich jedoch in keinem Fall auch auf die Gründe für eine Abwesenheit (z. B. wegen Urlaub, Krankheit) des Hauswartes. Aufgrund der vertraglichen Verpflichtungen, die der Hauswart gegenüber seinem Arbeitgeber eingegangen ist, kann er kein schutzwürdiges Interesse am Ausschluss der Übermittlung der Abwesenheitszeiten haben.

Auch wenn die datenschutzrechtlichen Bestimmungen einer Übermittlung von Daten über die Abwesenheit des Hauswartes an den Mieter durch den Vermieter damit nicht entgegenstehen, lässt sich daraus jedoch kein Anspruch des Mieters auf eine derartige Datenübermittlung ableiten.

Wohnungsangebot im Internet

Ein Mieter, der seine Mietwohnung fristgerecht gekündigt hatte, beschwerte sich darüber, dass ein Makler seinen Namen und seine Telefonnummer zur Vermittlung seiner Mietwohnung an einen Nachmieter auf seiner Website im Internet veröffentlicht habe. Eine Überprüfung der Website ergab, dass der Makler über das Internet eine Vielzahl von Wohnungen in Berlin

anbietet. Neben den Daten über die Wohnung (Adresse, Ausstattung, Miethöhe usw.) waren bei noch bewohnten Objekten jeweils auch – zur Kontaktaufnahme – der Name und die Telefonnummer der (Noch-)Mieter angeben.

Der *Makler* speichert als verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG die personenbezogenen Daten der Mieter auf einem mit dem Internet verbundenen Server. Er hält die Daten zum Abruf bereit bzw. lässt dies im Auftrag tun. Bei jedem Abruf werden die entsprechenden Daten an die abrufende Stelle übermittelt (§ 3 Abs. 4 Ziff. 3 b BDSG). Die Übermittlung von personenbezogenen (Mieter-)Daten zu eigenen Geschäftszwecken ist nur zulässig, soweit es zu Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Datenverarbeitung überwiegt (§ 28 Abs. 1 Nr. 2 BDSG). Ob die Übermittlung der Mieterdaten zur Wahrung der berechtigten Interessen des Maklers überhaupt erforderlich ist, kann dahinstehen, da hier in jedem Fall die schutzwürdigen Interessen der betroffenen Mieter am Ausschluss der Übermittlung überwiegen.

Der Makler hat bestätigt, dass er unserer Aufforderung, die Mieterdaten zukünftig nur mit deren Einwilligung auf seiner Website zu veröffentlichen, nachkommen wird.

Veröffentlichung der Standortangaben von Mobilfunkanlagen

Die Speicherung und die Veröffentlichung der Standortdaten von Mobilfunkanlagen durch öffentliche Stellen stehen zurzeit in verstärktem Maße in der öffentlichen Diskussion. Da die Standortdaten sowohl Angaben zur Straße als auch zur Hausnummer enthalten und diese Daten auch Grundstücke betreffen, die eigentumsrechtlich natürlichen Personen zuzuordnen sind, ist davon auszugehen, dass es sich um personenbezogene Daten im Sinne des § 4 Abs. 1 BlnDSG handelt. Diese Daten dürfen nach § 13 BlnDSG nur an private Personen oder Stellen übermittelt (veröffentlicht) werden, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene darin eingewilligt hat.

Eine Rechtsgrundlage existiert nicht. Der Mobilfunk unterfällt hinsichtlich der Strahlenbelastung dem Bundesimmissionsschutzgesetz. Weder dieses Gesetz noch eine andere Rechtsgrundlage sieht ein besonderes Kataster für die Standortdaten von Mobilfunkanlagen vor. Insofern ist bereits fragwürdig, ob ein derartiges Kataster durch die in Berlin zuständigen Umweltämter überhaupt erstellt werden darf. Eine Veröffentlichung dieser Daten ist mangels Rechtsgrundlage in jedem Fall unzulässig.

Unabhängig davon stellt sich die Frage, ob die Stand-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

ortdaten öffentlich gemacht werden dürfen. Nach § 7 der 26. Bundesimmissionsschutzverordnung sind die Betreiber von Hochfrequenzanlagen sowie bestimmter Niederfrequenzanlagen verpflichtet, den Betrieb dieser Anlagen gegenüber den in Berlin zuständigen Umweltämtern in den Bezirken anzuzeigen. Unbestritten handelt es sich bei diesen Angaben um umweltrelevante Daten, die nach § 4 Abs. 1 Umweltinformationsgesetz (UIG) grundsätzlich jedermann – auf Antrag – zugänglich zu machen sind. Einschränkungen ergeben sich jedoch aus § 8 Abs. 1 Nr. 1 und § 8 Abs. 2 Satz 1 UIG bei personenbezogenen Daten. Sind – wie im vorliegenden Fall – personenbezogene Daten von dem Informationsbegehren betroffen, besteht dann kein Zugang zu diesen Informationen, wenn durch das Bekanntwerden schutzwürdige Interessen der Betroffenen beeinträchtigt werden. Eine solche Beeinträchtigung ist hier nicht ausgeschlossen, da zu befürchten ist, dass Mobilfunkgegner Druck auf die Grundstückseigentümer ausüben könnten.

Der Wunsch nach Veröffentlichung der Standortangaben von Mobilfunksendeanlagen durch die Bezirksämter in Berlin war schon Anlass einer Kleinen –Anfrage und eines Antrags aus dem Abgeordnetenhaus.

Der Senat begrüßt und unterstützt die Anregung der Datenschutzbeauftragten des Bundes und der Länder, für die Veröffentlichung der Standortangaben von Mobilfunksendeanlagen eine immissionsschutzrechtliche Grundlage zu schaffen.

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 64. Konferenz am 24./25. Oktober 2002 den Bundesgesetzgeber aufgefordert, im Rahmen einer immissionsschutzrechtlichen Regelung über die Erstellung von Mobilfunkkatastern zu entscheiden[86].

Die von den Datenschutzbeauftragten des Bundes und der Länder auf ihrer 64. Konferenz vorgenommene Aufforderung an den Bundesgesetzgeber erfolgte im Rahmen einer dort erarbeiteten Entschließung „Speicherung und Veröffentlichung von Mobilfunkantennen“.

Die Ausführungen in dieser Entschließung stimmen inhaltlich im Wesentlichen mit den Ausführungen des Berliner Beauftragten für Datenschutz und Informationsfreiheit im vorgelegten Tätigkeitsbericht überein; darüber hinaus enthält sie die Forderung nach konkreteren Bestimmungen darüber, wie derartige Kataster erstellt werden sollen und bezüglich der Frage, ob und unter welchen Bedingungen eine Veröffentlichung derartiger Kataster im Internet oder in vergleichbaren Medien zulässig ist.

Das Bundesumweltministerium hat die Anregung der Datenschutzbeauftragten des Bundes und der Länder aufgegriffen und prüft derzeit die Möglichkeit einer Umsetzung. Ein Ergebnis liegt noch nicht vor..

Übermittlung von Gewerbedaten zur Abfallentsorgung

Nach der am 1. Januar 2003 in Kraft getretenen *Gewerbeabfallverordnung* (GewAbfV) haben die Erzeuger und Besitzer von gewerblichen Siedlungsabfällen zukünftig Abfallbehälter des öffentlich-rechtlichen Entsorgungsträgers in angemessenem Umfang nach den näheren Festlegungen des öffentlich-rechtlichen Entsorgungsträgers zu nutzen (§ 7 Satz 4 GewAbfV).

Im Land Berlin nehmen die Berliner Stadtreinigungs-

– Nach abschließender Klärung des Vorgangs durch das zuständige Gewerbereferat des Senats wurde festgestellt, dass sich die BSR bei der Umsetzung der Gewerbeabfallverordnung nicht hoheitlich betätigen, sondern sich entgegen der ursprünglichen Annahme im Wettbewerb befinden.

–

– Demnach wäre eine Übermittlung der drei soge-

[86] : Entschließung zur Speicherung und Veröffentlichung der Standortverzeichnisse von Mobilfunkantennen, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2002”, S. 27

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

betriebe die Aufgaben des öffentlich-rechtlichen Entsorgungsträgers wahr (§ 5 Abs. 1 Satz 2 des Gesetzes zur Förderung der Kreislaufwirtschaft und Sicherung der umweltverträglichen Beseitigung von Abfällen in Berlin (Kreislaufwirtschafts- und Abfallgesetz Berlin – KrW-/AbfG Bln)).

Um alle durch die neue Verordnung verpflichteten Gewerbebetriebe anschreiben und über die neue Verordnung informieren zu können und um nach In-Kraft-Treten der Verordnung Zuwiderhandlungen gegen die Verordnung ahnden zu können, fordert die BSR von den Gewerbeämtern die Übermittlung von Namen, betrieblicher Anschrift und angezeigter Tätigkeit des Gewerbetreibenden. Wir haben der Senatsverwaltung für Wirtschaft auf Nachfrage mitgeteilt, dass die von der BSR gewünschte Datenübermittlung wegen Fehlens einer Rechtsgrundlage rechtswidrig ist.

§ 14 Abs. 1 Satz 4 Gewerbeordnung (GewO) scheidet als Rechtsgrundlage für die Datenübermittlung aus, da das Aufstellen eines Abfallbehälters und die Einhaltung der Gewerbeabfallverordnung noch nicht als Gewerbeaufsicht im engeren Sinne zu verstehen sind, sich vielmehr an der Peripherie sonstiger Verpflichtungen von Gewerbetreibenden bewegen. Öffentlichen Stellen, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, und nicht-öffentlichen Stellen dürfen die Gewerbeämter bei berechtigtem Interesse der Stelle Gewerbedaten übermitteln. Als öffentlich-rechtlicher Entsorgungsträger nimmt die BSR jedenfalls bei der Umsetzung der Verpflichtungen aus der Gewerbeabfallverordnung nicht am Wettbewerb teil, so dass § 14 Abs. 8 GewO als Rechtsgrundlage ausscheidet. Für öffentliche Stellen, die nicht am Wettbewerb teilnehmen, sieht das Gesetz zur Erfüllung der in ihre Zuständigkeit fallenden Aufgaben nur eine fallweise Datenübermittlung vor. Die Übermittlung der Daten sämtlicher Gewerbetreibender, wie sie von der BSR gefordert wird, kann nicht mehr unter dem Begriff „fallweise" subsumiert werden, die Übermittlung muss sich auf Einzelfälle oder bestimmte Fallgruppen beziehen[87].

§ 14 Abs. 9 GewO gestattet zwar eine Übermittlung von Gewerbedaten für andere Zwecke, soweit eine

nannten gewerberechtlichen Grunddaten (Firmenname, Anschrift und Geschäftsgegenstand) nach § 14 Abs. 8 GewO an die BSR nur unter denselben Bedingungen möglich, wie sie für alle anderen privatwirtschaftlich tätigen Unternehmen auch gelten, insbesondere gegen Zahlung der für die Einzelauskunft festgelegten Gebühr.

–

– Das Ergebnis dieser Feststellungen wurde den BSR mit Schreiben vom 18.03.2003 mitgeteilt, der BlnBDI hat eine Kopie des Schreibens erhalten.

–

Es ist davon auszugehen, dass die BSR in Anbetracht der durch die zu entrichtenden Gebühren entstehenden außerordentlich hohen Kosten davon absehen werden, die Gewerbedaten anzufordern.

[87] vgl. von Landmann, Robert; Rohmer, Gustav: Gewerbeordnung und ergänzende Vorschriften, Bd. 1. München: C. H. Beck, Stand: 1. Juli 2002, § 14, Rdn. 80

besondere Rechtsvorschrift dies vorsieht, für die von der BSR gewünschte Datenübermittlung ist aber keine besondere Rechtsvorschrift ersichtlich. So gestatten zwar sowohl § 2 Berliner Betriebedatenverordnung als auch § 25 Abs. 7 KrW-/AbfG Bln die Erhebung und Speicherung von personenbezogenen Daten, eine Datenübermittlungsvorschrift, die die Datenübermittlung durch die Gewerbeämter gestattet, enthalten diese Rechtsvorschriften aber nicht.

4.5 Wissen und Bildung

4.5.1 Wissenschaft und Forschung

Datenschutzgerechte Forschung

Wie in den vergangenen Jahresberichten wollen wir wieder eine Auswahl von *Forschungsprojekten* kurz vorstellen, für die es mit zum Teil erheblichem Beratungsaufwand gelang, einen optimalen Datenzugang für die Forscher zu ermöglichen und zugleich die Rechte der Betroffenen auf informationelle Selbstbestimmung zu wahren. Im Zentrum der Beratung stand dabei die Freiwilligkeit bei Befragungen, die frühestmögliche Anonymisierung und, insbesondere bei Längsschnittstudien und dem Aufbau von Forschungsregistern, die Pseudonymisierung der personenbezogenen Daten.

Von Forschern befragt wurden u. a.:

- Schüler, Eltern und Lehrer im Rahmen des Feldtests für die internationale Schulvergleichsuntersuchung PISA 2003,

- Schüler von 5., 7. und 9. Klassen im Rahmen einer internationalen Vergleichsstudie zum Gesundheitsverhalten,

- Frauen und Männer zum Zusammenhang von Kortisoneinnahmen und Osteoporose,

- Strafgefangene sowie eine Kontrollgruppe zu „Werten in unserer Gesellschaft",

- Jugendliche zu Verzehrmengen ausgewählter Lebensmittelgruppen zur Abschätzung der Acrylamid-Aufnahme,

- jugendliche nicht deutsche Straftäter zu Sozialisationsproblemen in Deutschland,

- Schüler und Lehrer in einer Längsschnittuntersuchung zur Evaluation des mathematisch-naturwissenschaftlichen Unterrichts,

- Jugendliche zur Nutzung wohnortnaher Jugendeinrichtungen,

- Kinder im Grundschulalter zur Ernährungs-/Fehlernährungssituation,

- jugendliche Gewalttäter zu Gewalterfahrungen,

- türkische und arabische Jugendliche über ihre Einstellungen zur gegebenenfalls eigenen sowie gegenüber fremden Religionen,

- Mieter zur Fortschreibung der Mietobergrenzen in Sanierungsgebieten,

- Schüler zum Einfluss von Freunden, Eltern und der Schule auf die Berufswahl,

- afghanische Emigrantinnen und Emigranten zum Unterstützungspotenzial für eine Rückkehr,

- Bewohner eines Bezirks zu Möglichkeiten und Nutzung der Mülltrennung,

- Stadtplaner zum landschaftsgestalterischen Umgang mit dem ehemaligen Mauerstreifen,

- Schüler, deren Eltern und Großeltern zur Entwicklung von Vertrauen und Misstrauen in politische Institutionen und gegenüber anderen Menschen,

- Schüler und Eltern zu ihrer Eigeneinschätzung im Vergleich zur Fremdwahrnehmung,

- Strafgefangene nach Suizidversuchen,

- Frauen zu körperlichen und sexuellen Gewalterfahrungen,

- BVV-Mitglieder zu gesundheitspolitischen Fragen,

- Schüler und Lehrer zu Lernschwierigkeiten,

- HIV-infizierte Frauen zur aktuellen Lebens- und Gesundheitssituation,

- Auszubildende des Baugewerbes zu politischen Vorurteilen gegenüber Ausländern,

- Mieter und Vermieter für den neuen Berliner Mietspiegel 2002.

Akteneinsicht nahmen Forscher in

- Studienprotokolle zur retrospektiven Analyse von Behandlungen nach schwerem Polytrauma,

- Bundeszentralregisterauszüge zur Überprü-

fung von Prognosemethoden bei Rechtsbrechern mit gravierender Gewaltkriminalität,

- Erfahrungsberichte deutscher Fremdsprachenassistenten im Ausland,
- Narkoseprotokolle zum Einfluss von Blutdruckmedikamenten,
- Strafakten zur Auswahl von zu Befragenden für eine Differenzialanalyse von Sexualstraftätern,
- Generalakten der Justiz der 60er Jahre zum Missbrauch von Rauschgiften,
- Unterlagen des Amtes zur Regelung offener Vermögensfragen zur Analyse der Entwicklung der Eigentumsverhältnisse an Grundstücken im 20. Jahrhundert in Berlin-Mitte.

Darüber hinaus wurden Forscher zu folgenden Themen beraten:

- zur Anonymisierung in Stammbaumveröffentlichungen bei Erkrankungen an fataler familiärer Insomnie,
- zum internationalen Verbund von Gedenkstätten mit einer Recherchemöglichkeit nach Häftlingsdaten aus den Jahren 1933 bis 1945,
- zur Analyse der politischen Kommunikation im Internet für eine Begleitdokumentation an der Staatlichen Europaschule,
- zu einer Analyse des Rauchverhaltens von Schülern der 6. und 7. Klassen,
- zu einer Längsschnittstudie zur Lesekompetenz in der Grundschule,
- zu einer Untersuchung der Lernausgangslage von Schülerinnen und Schülern der Klassenstufen 8 bis 10 an Schulen für Lernbehinderte zur gezielten Unterstützung der Berufswahl,
- zum Neugeborenen-Hörscreening mit Patiententracking in den ersten drei Lebensmonaten für eine Früherkennung und Frühtherapie in Zusammenarbeit mit dem Deutschen Zentralregister für kindliche Hörstörungen.

Nachfolgende Projekte wurden einer rechtlichen und technisch-organisatorischen Prüfung vor Ort unterzogen:

- Normierung und Validität von Lehrerfragebögen zu Stärken und Schwächen an der Charité,

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

- die Evaluationsstudie zu Integrationsverträgen bei der Gesellschaft für Innovationsforschung und Beratung im Auftrag des Bundesverwaltungsamtes,

- die Umfrage zu Gesundheit, Lebensqualität und Sexualität bei Männern zwischen 40 und 80 Jahren an der Charité,

- das Deutsche Zentralregister für kindliche Hörstörungen am Universitätsklinikum Benjamin Franklin,

- das Nationale Register für Patienten mit angeborenen Herzfehlern an der Charité und dem Deutschen Herzzentrum.

Die Projekte, die schon zum Teil seit Jahren von uns datenschutzrechtlich betreut werden, waren im Ergebnis der Prüfung nicht grundsätzlich zu bemängeln. Kleine Unzulänglichkeiten wurden umgehend abgestellt.

In den Universitätsklinika Charité und Benjamin Franklin sind die Prüfungen unter Einbeziehung des Datenschutzbeauftragten erfolgt; die Berücksichtigung von Hinweisen wurde von ihm kontrolliert.

Datennetze für die medizinische Forschung

Ausführlich berichteten wir im Jahresbericht 2000 über die datenschutzrechtlichen Ansätze für die Ausgestaltung von *medizinischen Forschungsnetzwerken*. Im vergangenen Jahr wurden im Auftrag des Koordinierungsrates der Telematikplattform „Medizinische Forschungsnetze" generische Lösungen zum Datenschutz vorgelegt. Im gesamten Jahr 2002 diskutierten wir mit den Forschern und den Informatikern des Berliner Fraunhofer Instituts für Software und Systemtechnik (ISST) die verschiedenen Modelle. Während wir, wie im Jahresbericht 2000 dargelegt[88], zunächst von einer Musterlösung ausgingen, zeigte sich, dass der Bedarf aller Forschungsnetze mit nur einem generischen Modell nicht abgedeckt werden kann. Neben den behandlungsfernen, wissenschaftlich fokussierten Forschungsnetzen entstand ein Bedarf an behandlungsnahen, klinisch fokussierten Forschungsnetzen.

Bei klinisch fokussierten Forschungsnetzen steht die unmittelbare Ableitung der wissenschaftlichen Daten aus dem Behandlungsprozess im Mittelpunkt. Durch die zeitnahe Zusammenführung der Daten aus den Behandlungsprozessen wird auch die klinische Befundkommunikation verbessert. Die wissenschaftliche Nutzung der in einer klinischen Datenbank zusammengeführten Informationen darf aber, um eine Vermengung von Behandlung und Forschung zu vermeiden, nicht online erfolgen. Aus der klinischen Datenbank werden nur entsprechend der wissenschaftlichen Fragestellung anonymisierte oder pseudonymisierte Daten-

Im Hinblick auf die in den Universitätsklinika angestrebten Telematikanwendungen erfolgt hinsichtlich des Datenschutzes durch die Datenschutzbeauftragten der Klinika mittels Instrument der Vorabkontrolle die Prüfung der besonders sensiblen personenbezogenen Daten. Festgestellte Risiken werden mittels angemessener Schutzmaßnahmen eingedämmt.

Von den Möglichkeiten der Anonymisierung und Pseudonymisierung wird nach Auskunft der Datenschutzbeauftragten der Universitätsklinika ebenfalls Gebrauch gemacht, soweit dies möglich ist und der

[88] JB 2000, 4.5.1

teilmengen exportiert. Hier besteht jedoch weiterer Diskussionsbedarf im Arbeitskreis „Wissenschaft" der Konferenz der Datenschutzbeauftragten des Bundes und Länder.

Im Unterschied dazu stützen sich wissenschaftlich fokussierte Forschungsnetze auf die zum Zweck der Forschung erhobenen Daten. Diese stammen sowohl aus dem Behandlungsprozess als auch aus speziellen Erhebungen beim Patienten selbst oder seinem behandelnden Arzt. Ein gravierendes Problem dieser Netzwerkkonstellation ist die Qualitätskontrolle der eigens für die Forschung erhobenen Daten. Sie unterliegen nicht unmittelbar der klinischen Qualitätskontrolle der Behandlungsdaten, da sie häufig eigens zusätzlich für die Forschung erhoben werden. Es ist daher erforderlich, sie vor der Übernahme in das jeweilige Forschungsregister auf Plausibilität und Vollständigkeit zu überprüfen. Dies wirft ein grundsätzliches Problem bei der stufenweisen Pseudonymisierung auf. Die Lösung wurde darin gefunden, dass die an die Forschungsdatenbank zu übermittelnden Daten zunächst zwischengespeichert werden und in einem automatisierten Prozess der Depseudonymisierung von Daten aus der Forschungsdatenbank auf ihre Plausibilität hin überprüft werden. Lediglich unplausible Datensätze werden durch eine gesonderte Stelle bis zur Klärung mit der meldenden medizinischen Einrichtung in einem schwächer pseudonymisierten Zustand gespeichert. Durch dieses Verfahren wird insbesondere auch die treuhänderische Verwaltung der Pseudonyme bei einem Datentreuhänder gewährleistet.

Wir betreuen die nachfolgenden patientenbeziehbaren Forschungs- bzw. Behandlungsregister:

- das „Nationale Register für Patienten mit Angeborenen Herzfehlern" des Kompetenznetzwerkes „Angeborene Herzfehler",
- das Deutsche Zentralregister für angeborene Hörstörungen,
- die Kerndokumentation des Kompetenznetzes Rheuma,
- das Nierenbehandlungsregister „QuaSi-Niere"
- das Patientenregister des Kompetenznetzwerkes chronisch-entzündliche Darmerkrankungen,
- das Patientenregister des Projektes „Evaluation anthroposophischer Medizin",
- die Verwaltung der Proben und Zweitbefunde des Kompetenznetzes Maligne Lymphome.

Des Weiteren haben wir die Deutsche Aidshilfe im Zusammenhang mit dem Aufbau eines Patientenregis-

Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

ters HIV-infizierter bzw. -erkrankter Personen ausführlich beraten.

Pseudonymisierung in der pharmakologischen Forschung

Im Frühjahr 2002 bat uns die *Ethik-Kommission* der Ärztekammer Berlin, das *Pseudonymisierungsverfahren* eines pharmakologischen Forschungsunternehmens zu prüfen. Das Unternehmen ist in der so genannten Phase I der klinischen Forschung tätig. In dieser Phase wird die Unschädlichkeit bzw. werden die Nebenwirkungen von neuen Medikamenten durch gesunde Probanden überprüft. Das Unternehmen übermittelte nach Abschluss der Studie dem Auftraggeber die medizinischen Daten unter Nutzung der Namensinitialen, des vollständigen Geburtsdatums und des Geschlechts. Gegenüber den Laboren wurden zur Kennzeichnung der Proben wie auch dann der Ergebnisse die Namensinitialen, das Geschlecht und das Alter genutzt. Lediglich im Zusammenhang mit Probenentnahmen zur Genotypisierung wurden randomisierte Initiale erzeugt und diese mit einer studienbezogenen, nicht aus den personenbezogenen Daten hergeleiteten Nummer versehen. Wir empfahlen dem Unternehmen, dieses Verfahren grundsätzlich für alle Datenübermittlungen zu nutzen. Die Forscher kamen dieser Empfehlung nach.

Daraufhin kam es bei der Ärztekammer Berlin im Frühsommer zu einem Gespräch mit Berliner Unternehmen, die Arzneimittelforschung in der Phase II und III betreiben. In diesen Phasen werden die neuen Arzneimittel auf ihre Wirksamkeit bei erkrankten Personen in verschiedenen Behandlungseinrichtungen getestet. Die Prüfärzte in verschiedensten Kliniken und Arztpraxen führen dazu neben den Behandlungsunterlagen gesonderte Protokolle, die dann den pharmakologischen Unternehmen übermittelt werden. Diese Prüfberichte enthalten als identifizierende Merkmale die Namensinitialen, das Geschlecht, das Geburtsdatum und die ethnische Zugehörigkeit. Diese Art der „sprechenden" Pseudonymisierung erlaubt es den Prüfärzten, bei Rückfragen durch das forschende Unternehmen relativ einfach und unter Ausschluss möglicher Verwechslungen anhand der Patientenakten Rückfragen und Unplausibilitäten zu klären.

§ 3 a BDSG gebietet jedoch, von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Die gegenwärtige Art der Verschlüsselung entspricht nicht mehr der Definition des Pseudonymisierens als „des Ersetzens des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren". Die pharmakologischen Unternehmen gaben aber zu bedenken, dass der Datenaustausch unter Nutzung einer echten Pseudonymisierung möglicherweise zu größe-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

ren Datenausfällen und einer Reihe von nicht klärbaren Unplausibilitäten in den Datenbeständen und in den Prüfberichten führen würde.

Eine Möglichkeit bestünde zunächst darin, dass im Datenaustausch zwischen den Prüfärzten und den pharmakologischen Unternehmen auf die Nutzung des vollständigen Geburtsdatums verzichtet wird. Hier dürften Namensinitialen, Geburtsjahr und Geschlecht die Person bei den Prüfärzten hinlänglich reidentifizierbar machen. Eine derartige Empfehlung hat auch der Hamburgische Datenschutzbeauftragte bei der Prüfung eines privaten Labors gegeben. Im Weiteren sollten dann im pharmakologischen Unternehmen diese Verschlüsselungen durch ein echtes Pseudonym ersetzt werden und dieses Pseudonym mit der Verschlüsselung und der Nutzung von Namensinitialen in einer Zuordnungsliste gesondert und geschützt gespeichert werden. Treten dann beispielsweise nach der Übermittlung an eine Arzneimittel-Zulassungsbehörde Fragen auf, kann mit Hilfe der Zuordnungsliste eine Überprüfung bei den Prüfärzten bzw. Kliniken erfolgen.

Die Vorschläge werden gegenwärtig sowohl im Arbeitskreis Wissenschaft der Datenschutzbeauftragten als auch im Arbeitskreis der Ethik-Kommissionen und im Verband der pharmakologischen Industrie erörtert.

4.5.2 Schule

Mehr Datenschutz im neuen Schulgesetz

Im Gesetzentwurf für ein neues *Schulgesetz* (E-SchulG)[89] finden sich viele der von unserer Behörde in den letzten Jahren gegebenen Hinweise wieder. Obwohl die Erhebung personenbezogener Daten der Schüler sowie deren Erziehungsberechtigten auch bisher geregelt waren (§ 5 a Schulgesetz, Schuldatenverordnung, Sonderpädagogikverordnung), blieben immer wieder Fragen offen, die unter Rückgriff auf allgemeine datenschutzrechtliche Festlegungen sowie verfassungsrechtliche Grundsätze zu entscheiden waren. Insbesondere der innere Schulbereich „Datenschutz im Unterricht" entzog sich rechtlichen Regelungen. Dieses Problem ist zwar auch durch das neue Schulgesetz nicht grundsätzlich lösbar. Da aber stärker als im alten Schulgesetz und im alten Schulverfassungsgesetz die inhaltlichen Schwerpunkte von „Bildung und Erziehung" einschließlich der Bildungs- und Erziehungsziele ausformuliert wurden, sind Lehrer, Schulleiter und Schulaufsichtsbeamte nach dem neuen Schulgesetz mehr als bisher auf die Vermittlung der informationellen Selbstbestimmung verpflichtet.

Kern des neuen Schulgesetzes ist die Neuformulierung

Die datenschutzrechtlich relevanten Regelungen im Entwurf für eine neues Schulgesetz wurden von der Senatsverwaltung für Bildung, Jugend und Sport mit dem Berliner Datenschutzbeauftragten bereits frühzeitig und in enger Kooperation abgestimmt. Den im Jahresbericht 2002 noch angesprochenen datenschutzrechtlichen Bedenken, beispielsweise zum Datenschutz an den Privatschulen, ist zwischenzeitlich Rechnung getragen worden; der Entwurf wurde insoweit nach erneuter gemeinsamer Beratung geändert.
Der Berliner Datenschutzbeauftragte wird auch im weiteren Gesetzgebungsverfahren rechtzeitig von der Senatsverwaltung für Bildung, Jugend und Sport beteiligt werden.

[89] neues Schulgesetz für das Land Berlin, Entwurf der Senatsverwaltung für Bildung, Jugend und Sport vom 20. November 2002

der Schulgestaltung. Insbesondere geht es dabei darum, die Selbständigkeit und Eigenverantwortung der Schule zu sichern sowie Maßnahmen der Qualitätssicherung durch Gesetz zu legitimieren und hierfür als regelmäßiges Arbeitsinstrument die *Evaluation des Schulbetriebes* einzuführen. Evaluationsmaßnahmen sind allerdings nicht möglich, ohne dass personenbezogene Daten gesammelt werden.

Das mildeste Mittel von *Evaluationsmaßnahmen* sind Datenerhebungen auf freiwilliger Grundlage. Freiwillige Datenerhebungen erlauben jedoch nicht mit hinreichender Wahrhaftigkeit ein Abbild der realen Situation einer Schule oder des Vergleichs zwischen den Schulen. Das Schulverhältnis ist ein Pflichtverhältnis. Die Schulpflicht ist einer der erheblichsten staatlichen Eingriffe in das Persönlichkeitsrecht eines jeden Menschen, da er ihr mindestens für zehn Jahre unterliegt. Da aber die Schule in demokratisch verfassten Gesellschaften humanistische Ideale zu verfolgen hat und Demokratie bildend wirken soll, kann es weder dem Lehrer noch dem Schüler überlassen bleiben, die Wirksamkeit dieses staatlichen Eingriffs zu bewerten.

Daher findet sich als Gegenstück zu den Bestimmungen über die Evaluation die datenschutzgerechte Ausgestaltung der Verpflichtung von Schülern und Lehrern, sich an Tests, Befragungen, Erhebungen und Unterrichtsbeobachtungen zu beteiligen. Der Ausgleich zu dieser Auskunftspflicht liegt insbesondere in der umfassenden Information über die Evaluationsmaßnahme sowie die Verpflichtung, die Einzeldaten zu anonymisieren oder wenigstens ersatzweise zu pseudonymisieren (§ 65 ESchulG).

Kennzeichnend für die Berliner Schulen ist eine Vielzahl von *Schulversuchen* sowie die Entwicklung verschiedenster Schulen besonderer pädagogischer Prägung. Diese Schulversuche und Schulen sind insbesondere dadurch charakterisiert, dass durch den Inhalt des schulischen Angebots bestimmte förderungsfähige Schüler angesprochen werden sollen. Um diesem Schulzweck zu genügen, ist eine Auswahl der Schüler erforderlich. Dabei werden personenbezogene Daten über Schüler, aber auch deren Erziehungsberechtigte, insbesondere über die Fähigkeiten und Fertigkeiten der Schüler erhoben. Auch hier ist zu begrüßen, dass für Schulen dieser besonderen pädagogischen und organisatorischen Konzepte eine Rechtsverordnung erlassen werden soll.

§ 19 Abs. 4 ESchulG regelt erstmals die Rechtsstellung von Internaten. Schule und Internat bilden eine pädagogische Einheit. Die Schulaufsicht erstreckt sich auch auf das Internat und die außerunterrichtliche Betreuung der Internatsbewohner. Leider wurden hier unsere früheren Anregungen zum Erlass von Internatsordnungen, die anders als Hausordnungen der Schule auch die Achtung der Privatheit der Internatsbewohner berücksichtigen, nicht aufgenommen. Beschwerden haben

gezeigt, dass die Persönlichkeit, ja die Intimsphäre nicht immer hinreichend geachtet wurde.

Zu begrüßen ist, dass die *Schulpflicht* umfassend geregelt werden soll. Bislang war diese nur zum Teil Gegenstand des Schulgesetzes, zu einem wesentlichen Teil aber auch Gegenstand der Schulpflichtverordnung. Die Festlegungen zur Schulpflicht in diesem Teil finden ihre Ergänzung in den Ordnungswidrigkeitstatbeständen des § 126 ESchulG. Die Regelung des § 44 ESchulG weist jedoch eine Ungenauigkeit auf. Die Verantwortung für die Einhaltung der Schulpflicht wird hier lediglich bei den Erziehungsberechtigten bzw. den Ausbildenden festgemacht. Die Problematik volljähriger Schüler in Regelschulen sowie in berufsbildenden Schulen wurde vergessen. Dies sollte ergänzt werden. Ebenso sollte die Schuldatenverordnung nochmals bezüglich der Datensammlungen zu Entschuldigungen überprüft werden.

§ 46 Abs. 5 ESchulG legt fest, dass Schüler aus wichtigem Grund auf Antrag vom Unterricht beurlaubt oder von der Teilnahme an einzelnen Unterrichts- oder Schulveranstaltungen befreit werden können. Lediglich im Zusammenhang mit der Niederkunft von Schülerinnen wird klar, dass die zuständige Schulbehörde über den Antrag entscheidet. Wer im anderen Falle über Anträge entscheidet, ist nicht ersichtlich. Da diese Entscheidungen jedoch erhebliche Auswirkungen haben, dürften die Festlegungen wohl kaum durch eine Ausführungsvorschrift geregelt werden.

Auch § 47 ESchulG zu den Informationsrechten der Schülerinnen und Schüler und der Erziehungsberechtigten dürfte zu Missverständnissen führen. Wir gingen bislang davon aus, dass es im Rahmen des Bildungs- und Erziehungsauftrages zulässig ist, dass im Rahmen des Unterrichts einzelne Leistungen von Schülern ausgewertet und die Benotung allen mitgeteilt wird, ebenso bei der Rückgabe von Klassenarbeiten oder auch der Übergabe von Zeugnissen, solange dabei der Grundsatz der Gleichbehandlung gewahrt bleibt und stigmatisierende oder diskriminierende Praktiken unterbleiben. § 47 Abs. 4 ESchulG erlaubt es lediglich, dass der Schulleiter oder die Lehrkräfte die Schüler sowie deren Erziehungsberechtigte individuell und in angemessenem Umfang über die Lern-, Leistungs- und Kompetenzentwicklung des Schülers informieren. Diese allgemeinen, die Persönlichkeit in größerem Umfang charakterisierenden Informationen sollten zwar individuell erfolgen. Die Regelung lässt jedoch auch den Fehlschluss zu, dass Einzelleistungen wie bei der Rückgabe von Klassenarbeiten nicht mehr im „Klassenverband" ausgewertet werden dürften.

Zu begrüßen ist, dass in § 47 Abs. 5 ESchulG eine Informationsbefugnis für frühere Erziehungsberechtigte von nunmehr volljährigen Schülern über bestimmte gravierende Tatbestände aufgenommen werden soll, eine Reaktion auf die Ereignisse in Erfurt (vgl. unten).

Deutlicher als bisher legt § 52 Abs. 2 ESchulG fest, dass schulärztliche, schulzahnärztliche oder schulpsychologische Untersuchungen sowie Untersuchungen bei Feststellungsverfahren von sonderpädagogischem Förderbedarf oder zur Feststellung der Kenntnisse der deutschen Sprache auch der Schulpflicht unterliegen und Kinder, Schüler sowie deren Erziehungsberechtigte verpflichtet werden, erforderliche Angaben zu machen. Zu begrüßen ist, dass Fragen zur Privatsphäre der Erziehungsberechtigten ausgeschlossen sind.

In § 58 ESchulG (*Lernerfolgskontrollen* und *Zeugnisse*) werden erstmals auch Datenerhebungen im Unterricht legitimiert. Nach Abs. 5 stützt sich die Leistungsbeurteilung der Schüler durch ihre Lehrkräfte „auf die regelmäßige Beobachtung und Feststellung der Lern-, Leistungs- und Kompetenzentwicklung". Damit wird die unvermeidliche Praxis auch gesetzlich legitimiert, dass der Leistungsbeurteilung durch den Lehrer eine erhebliche subjektive Komponente innewohnt, die sich auf seine Fähigkeiten der „ständigen Beobachtung und Registratur" der Aktivitäten der Schüler stützt. § 58 ESchulG öffnet auch die Möglichkeit, dass durch Beschluss der Schulkonferenz „Tugendnoten" zum Arbeits- und Sozialverhalten vergeben werden. Dagegen ist datenschutzrechtlich nichts einzuwenden, solange die Formen der Information der Erziehungsberechtigten und Schüler sich von dem Grundsatz der Gleichbehandlung und Nichtstigmatisierung leiten lassen.

Bislang war im Schulgesetz nur ein Verbot der körperlichen Züchtigung enthalten. Die Neuregelung in § 63 Abs. 2 ESchulG schließt auch ein Verbot anderer entwürdigender Maßnahmen ein. Diese Ergänzung erlaubt es, stärker als bislang Maßnahmen mit stigmatisierendem Charakter im Unterricht als datenschutzrechtliche und nicht nur als pädagogische Verstöße zu bewerten. So können nunmehr auch entwürdigende Maßnahmen wie das Vorlesen von intimen Aufzeichnungen von Schülern beanstandet werden.

Nach der bisherigen Fassung werden die datenschutzrechtlichen Regelungen des Schulgesetzes nicht auf die *Privatschulen* ausgedehnt, die als Ersatz- oder Ergänzungsschulen tätig sind. Dem Datenschutz kommt aber gerade an Privatschulen besondere Bedeutung zu, weil hier häufig eine tendenziöse Grundausrichtung des Schulträgers die Erhebung und Verarbeitung nicht erforderlicher, teilweise auch sensitiver Daten nahe legt.

Durch die Einordnung des schulpsychologischen Dienstes in die Schulaufsicht (§ 107ESchulG) dürfte das grundlegende datenschutzrechtliche Problem der Schweigepflicht der einzelnen Schulpsychologen einerseits und der Notwendigkeit der Verarbeitung sensitiver Daten zur Erfüllung der Aufgaben des Schulgesetzes andererseits rechtlich lösbar werden.

Die Befugnis der Gremien, sich mit personalrechtlichen Angelegenheiten zu befassen, wird begrenzt. Dienst- und personalvertretungsrechtliche Bestimmungen werden durch die Gremienarbeit nicht eingeschränkt. In § 122 ESchulG ist von Bedeutung, dass bei den Sitzungsprotokollen der Gremien zwischen einem öffentlich einsehbaren Teil und einem vertraulichen Teil zu unterscheiden ist. Ebenso gilt für die Gremienmitglieder die Verpflichtung zur Verschwiegenheit in allen Personalangelegenheiten oder weiteren Angelegenheiten, bei denen für das Gremium die Vertraulichkeit beschlossen wurde. Bei Verstößen droht der Ausschluss aus dem Gremium. Dies war bislang lediglich in einem Rundschreiben zur Gremienarbeit von 1990 als erläuternde Verwaltungsvorschrift festgeschrieben.

In einem allgemeinen Abschnitt zum Datenschutz werden eingeführt:

- eine Auskunftspflicht der Erziehungsberechtigten zur Erhebung der Daten nach der Schuldatenverordnung (§ 64 Abs. 1);

- eine Beschränkung des Austauschs personenbezogener Daten im internen Geschäftsbetrieb der Schulen und Schulbehörden (§ 64 Abs. 2 Satz 1);

- das Verbot zur Nutzung privater Datenverarbeitungsgeräte zur Verarbeitung personenbezogener Daten in der Schule und außerhalb der Schule sowie die Befugnis zu Ausnahmegenehmigungen (§ 64 Abs. 2 Satz 2 und 3) wurden von der Ebene der Schuldatenverordnung in das Schulgesetz selbst hineingezogen; eine Mitwirkung der schulischen Datenschutzbeauftragten ist so jedoch nicht vorgesehen, es sei denn, die Regelung in der Schuldatenverordnung bleibt erhalten;

- bei Datenübermittlungen wird explizit ein Nachweis verlangt.

Die Befugnis zur Übermittlung personenbezogener Daten an Stellen außerhalb des öffentlichen Bereichs (§ 64 Abs. 4) wird klarer gefasst. Sie besteht bei

  - Einwilligung,

  - Informationsrechten der Erziehungsberechtigten und der Schüler selbst,
  - glaubhaft gemachtem rechtlichem Interesse des Empfängers nebst Abwägung der schutzwürdigen Interessen,

  - Richtigstellung unwahrer Tatsachenbehauptungen Betroffener im Zusammenhang mit Angaben nach dem Schulgesetz (Befugnis zu Dementis und Richtigstel-

lungen in der Presse).

– § 65 ESchulG regelt das Verfahren bei der Evaluation, bei wissenschaftlichen Untersuchungen und statistischen Erhebungen. Wissenschaftliche Erhebungen bedürfen nach wie vor der schulaufsichtlichen Genehmigung. Im Unterschied zur bisherigen Regelung ist die Einwilligung der Erziehungsberechtigten nur noch bei Schülern, die das 14. Lebensjahr noch nicht vollendet haben, erforderlich.

Bislang war ein einfacher Verweis auf die Forschungsklausel des § 30 BlnDSG im § 5 a SchulG vorhanden. Nunmehr werden die Abwägung bei Forschung ohne Einwilligung der Betroffenen und das Anonymisierungsgebot unmittelbar geregelt.

Die Statistikregelung der Schuldatenverordnung genügte bislang nicht den Regelungen des Landesstatistikgesetzes. Nunmehr ist vorgesehen, dass die Schulen verpflichtet sind, der Schulbehörde für statistische Zwecke Einzelangaben zu übermitteln.

Informations- und Auskunftsrechte von Eltern volljähriger Schüler – Einwilligungsfähigkeit minderjähriger Schüler

Nach den tragischen Ereignissen in Erfurt befassen sich die Kultusministerien der einzelnen Bundesländer mit der Frage, ob und wenn ja, in welchen Fällen die *Eltern volljähriger Schüler* auch ohne deren Einverständnis durch die Schule über schulische Angelegenheiten ihres Kindes informiert werden dürfen. Die Thüringer Landesbeauftragte für den Datenschutz führte eine Umfrage bei allen Datenschutzbeauftragten mit dem Ziel eines Informationsaustausches über die Gesetzeslage der Bundesländer durch. Es stellte sich heraus, dass in den meisten Bundesländern Gesetzesänderungen in Vorbereitung sind, die ein derartiges Informationsrecht ermöglichen sollen. Im Detail gibt es hierzu unterschiedliche Lösungen.

Nach der Berliner Rechtslage gab es bisher keine eindeutige Regelung. So könnte zwar aus der Regelung des § 5 a SchulG in schwerwiegenden Einzelfällen ein derartiges Informationsrecht abgeleitet werden. Dieser Auffassung folgte die Senatsverwaltung für Bildung, Jugend und Sport so nicht. Im neuen Schulgesetz wird nunmehr eine Regelung zu den zulässigen Informationsmöglichkeiten vorbereitet (vgl. oben).

Auf der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurde die Thematik ebenfalls aufgegriffen. Sie kam zu dem Ergebnis, dass für eine derartige Datenübermittlung zumindest folgende Voraussetzungen geboten sein müssen:

- eine klare gesetzliche Regelung;

- kein Automatismus bei entsprechenden Datenweitergaben, sondern differenzierte Entscheidungsmöglichkeiten der Schulen im Einzelfall;

- möglichst eine Unterrichtung der betroffenen Schüler über die beabsichtigte Datenübermittlung.

Schulwegbeförderung für Kinder mit Behinderung

Zum Schuljahr 2002/2003 wurde in einem Berliner Bezirksamt damit begonnen, im Rahmen der Bewilligung der Beförderungsübernahme behinderter Schüler von den Eltern Angaben zu ihren wirtschaftlichen Verhältnissen zu verlangen. Die Übernahme der Beförderung sollte von den wirtschaftlichen Möglichkeiten der Eltern abhängig gemacht werden. Eltern wandten sich daraufhin an uns.

Für das Erheben dieser Daten gibt es keine rechtliche Grundlage. Die Regelung über das Antragsverfahren (§ 37 *Sonderpädagogikverordnung* - VO Sonderpädagogik) sieht keine wirtschaftlichen Erwägungen bei der Entscheidung über die Beförderungsübernahme vor.

Bei der Neufassung des § 37 VO Sonderpädagogik wurden bewusst keine wirtschaftlichen Aspekte in die Regelung aufgenommen. Zu der Neufassung war es gekommen, weil schon 1996 die Frage problematisiert worden war, welche Angaben von den Eltern bei einem derartigen Antrag verlangt werden dürfen. Daraufhin wurden nähere Entscheidungskriterien, der Grad der Behinderung und die Länge und Dauer des Schulweges, in die VO Sonderpädagogik aufgenommen. Über die Problematik berichteten wir bereits im Jahresbericht 1996[90].

Im Rahmen der erneut entstandenen Diskussion über das Antragsverfahren wurde außerdem offenbar, dass es in den Bezirksämtern unterschiedliche Antragsverfahren für die Beförderungsübernahme behinderter Schüler gibt. Vertreter der Bezirksämter, der Senatsverwaltung für Bildung, Jugend und Sport und unserer Behörde verständigten sich nunmehr darauf, hierfür zum nächsten Schuljahr ein Berlin-einheitliches Verfahren einzuführen. Damit wird auch die Kritik des Berliner Rechnungshofes an der uneinheitlichen Praxis des Antragsverfahrens berücksichtigt. Eine Arbeitsgruppe aus Vertretern einiger Bezirksämter der Senatsverwaltung für Bildung, Jugend und Sport und unserer Behörde erarbeitet zurzeit ein einheitliches Antragsformular.

---

[90] JB 1996, 4.5.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Führung der Schülerbögen an den Schulen

Obwohl wir die Schulen bereits mehrfach darauf hingewiesen haben, finden sich doch immer wieder im Innenteil des Aktendeckels eines Schülerbogens Eintragungen über die Teilnahme der Eltern bzw. Erziehungsberechtigten am Elternabend.

Wenn nicht unmittelbar im Zusammenhang mit dem Elternabend ein persönliches Gespräch mit dem Klassenlehrer stattgefunden hat, gehört dies nicht in den *Schülerbogen*. Der Schülerbogen ist im Gegensatz zur Elternversammlung, in der pädagogische Fragen von allgemeinem Interesse besprochen werden, eine individuell geführte Unterlage. Er dient dem besseren Verständnis der Persönlichkeit des Schülers und als Grundlage für die Zusammenarbeit zwischen Schule und Elternhaus. Die Teilnahme an Elternversammlungen ist im Schülerbogen nicht von Bedeutung und hierin auch nicht zu vermerken.

Wir bereiten in Zusammenarbeit mit dem Landesschulamt ein Rundschreiben vor, in dem auf verschiedene problematische Punkte bei der Führung der Schülerbögen eingegangen werden soll.

Information des nichtehelichen Lebenspartners eines Erziehungsberechtigten

Eine Lehrerin fragte aufgrund einer Auseinandersetzung mit ihrem Schulleiter, wieweit nichteheliche Lebenspartner eines Erziehungsberechtigten vom Lehrer Auskünfte über das schulpflichtige Kind erhalten dürfen.

Lehrer und Lehrerinnen sind nicht verpflichtet, mit dem *nichtehelichen Partner* über das betreffende Kind zu sprechen. Die Informationspflicht der Lehrer über den Leistungsstand des Schülers und die Unterrichtsgestaltung richtet sich nur an die Erziehungsberechtigten (§ 40 Schulverfassungsgesetz). So kann der Lehrer auch telefonische Gespräche über einen Schüler abbrechen, wenn sich in deren Verlauf der Lebenspartner des/der Erziehungsberechtigten einschaltet.

An Elternversammlungen kann der Lebenspartner nur als Gast ohne Stimmrecht teilnehmen, wenn zwei Drittel der Anwesenden dem zustimmen.

4.5.3 Statistik

Zensustest

Über einen guten Start beim ersten Teil des *Zensustestes* konnten wir bereits im Jahresbericht für das Jahr

Der Zensustest ist eine bundesweit einheitliche Unternehmung, die vom Statistischen Bundesamt koordiniert

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

2001[91] informieren. Im Sommer des vergangenen Jahres lagen dann auch die Ergebnisse der „Geburtstagsstichprobe" vor. Danach wurden die Daten aller Personen, die am 1. Januar, 15. Mai oder 1. September geboren sind oder ein unvollständiges Geburtsdatum haben, von den Meldebehörden an das Statistische Bundesamt übermittelt. Dies waren ca. 900.000 Datensätze. Im Statistischen Bundesamt wurde dann geprüft, ob für jede Person nur ein Hauptwohnsitz vorliegt oder ob für Personen mit Nebenwohnsitz auch immer eine Hauptwohnung verzeichnet ist. In bundesweit lediglich knapp 9.000 Fällen wurden die Betroffenen angeschrieben und danach befragt, ob es sich bei den verschiedenen Wohnungen um die alleinige Wohnung oder die Hauptwohnung handele. Dazu wurden diese Anschriften in den Fragebogen eingedruckt. Der Betroffene brauchte nur noch die entsprechende Kategorie anzukreuzen.

Von den Datenschutzbeauftragten wurde kritisiert, dass die Betroffenen im Anschreiben nicht ausdrücklich auf die Auskunftspflicht hingewiesen wurden. Lediglich aus dem dem Schreiben beigelegten Text des Zensustestgesetzes war die Auskunftspflicht ersichtlich.

In Berlin wurden insgesamt weniger als Tausend Personen in die Befragung einbezogen. Ob dieses Ergebnis nun darauf hindeutet, dass das zu testende neue Zensusverfahren auf Meldedaten hoher Qualität zurückgreifen kann, oder ob bei der Zusammenführung der Daten aus verschiedenen Melderegistern möglicherweise unterschiedliche Personen für identisch erklärt wurden und somit Fehler aus den Melderegistern kaschiert werden, bleibt erst der späteren Auswertung der Tests vorbehalten.

wird. Der Senat hat mehrfach darauf gedrungen, auch in dem Anschreiben, das fester Bestandteil des Fragebogens ist, den Hinweis auf die Auskunftspflicht unterzubringen. Die das Thema „Hauptwohnsitz" bundeseinheitlich bearbeitende Projektgruppe hat sich jedoch dagegen entschieden, weil auf die Auskunftspflicht in den beiliegenden Informationen hingewiesen wurde. Da die Fragebögen bundeseinheitlich gestaltet waren, konnte der Senat von den bundeseinheitlichen Vorgaben nicht abweichen und somit auf die Auskunftspflicht im Anschreiben auch nicht direkt hinweisen.

Immer andere Zahlen – Wie viel Beschäftigte hat der öffentliche Dienst Berlins?

In der Sitzung des Hauptausschusses des Abgeordnetenhauses vom 28. August 2002 wurde das Dilemma offensichtlich, dass je nach Berechnungsgrundlage ständig andere Beschäftigtenzahlen des öffentlichen Dienstes in Berlin in der öffentlichen Diskussion, aber auch in den Solidarpaktverhandlungen zugrunde gelegt wurden. Zwar wurde mit der Umstellung des *Bezügeverfahrens* auf das Integrierte Personalverfahren (IPV) eine Schnittstelle für das Statistische Landesamt zur Erarbeitung der bundesweiten *Personalstandsstatistik* geschaffen. Aber die Aufbereitung dieser Einzeldaten erfolgt ausschließlich nach bundeseinheitlichen Vorgaben und erlaubt keine Berlin-spezifische Auswertung. Da die an das Statistische Landesamt übermittelten Einzeldaten den strengen Vorschriften der statistischen Geheimhaltung unterliegen, ist eine weitere statistische Auswertung durch Dritte, insbesondere um einheitliche

Die Darstellung wird in allen wesentlichen Punkten geteilt.

Die senatsinterne Abstimmung über den Entwurf des beabsichtigten Personalstrukturstatistikgesetzes ist derzeit noch nicht abgeschlossen.

[91] JB 2001, 4.5.1

Planungsgrundlagen für das Land Berlin zu schaffen, rechtlich ausgeschlossen.

Nur wenn ein nach dem Landesstatistikgesetz verfasstes einzelstatistisches Landesgesetz dieses erlaubt, wäre die rechtliche Zulässigkeit gegeben. Wir schlugen im Sommer des Jahres 2001 vor, eine solche Rechtsgrundlage zu erarbeiten. Ein erster Vorentwurf für ein Personalstrukturstatistikgesetz lag im Februar des Berichtsjahres vor. Kern einer solchen Vorschrift kann nur sein, dass diese Daten entweder durch das Statistische Landesamt selbst oder durch eine organisatorisch, personell und räumlich von Stellen des Verwaltungsvollzuges einschließlich der Personalstellen abgeschottete eigenständige Statistikstelle unter Wahrung des Statistikgeheimnisses aufbereitet und zu statistischen Ergebnissen aggregiert werden. Ein Zugriff Dritter außer den mit dieser Aufbereitung beauftragten Personen auf Einzeldaten ist strafbewehrt auszuschließen.

Die Aufbereitung der Daten durch eine abgeschottete Statistikstelle wurde auch schon im Volkszählungsurteil als rechtlich zulässig angesehen. Dem Gebot der Trennung von Statistik und Verwaltungsvollzug folgend sahen es die Verfassungsrichter als zulässig an, dass die „zu statistischen Zwecken erhobenen, noch nicht anonymisierten, also noch personenbezogenen Daten .... kraft ausdrücklicher gesetzlicher Ermächtigung weitergeleitet werden, soweit und sofern dies zur statistischen Aufbereitung durch andere Behörden erfolgt und wenn dabei die zum Schutz des Persönlichkeitsrechts gebotenen Vorkehrungen, insbesondere das Statistikgeheimnis und das Gebot der Anonymisierung, in gleicher Weise zuverlässig sichergestellt sind, wie bei den Statistischen Ämtern des Bundes und der Länder”[92].

Neben der Abschottung der Statistikstelle sind auch Regelungen zu treffen, mit denen die Möglichkeiten der Identifizierung einzelner Beschäftigter so gering wie möglich zu halten sind. Unmittelbar nach der Plausibilisierung und dem Vergleich mit den Daten der vorherigen Erhebung muss ein mehrstufiges Pseudonymisierungsverfahren einsetzen. Eine Speicherung der Daten zu einer Person im Längsschnitt (die aktuellen Daten sollen mit den zuvor erhobenen verbunden werden, um somit Veränderungen abbilden zu können) ist auch in der Anonymität der Statistik nur zulässig, wenn nicht alle Daten zu einer Person gemeinsam gespeichert werden. Daher ist es notwendig, inhaltliche Komplexe, die auch schon im Gesetz zu formulieren sind, zu bilden. Dafür dürften auch noch einige technische und organisatorische Probleme zu meistern sein.

Nur wenn durch die rechtliche Abschottung der Statistikstelle ein „politischer Durchgriff” auf die Einzeldaten verhindert und dies zugleich auch durch technische

[92] BVerfGE 65, 1 (61)

Pseudonymisierungsmaßnahmen sowie andere Vorkehrungen faktisch erschwert, wenn nicht unmöglich gemacht wird, dürfte ein so erheblicher Eingriff in die Rechte der Bediensteten und Arbeitnehmer des unmittelbaren Landesdienstes auch verfassungskonform sein.

Die Arbeiten an dem Entwurf für ein Personalstrukturstatistikgesetz werden gegenwärtig mit Hochdruck federführend durch die Senatsverwaltung für Finanzen im Auftrag des Hauptausschusses durchgeführt. Bislang wurden unsere Hinweise in jeder Phase des Verfahrens berücksichtigt.

4.6 Wirtschaft

4.6.1 Banken und Versicherungen

Bürgerinitiative Berliner Bankenskandal

Die Bürgerinitiative Berliner Bankenskandal versucht, die Bürgschaftsverpflichtung des Landes Berlin gegenüber der Bankgesellschaft Berlin dadurch zu reduzieren, dass sie Fondszeichner der Fonds, die zu der finanziellen Schieflage bei der Bank geführt haben, dazu veranlasst, ihren Fondsanteil zu verkaufen. Um Kontakt mit den Fondszeichnern aufnehmen zu können, hat sich die Bürgerinitiative die personenbezogenen Daten der Fondszeichner, deren Fonds eine Kommanditgesellschaft ist, aus dem Handelsregister beschafft. Es gelang der Bürgerinitiative auch, die personenbezogenen Daten der Fondszeichner zu ermitteln, die Mitglieder einer BGB-Gesellschaft sind, obwohl deren Namen nicht im Handelsregister stehen.

Die namentlich bekannten Fondsbesitzer wurden angeschrieben und um Rückgabe ihres Fondsanteils, hilfsweise um eine Spende für eine soziale Einrichtung gebeten. Die Betroffenen wurden darauf hingewiesen, dass die Bürgerinitiative sich vorbehält, Namen von „uneinsichtigen Fondsbesitzern" zu veröffentlichen. Eine Liste von etwa 150 Fondsbesitzern wurde unter dem Titel „Die ehrenwerte Gesellschaft" von der Bürgerinitiative an die Medien verteilt. Eine Zeitung hat diese Liste auf ihrer Website veröffentlicht, die Bürgerinitiative hatte die Liste ursprünglich selbst ins Netz gestellt, später verwies sie nur noch auf die Website der Zeitung.

Da die Bürgerinitiative nicht als Verein oder Gesellschaft organisiert ist, ist sie nicht selbst verantwortliche Stelle nach § 3 Abs. 7 BDSG, sondern die einzelnen für sie handelnden Personen. Diese können sich nicht darauf berufen, dass die Erhebung, Verarbeitung oder Nutzung der Fondsbesitzerdaten im öffentlichen Interesse liegt, da nach § 28 Abs. 3 Nr. 2 BDSG die Nutzung oder Übermittlung im öffentlichen Interesse nur zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten zulässig ist. Allerdings wird man den für die Bürgerini-

tiative handelnden Personen in einem gewissen Umfang ein berechtigtes Interesse an den Daten der Fondsbesitzer zuerkennen müssen. Hierbei ist die politisch-wirtschaftliche Ausnahmesituation im Land Berlin zu berücksichtigen, die dazu führt, dass viele Bürger nicht mehr das Vertrauen darin haben, dass die betroffenen Bankiers und Politiker ohne „Druck von unten" bereit sind, den *Bankenskandal* aufzuklären und den wirtschaftlichen Schaden für die Stadt zu minimieren.

Die Rechtmäßigkeit der Datenerhebung, -verarbeitung und -nutzung der BGB-Gesellschafter richtet sich nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG, da diese Daten nicht allgemein zugänglich sind. Danach darf kein Grund zu der Annahme bestehen, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Da ein Mitglied der Bürgerinitiative auf die Frage, wie die Bürgerinitiative die Daten der BGB-Gesellschafter erhoben hat, die Aussage nach § 38 Abs. 3 Satz 2 BDSG verweigert hat, um sich nicht selbst zu belasten – dies deutet auf eine nicht gesetzmäßige Beschaffung der Daten hin – sind die schutzwürdigen Interessen der betroffenen BGB-Gesellschafter höher zu gewichten als etwaige berechtigte Interessen der Bürgerinitiative. Danach ist das Speichern, Übermitteln und Nutzen der personenbezogenen Daten der BGB-Gesellschafter rechtswidrig. Die Bürgerinitiative hat uns zugesagt, die Daten der BGB-Gesellschafter zu löschen.

Für die personenbezogenen Daten der Kommanditisten gilt § 28 Abs. 1 Satz 1 Nr. 3 BDSG. Danach ist das Erheben und Verarbeiten personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn die Daten allgemein zugänglich sind, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Da das Gesetz hier ein offensichtliches Überwiegen der berechtigten Interessen der Betroffenen fordert, ist das Speichern der Fondsbesitzerdaten sowie das Anschreiben dieser Personen (Datennutzung) noch rechtmäßig, sofern das Anschreiben keine Drohungen enthält. Demgegenüber überwiegen bei der Veröffentlichung der Kommanditistendaten die schutzwürdigen Interessen der Betroffenen. Die Veröffentlichung der Kommanditistendaten ist somit rechtswidrig. Hierbei ist zu berücksichtigen, dass die Liste der 150 Fondsbesitzer eine Prangerwirkung hat. Erschwerend kommt auch hinzu, dass in der Liste Fondsbesitzer, die in gutem Glauben die Fonds gekauft haben, mit denen in einer Liste auftauchen, die Mitverantwortung für den Bankenskandal tragen.

Bei der Veröffentlichung von Daten im Internet werden diese Daten zum Zwecke der Übermittlung gespeichert. Damit ist der Bewertung § 29 BDSG zugrunde zu legen. Soweit Daten von BGB-Gesellschaftern ins Internet eingestellt werden, ist dies wegen der rechtswidrigen Erhebung dieser Daten unzulässig, da nach § 29

Abs. 1 Satz 1 Nr. 1 BDSG Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Speicherung der Daten hat.

Das geschäftsmäßige Speichern von allgemein zugänglichen Daten – hier den Daten der Kommanditisten – ist nach § 29 Abs. 1 Satz 1 Nr. 2 BDSG zulässig, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Speicherung offensichtlich überwiegt. Bei der erforderlichen Abwägung ist zusätzlich zu dem oben Gesagten zu berücksichtigen, dass die Daten weltweit im Netz abrufbar sind, diese Daten könnten auch Straftäter (z. B. Entführer) interessieren, da man der Liste entnehmen kann, wer im großen Umfang Geld angelegt hat. Danach ist auch die Einstellung der Kommanditistendaten ins Internet rechtswidrig.

Erst recht ist die Übermittlung der Daten beim konkreten Abruf rechtswidrig. Formal fehlt es bereits an der Möglichkeit, das berechtigte Interesse des Abrufenden glaubhaft zu machen (§ 29 Abs. 2 Ziff. 1 a BDSG). Selbst wenn man dieses Erfordernis mangels Realisierbarkeit für Internet-Angebote nicht für anwendbar hielte, bliebe gleichwohl der Umstand, dass die Betroffenen ein schutzwürdiges Interesse am Ausschluss der Übermittlung haben.

Das Medienunternehmen, welches die Namensliste von Fondszeichnern ins Internet eingestellt hat, kann sich auf das Medienprivileg berufen. Soweit die Bürgerinitiative einen Link auf die Internet-Seite des Medienunternehmens gesetzt hat, haben wir darauf aufmerksam gemacht, dass das Setzen von Links selbst zwar noch keine Verarbeitung personenbezogener Daten darstellt, da dadurch keine (eigenen) Daten erhoben, verarbeitet oder genutzt werden. Setzt ein Anbieter jedoch bewusst einen Link, um den Nutzer auf bestimmte personenbezogene Daten hinzuführen, gegebenenfalls sogar durch eine entsprechende Kommentierung des Links unterlegt (Deep-Link), hat er nicht nur Kenntnis von diesen Daten, sondern will diese geradezu dem Nutzer verschaffen. Hier ist von der Verantwortlichkeit des Anbieters für die fremden Inhalte auszugehen und er ist so zu stellen, als würde er die Daten selbst veröffentlichen (§ 7 Abs. 1 Mediendienste-Staatsvertrag).

Wir haben der Bürgerinitiative empfohlen, die Daten der Fondsbesitzer zukünftig ausschließlich zum Anschreiben dieser Personen zu verwenden. Die Bürgerinitiative hat zugesagt, unsere Empfehlungen umzusetzen.

Unwirksame Einwilligungserklärung

Die Berliner Sparkasse möchte ihre Kreditkarten dadurch attraktiver machen, dass sie in Zusammenarbeit mit einem Bonussystemanbieter bestimmte Incentives verteilt. Die Sparkasse benutzte folgende Einwilli-

Nach Auskunft der Landesbank Berlin (LBB) wurde der Vorfall im Juni 2002 bekannt. Er beruht auf eine, im Hinblick auf den Datenschutz, ungeprüfte Übernahme einer Anwendungsempfehlung eines Vertrags-

gungserklärung: „Alle bei der Registrierung und im Rahmen der Nutzung der Karten anfallenden personenbezogenen Daten des Kunden („Daten") werden von der Bank gespeichert. Eine Löschung der Daten durch die Bank erfolgt, sobald die Teilnahme des Kunden am webmiles Programm endet. Die Speicherung der Daten erfolgt zu dem Zweck, die Kartenumsätze zu verbuchen und abzuwickeln. Sie erfolgt des Weiteren, um eine möglichst einfache und effiziente Teilnahme am webmiles Programm sowie die Inanspruchnahme der damit verbundenen Leistungen zu ermöglichen. Der Kunde erklärt sich ausdrücklich damit einverstanden, dass die Bank die bei der Registrierung und im Rahmen der Nutzung der Karten anfallenden Daten verarbeitet und nutzt und an webmiles übermittelt. Dies erfolgt jedoch ausschließlich zur Erfüllung der im vorstehenden Absatz genannten Zwecke. Der Kunde erklärt ausdrücklich, dass er die Erläuterungen zum webmiles Programm, insbesondere die hierauf anwendbaren Teilnahmebedingungen, zur Kenntnis genommen hat. Die hiermit erklärte Einwilligung des Kunden an die Speicherung, Verarbeitung, Nutzung und Übertragung der Daten ist völlig frei und kann jederzeit widerrufen werden."

Dieser Text befand sich in einem Fließtext, in dem auch die ergänzenden Bedingungen zu den Kreditkarten der Berliner Sparkasse dargestellt wurden. Auf der Rückseite des Textes sollte der Kreditkarteninhaber oben links unterschreiben.

Die *Einwilligungserklärung* war schon deshalb rechtswidrig, da nach § 126 BGB die Unterschrift unter die Urkunde, die Schriftform erfordert, gegeben werden muss, „eine Überschrift" auf der Rückseite der Urkunde genügt demgegenüber nicht. Die für die Datenschutzeinwilligung nach § 4 a letzter Satz BDSG erforderliche deutliche Hervorhebung fehlte. Die Überschrift „Datenschutz; Nutzung der Daten des Kunden durch die Bank und webmiles" ist missverständlich, da die Einwilligung nicht nur Nutzungen, sondern auch Übermittlungen von personenbezogenen Daten betrifft.

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. Danach sind die Daten der Teilnehmer zu löschen, wenn sie zur Erfüllung des Zwecks – hier also der Rabattierung – nicht mehr benötigt werden. Dass die Sparkasse nach der Datenschutzerklärung die Teilnehmerdaten erst mit Beendigung der Teilnahme des Kunden am webmiles-Programm löscht, verstößt gegen § 35 Abs. 2 Satz 2 Nr. 3 BDSG und eine entsprechende Einwilligung ist nach § 6 BDSG ebenfalls rechtswidrig.

Problematisch war bei der Einwilligungserklärung auch, dass sie aus sich heraus nicht verständlich war, sondern die Kenntnisnahme des Kunden von den Teilpartners. Bereits im August 2002 konnte im Einvernehmen mit dem Berliner Datenschutzbeauftragten ein gesetzeskonformer Zustand wieder hergestellt werden.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

nahmebedingungen von webmiles voraussetzte.

Plötzlich online

Eine Geschäftsfrau erteilte ihrem Sohn für das Geschäftskonto Kontovollmacht. Sie legte Wert darauf, dass mit ihrem Geschäftskonto kein Online-Banking betrieben werden kann, da sie Sicherheitsbedenken hatte. Ihr Sohn hat bei der Bank ein eigenes Konto, bei dem er antragsgemäß die Möglichkeit zu Telefon- und Online-Banking hat. Dies führte automatisch dazu, dass er auch mit dem Konto seiner Mutter Online-Banking betreiben konnte.

Der Bankkunde muss das Recht haben zu bestimmen, ob er am *Online-Banking* teilnehmen möchte oder nicht. Die Tatsache, dass der Inhaber einer Bankvollmacht auf einem eigenen Konto Online-Banking betreibt, darf nicht dazu führen, dass die Vollmachtgeber praktisch dazu gezwungen werden, ihr eigenes Konto online zu betreiben.

Die Bank sah sich nicht im Stande, die Möglichkeit des Online-Banking bei Bankkunden mit mehreren Konten bzw. Kontovollmachten auf einzelne Konten zu beschränken. Allerdings werden zukünftig Vollmachtgeber bei der Erteilung einer Vollmacht auf die Möglichkeit hingewiesen, dass der Bevollmächtigte die Möglichkeit zum Online-Banking auch dann haben kann, wenn der Vollmachtgeber selbst darauf verzichtet hat.

Der Senat hat den beschriebenen Sachverhalt zum Anlass genommen zu prüfen, ob diese Möglichkeit auch für die öffentlich rechtliche Landesbank Berlin zutrifft. Nach den vorliegenden Erkenntnissen, ist ein unberechtigter Onlinezugriff bei der LBB nicht möglich, da die Internetberechtigung für jedes Konto einzeln beantragt werden muss.

Ombudsmann für Versicherungen

Mit dem Versicherungsombudsmann hat die Versicherungswirtschaft seit dem 1. Oktober 2001 eine außergerichtliche Schlichtungsstelle geschaffen. Der betroffene Versicherer ist an die Entscheidung des Ombudsmanns bis zu einem Beschwerdewert von 5000 € einseitig gebunden, nicht dagegen der Verbraucher (Versicherungsnehmer), dem auch nach seiner Beschwerde der Weg zum Gericht offen steht. Bei dem „eigentlichen" Ombudsmann für Versicherungen arbeiten sechs Mitarbeiter, in dem angeschlossenen Call-Center, welches juristisch selbstständig ist, arbeiten derzeit zwölf Mitarbeiter. Das Call-Center ist als eine Art Front-Office für die Vorgangserstbearbeitung zuständig. Betroffene wenden sich per E-Mail, Fax, schriftlich und telefonisch mit Eingaben an das Call-Center. Dieses prüft die Zuständigkeit und fordert bei entsprechendem Bedarf weitere Unterlagen von dem Versicherten an. Wir haben der im Aufbau begriffenen Einrichtung verschiedene datenschutzrechtliche Hinweise gegeben.

Sowohl für den *Ombudsmann für Versicherungen* als auch für das Call-Center wurden auf unsere Initiative hin betriebliche Datenschutzbeauftragte bestellt. Da die Call-Center-Mitarbeiter Daten nach festen Vorgaben des Ombudsmanns erheben und verarbeiten, ist die

Arbeit des Call-Centers als Auftragsdatenverarbeitung anzusehen. Wir haben den Ombudsmann darauf hingewiesen, dass bei Auftragsdatenverarbeitung nach § 11 Abs. 2 Satz 2 BDSG ein schriftlicher Auftrag vorliegen muss. Für den Bürger, der sich an das Call-Center wendet, sollte transparent sein, dass er sich nicht direkt an den Ombudsmann wendet.

Der Ombudsmann erhebt, verarbeitet und nutzt die Daten der Betroffenen, soweit dies im Rahmen des vertragsähnlichen Vertrauensverhältnisses erforderlich ist. Originalunterlagen werden kopiert und zurückgesandt, ebenso zu viel übersandte Unterlagen. Die Datenerhebung, Verarbeitung und Nutzung der personenbezogenen Daten des Betroffenen ist nach § 28 Abs. 1 Nr. 1 BDSG rechtmäßig (vertragsähnliches Vertrauensverhältnis). Falls von dem Betroffenen weitergehende Daten angefordert werden, da seine Eingabe ansonsten nicht bearbeitet werden kann, wird dem Betroffenen eine Einwilligungserklärung zugeleitet. In diesem Fall läuft die Datenerhebung, Verarbeitung und Nutzung nicht mehr über § 28 BDSG, sondern nach §§ 4, 4 a BDSG.

Bezüglich der Verarbeitung sensitiver Daten verweisen wir auf Kapitel 3.2.

Wenn der Versicherte Daten über Dritte übermittelt, wie etwa Name, Anschrift und eventuell gesundheitliche Schädigung in einem Haftpflichtfall, ist der Dritte nach § 33 Abs. 1 BDSG hiervon zu unterrichten. Bei der Frage, wie lange Eingaben gespeichert werden dürfen, ist § 35 Abs. 2 Satz 2 Nr. 3 BDSG zu beachten. Danach 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. Der Ombudsmann speichert auch nach Beantwortung der Beschwerde Vorgänge weiter, da

- auch nach Beendigung eines Verfahrens häufig Nachfragen der Betroffenen zu erwarten sind, auch werden Eingaben teilweise sogar wiederholt,

- der Ombudsmann ein Interesse daran hat, eine kontinuierliche „Rechtsprechung" bei seiner Arbeit zu dokumentieren und

- die Vorgänge für statistische Zwecke benötigt würden.

Die weitere Aufbewahrung von Daten kann nicht allein mit statistischen Zwecken begründet werden. Allerdings müssen Daten erst gelöscht werden, wenn sie im operativen Geschäft nicht mehr benötigt werden. Solange der Ombudsmann damit rechnen muss, dass Nachfragen gestellt werden, befinden sich die Vorgänge im operativen Geschäft und müssen nicht gelöscht werden. Soweit der Ombudsmann Vorgänge benötigt,

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

um die Kontinuität seiner „Rechtsprechung" zu sichern, haben wir empfohlen, von der Möglichkeit nach § 35 Abs. 3 Nr. 1 BDSG Gebrauch zu machen und sich satzungsmäßige Aufbewahrungsfristen aufzuerlegen. Der Ombudsmann wird diese Empfehlung prüfen.

4.6.2 Kreditinformationen

Berechtigtes Interesse

Eine Übermittlung personenbezogener Daten von einer *Wirtschaftsauskunftei* an einen Kunden setzt ein berechtigtes Interesse des Datenempfängers an der Kenntnis dieser Daten voraus. Zur Glaubhaftmachung des berechtigten Interesses müssen die Kunden der Auskunfteien Anfragegründe benennen. Wiederholt haben wir Auskunfteien darauf hingewiesen, dass Anfragegründe wie „Bonitätsprüfung" oder „Geschäftsanbahnung" nicht ausreichend sind, um ein berechtigtes Interesse des Kunden an der gewünschten Datenübermittlung darzulegen. Die „Geschäftsanbahnung" ist etwa dann kein Grund für eine Beauskunftung, wenn das Geschäft sofort abgewickelt wird und der Kunde der Auskunftei nicht in Vorleistung treten muss. Das Schlagwort „Bonitätsprüfung" erläutert nur den Wunsch des Kunden, stellt aber keinen Grund im Sinne des § 29 Abs. 2 BDSG dar.

Bei der Vielzahl der Anfragen sind die Auskunfteien nicht in der Lage, das berechtigte Interesse ihrer Kunden in jedem Einzelfall zu überprüfen. Die Auskunfteien haben sich aber gegenüber den Aufsichtsbehörden verpflichtet, bei zwei Promille der Auskunftsbegehren das berechtigte Interesse ihrer Kunden zu überprüfen. Bei dieser Vereinbarung waren die Aufsichtsbehörden davon ausgegangen, dass die Auskunfteien eine substanziierte Prüfung vornehmen. Bei zwei Kontrollen in Berliner Auskunfteien stellten wir fest, dass dies nicht der Fall ist.

An Kunden, die überprüft werden, versenden die Auskunfteien ein Formular, in dem Angaben zu dem berechtigten Interesse des Kunden gemacht werden sollen. In dem Formular werden die Kunden u. a. gebeten, schriftliche Unterlagen über das der Anfrage zugrunde liegende Vertragsverhältnis zu übersenden. In keinem Fall haben die Auskunfteien nach der Zurücksendung des Fragebogens eine Notwendigkeit darin gesehen, noch einmal „nachzuhaken". Die zurückgesandten Fragebögen wurden nur abgeheftet, nicht aber überprüft. In einigen Fällen, wie etwa bei einer hohen Bürgschaft oder einem Millionendarlehen einer Bank, übersandten die Kunden keinerlei schriftliche Unterlagen, obwohl nicht davon ausgegangen werden kann, dass hier keine schriftlichen Vertragsbeziehungen vorliegen. Dies wurde von der überprüften Auskunftei ebenso wenig gerügt wie die Zusendung eines Vertrages, der „aus Datenschutzgründen" anonymisiert wurde und somit keinerlei Beweiswert hatte.

Der Senat bzw. die bezirklichen Wirtschaftsämter sind in diesem Sachzusammenhang nicht als Beteiligte anzusehen, da sie keine spezifische Aufsichtsfunktion über Auskunfteien besitzen.

Umstritten zwischen Auskunfteien und Aufsichtsbehörden ist die Frage, unter welchen Voraussetzungen Negativdaten von dem Inkassobereich der Auskunfteien bzw. von Auskunfteikunden über deren Schuldner an die Auskunfteien übermittelt und bei diesen gespeichert werden dürfen. Bei dieser Frage sind die berechtigten Interessen eines Kreditinformationssystems und potentieller Gläubiger abzuwägen gegen die schutzwürdigen Interessen der Schuldner (§ 28 Abs. 3 Nr. 1 und § 29 Abs. 1 Nr. 1 BDSG). Den Auskunfteien ist zuzugestehen, dass eine Einmeldung erst bei Vorliegen eines Titels dazu führen würde, dass ein Informationssystem nicht rechtzeitig schlechte Schuldner erkennt. Auf der anderen Seite kann auch aus mehreren Mahnbescheiden, die gegen einen Schuldner erlassen werden, nicht automatisch auf eine schlechte Bonität des Schuldners geschlossen werden, wie dies von dem Verband der Handelsauskunfteien behauptet wird. Eine (fällige) Forderung sollte danach nur dann an ein Informationssystem gemeldet und dort gespeichert werden, wenn sich aus den Gesamtumständen ergibt, dass die Nichtbegleichung der Forderung auf Zahlungsunwilligkeit oder Zahlungsunfähigkeit beruht.

Bonitätsprüfung bei Internet-Spielzeughändler

Bei einem Berliner Internet-Spielzeughändler werden Kunden, die Spielzeuge in einen bestimmten virtuellen Warenkorb gelegt haben und hierdurch ihre Kaufabsicht signalisiert haben, im Auftrag des Händlers von einer Auskunftei überprüft. Nach der Überprüfung erhält der Betroffene die Information, ob das Unternehmen bereit ist, mit ihm einen Kaufvertrag abzuschließen, und welche Zahlungsart in Frage kommt.

Eine *Bonitätsabfrage* ist nach § 29 Abs. 2 Nr. 1 a BDSG nur rechtmäßig, wenn der Dritte ein berechtigtes Interesse an der Kenntnis der Bonitätsdaten hat, etwa weil er gegenüber dem Betroffenen vertraglich in Vorleistung tritt. Wenn ein Kunde Spielzeuge in den Warenkorb gelegt hat, hat er ein gewisses Interesse an dem Abschluss eines Kaufvertrages signalisiert. Es ist aber schon zweifelhaft, ob zum Zeitpunkt der Abfrage ein für das berechtigte Interesse erforderlicher Bindungswille des Kunden vorhanden ist, solange noch nicht ein wichtiger Punkt des Vertrages, nämlich die Zahlungsmodalität, dem Kunden bekannt ist und er mit dieser einverstanden ist.

Geht der Online-Verkäufer gegenüber einem Kunden ein kreditorisches Risiko ein, hat er ein Interesse, sich über die Bonität seines Kunden zu informieren. Ist im Falle eines Vertragsabschlusses die Bestellung per Rechnung beabsichtigt, trägt das Online-Unternehmen für den Fall mangelnder Zahlungswilligkeit oder Zahlungsfähigkeit des Kunden das Ausfallrisiko. Wird demgegenüber eine Zahlung per Nachnahme vereinbart, ist kein Bonitätsrisiko gegeben und eine Abfrage von Bonitätsdaten damit rechtswidrig. Bei Nachnah-

mesendungen kann sich der Internet-Verkäufer nicht darauf berufen, dass durch die Bonitätsüberprüfung die Zahl der Kunden verringert werden soll, die bei Ankunft der Ware den Vertrag widerrufen. Nach den neu ins BGB aufgenommenen Regelungen zu Fernabsatzverträgen (§§ 312 d, 355 BGB) wird dem Kunden ein Widerrufsrecht eingeräumt. Der Gesetzgeber geht also grundsätzlich davon aus, dass der Händler das Risiko dafür trägt, dass sich der Kunde innerhalb eines gesetzlich gesetzten Rahmens auf sein Widerrufsrecht berufen kann, der Händler also insoweit einen risikobehafteten Vertrag abgeschlossen hat. Ob der Internet-Händler bei dem Kauf per Kreditkarte ein Bonitätsrisiko trägt, hängt davon ab, ob das Kreditkartenunternehmen dem Händler (ausnahmsweise) das Bonitätsrisiko auferlegt hat.

Wir haben dem Unternehmen empfohlen, erst nach Festlegung der Zahlungsart bei den risikobehafteten Zahlungsmodalitäten eine Bonitätsprüfung vorzunehmen.

Die *SCHUFA* hat die Zusage, die rechtswidrige negative Beeinflussung des Score-Wertes durch Selbstauskünfte zu beenden, am 1. Juli 2002 erfüllt. Wir haben gegenüber der SCHUFA deutlich gemacht, dass wir davon ausgehen, dass auch die Ausübung sonstiger datenschutzrechtlicher Rechte der Betroffenen (z. B. Berichtigung, Sperrung) nicht in den Scoring-Wert einfließen.

Die SCHUFA hat entschieden, zukünftig wieder Vermieter an ihrem Kreditinformationssystem zu beteiligen. Die Prüfung dieses neuen Verfahrens wird von der für die SCHUFA örtlich zuständigen Aufsichtsbehörde, dem Hessischen Ministerium des Innern und für Sport, vorgenommen. Nach der SCHUFA-Klausel zu Mietanträgen melden die Vermieter Daten aufgrund nichtvertraglichen Verhaltens an die SCHUFA ein. Nach dieser Formulierung würde nicht nur ein Forderungsbetrag nach Kündigung eingemeldet, sondern auch sonstiges nicht vertragsgemäßes Verhalten. Insbesondere besteht die Gefahr, dass Mieter eingemeldet werden, die wegen der Geltendmachung von Sachmängeln oder eines Streits bezüglich der Betriebskostenabrechnung einen Prozess gegen den Vermieter (teilweise) verloren haben und dieser dadurch einen Titel in Höhe der zu Unrecht erfolgten Minderung gegen den Vermieter erlangt hat.

Schätzdaten

Wir berichteten darüber, dass Auskunfteien nicht gekennzeichnete *Schätzdaten* verwenden, die sich nach dem Branchendurchschnitt richten, wenn ihnen die konkreten Zahlen des Unternehmens nicht bekannt sind[93]. Unserer Forderung, die Schätzdaten als solche

[93] JB 2000, 4.6.2

zu kennzeichnen, sind die Auskunfteien bisher nicht nachgekommen. Allerdings haben sie sich nun bereit erklärt, zukünftig bei jeder Auskunft den Hinweis zu geben, dass sich in dem Datenbestand eines Unternehmens auch statistische Daten befinden können.

4.6.3 Verbraucher- und Jugendschutz

Der Europranger

Auf der Website der Verbraucherzentrale Bundesverband (www.preis-wert-forum.de) wird von der Verbraucherzentrale Nordrhein-Westfalen eine vom Bundesministerium für Verbraucherschutz, Ernährung und Landwirtschaft geförderte Maßnahme gegen „Euro-Sünder" durchgeführt. Verbraucher haben dort die Möglichkeit, Unternehmen einzumelden, die die Einführung des Euros zu versteckten Preiserhöhungen ausgenutzt haben. Soweit die Anschuldigung des Verbrauchers plausibel ist, wird sie ins Internet eingestellt. Allerdings hat das Unternehmen Gelegenheit, zu der Behauptung des Verbrauchers eine Gegenstellungnahme abzugeben.

Bei der Veröffentlichung von Daten von *„Euro-Sündern"* im Internet werden diese Daten zum Zwecke der Übermittlung gespeichert. Damit ist der Bewertung § 29 BDSG zugrunde zu legen, soweit sich die in dem Verbraucherforum benannten Unternehmen auf natürliche Personen beziehen (Friseurbetriebe, Werkstätten, Gastronomieunternehmen etc.). Die Speicherung zum Zwecke der Übermittlung ist zulässig bei fehlendem schutzwürdigem Interesse des Betroffenen an dem Ausschluss der Erhebung oder Speicherung sowie bei Daten aus allgemein zugänglichen Quellen, wenn nicht das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung oder Speicherung offensichtlich überwiegt (§ 29 Abs. 1 Nr. 1 und 2 BDSG).

Bei der Bewertung der ins Internet eingestellten Liste ist zu berücksichtigen, dass Deutschland anders als andere Länder der Euro-Zone darauf verzichtet hat, zu Beginn der Euro-Einführung Anfang 2002 Preiserhöhungen zu verbieten. In Politik und Wirtschaft wurde die Meinung vertreten, dass der Markt schon dafür sorgen würde, dass der Euro nicht zur Durchsetzung von Preiserhöhungen genutzt wird. Obwohl einige Verbandsfunktionäre zugesagt hatten, dass die Unternehmen die Euro-Umstellung nicht zu Preiserhöhungen ausnutzen würden, sind diese Zusagen unverbindlich.

Auch wenn das Verbraucherforum das Ziel verfolgt, die Bereitschaft der Kundinnen und Kunden zu Preisbeobachtungen und Preisvergleichen zu entwickeln, ändert dies nichts daran, dass die Aufnahme eines Unternehmers in diese Liste Prangerwirkung hat.

Bei einem Hinweis eines Verbrauchers – es könnte sich auch um den Hinweis eines Konkurrenten handeln – ist

der Unternehmer auch dann, wenn er kein „Euro-Sünder" ist, gezwungen, sich durch eine Gegenstellungnahme zu rechtfertigen. Häufig steht dann Aussage gegen Aussage und für den Leser der Liste entsteht der Eindruck, dass viele Unternehmen mit Hilfe von Schutzbehauptungen ihre „Euro-Sünde" leugnen wollen. Trotz der von der Verbraucherzentrale vorgenommenen Überprüfung wird man nicht ausschließen, dass Verbraucher – nicht unbedingt vorsätzlich – falsche Angaben machen, die dann schwer zu entkräften sind.

Teilweise wird es sich bei den Preisangaben um allgemein zugängliche Daten handeln. Aber auch die Speicherung dieser Daten ist rechtswidrig, da die schutzwürdigen Interessen des Betroffenen an dem Ausschluss der Speicherung in einer Liste mit Prangerwirkung offensichtlich überwiegen. Bei der Abwägung ist auch zu berücksichtigen, dass die Daten weltweit im Netz abrufbar sind. Erst recht ist die Übermittlung beim konkreten Abruf rechtswidrig. Formal fehlt es bereits an der Möglichkeit, das berechtigte Interesse des Abrufenden glaubhaft zu machen (§ 29 Abs. 2 Ziff. 1 a BDSG). Zweifelhaft ist schon, ob der Verbraucher in Berlin ein berechtigtes Interesse daran hat, Informationen über einen Friseurbetrieb in Bad Wiessee zu erhalten. Es kann aber auch nicht ausgeschlossen werden, dass der Abfragende (z. B. ein Konkurrent) die Informationen für sachfremde Zwecke verwendet.

Zigarettenautomaten

Nach der Novellierung des Jugendschutzgesetzes (JuSchG) dürfen Tabakwaren nur noch dann in Automaten angeboten werden, wenn Kinder und Jugendliche zu dem Automaten keinen Zugang haben oder durch technische Vorrichtungen oder durch ständige Aufsicht sichergestellt ist, dass Kinder und Jugendliche unter 16 Jahren Tabakwaren nicht entnehmen können (§ 10 JuSchuG)[94]. Da die Unzugänglichkeit des Ortes sowie die ständige Aufsicht der aufgestellten Automaten eher die Ausnahme sind, müssen Automatenhersteller ab 2003 bei neuen Automaten die geforderten technischen Vorrichtungen schaffen. Bis zum 31. Dezember 2006 müssen alle derzeit in Betrieb befindlichen Automaten entfernt werden (§ 29 JuSchuG).

Das neue *Jugendschutzgesetz* führt dazu, dass bei neuen *Zigarettenautomaten* eine Bargeldbezahlung nicht mehr möglich ist. Zahlungsmittel ist zukünftig die ec-Karte mit Geldkartenzusatzfunktion. Allerdings enthält die ec-Karte bisher keine Informationen über das Alter des Karteninhabers. Ein Wirtschaftsberatungsunternehmen des Bundesverbandes Deutscher Tabakwarengroßhändler und Automatenhersteller e. V. schlug vor, zukünftig alle ec-Karten mit einem Geburtsdatum zu versehen, welches dann von dem Zigarettenautomaten

[94] BGBl. I 2002, S. 2730

ausgelesen werden könne. Neukunden sollten in die Verwendung dieses Datums einwilligen, Altkunden sollten hierüber aus Praktikabilitätsgründen nur informiert werden, etwa als Information zu einem Kontoauszug. Diese hätten dann die Möglichkeit, Widerspruch gegen die Aufnahme des Geburtsdatums auf den Geldkartenchip einzulegen.

Für den Zweck, Zigarettenkäufe von Jugendlichen unter 16 Jahren zu verhindern, ist es nicht erforderlich, bei jeder ec-Karte das Geburtsdatum auf den Geldkartenchip einzutragen. Dies entspricht weder dem Erforderlichkeitsgrundsatz nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG noch dem Grundsatz der Datenvermeidung und Datensparsamkeit (§ 3 a BDSG). Auch kann nicht davon ausgegangen werden, dass Neukunden, die nach Erhalt der Information von der Verwendung des Geburtsdatums bei Geldkarten schweigen, konkludent hierin einwilligen.

Am datensparsamsten wäre es, lediglich die Karten der Minderjährigen mit dem Datum zu versehen, ab dem der Inhaber der Karte volljährig wird, und nur die Karten der Minderjährigen mit einer Zugangssperre zu belegen. Dies wäre allerdings nur dann eine mögliche Lösung der Problematik, wenn sich alle Banken daran halten würden, bei Kindern und Jugendlichen unter 16 Jahren das Geburtsdatum auf den Chip aufzunehmen. Der Zentrale Kreditausschuss sah sich allerdings nicht in der Lage, hierfür eine Gewähr abzugeben.

Gemäß dem von uns vorgeschlagenen Kompromissvorschlag werden die Banken die ec-Karten der über 16-Jährigen als „Erwachsenenkarten" ausgestalten, die mit einem Legitimationsvermerk versehen sind, der zum Zigarettenkauf an Automaten berechtigt. Demgegenüber enthält die Chipkarte bei Kindern und Jugendlichen unter 16 Jahren das Geburtsdatum, der Jugendliche bzw. der Erziehungsberechtigte muss hierzu seine Einwilligung erteilen. Soweit technisch möglich, wird sich die Karte des Jugendlichen nach Erreichen der Altersgrenze in eine Erwachsenenkarte „verwandeln".

4.6.4 Verkehrsunternehmen

Die Deutsche Bahn AG ist das größte Unternehmen in unserem Zuständigkeitsbereich. Naturgemäß gelangt so eine Vielzahl von Datenschutzproblemen auf unseren Schreibtisch.

Fahrpreiserstattung nur gegen Kundendaten

Mehrfach erreichten uns Beschwerden von Kunden, die sich gegen die Datenverarbeitungspraxis der Deutschen Bahn AG bei der Erstattung des Fahrpreises für nicht oder nur teilweise genutzte Fahrkarten wendeten. Die Deutsche Bahn AG verlangte im „Antrag Fahrpreiserstattung" Angaben der Kunden zum Familiennamen, Vornamen, Adresse, Telefonnummer und zur

Bankverbindung. In einem weiteren Vordruck hatte der Kunde die Gründe anzugeben, aus denen er die Fahrt nicht angetreten hat. Wurde die Fahrt mit dem Auto getätigt, hatte er den Halter des Fahrzeuges anzugeben. Die Angaben dazu mussten vom Halter durch Unterschrift bestätigt werden. Alternativ dazu hatte der Antragsteller eine Krankenbescheinigung, eine Mietwagenabrechnung oder eine eisenbahnseitige Bescheinigung als Nachweis für die Nichtnutzung des Fahrscheins vorzulegen. War er dazu nicht in der Lage, hatte er eine entsprechende Erklärung abzugeben.

Der „Gemeinsame Internationale Tarif" der Eisenbahnen von 2002 verlangt, dass dem Erstattungsantrag „entsprechende Beweisstücke beigefügt werden (Krankheitsbescheinigung oder neue Fahrscheine, die anstelle der nicht benutzten Fahrscheine gekauft wurden usw.)".

Durch den Erwerb eines Fahrscheines hat der Fahrgast mit der Deutschen Bahn AG einen Vertrag über die Personenbeförderung mit Wirkung vom ersten Gültigkeitstag der Fahrkarte an geschlossen. Kann er das Beförderungsangebot der Deutschen Bahn AG nicht wahrnehmen, indem er die Reise nicht antritt, hat er nach § 18 Abs. 1 Eisenbahn-Verkehrs-ordnung (EVO) einen Rechtsanspruch auf eine *Fahrpreiserstattung*. Diese ist somit Teil der Rückabwicklung des mit der Deutschen Bahn AG geschlossenen Personenbeförderungsvertrages. Die Identifikationsmerkmale bei Überweisung des Betrages – ebenso wie die Bankverbindung – werden in jedem Fall benötigt, die Telefonnummer für Nachfragen. Für die Rückabwicklung unerlässlich sind Angaben zu dem Fahrschein und Berechnungsgrößen für den Erstattungsbetrag und die Art der Auszahlung. Da § 18 Abs. 1 EVO die Rückerstattung des Fahrpreises für bestimmte Fälle – nämlich die Nichtbenutzung und die teilweise Benutzung – festlegt, dient auch die Frage nach dem Grund der Erstattung bzw. nach Bemerkungen des Kunden der Zweckbestimmung des Vertragsverhältnisses und ist für dessen Rückabwicklung erforderlich. Die Erhebung und weitere Verarbeitung der Daten im „Antrag Fahrpreiserstattung" als Mittel für die Erfüllung eigener Geschäftszwecke der Deutschen Bahn AG kann auf § 28 Abs. 1 Nr. 1 BDSG gestützt werden und ist zulässig.

Anders verhält es sich mit der Erhebung von Kundendaten im gesonderten Vordruck zur Nachweisführung der Nichtbenutzung oder teilweisen Nutzung der Fahrkarte.

Bei der als Nachweis geforderten Krankenbescheinigung handelt es sich um sensitive Daten (§ 3 Abs. 9 BDSG). Die Erhebung dieser Daten ist für eigene Geschäftszwecke nur unter den in § 28 Abs. 6 BDSG

genannten Voraussetzungen zulässig[95]. Keine der dort genannten Tatbestandsalternativen kommt hier in Betracht. Die Erhebung und weitere Verarbeitung dieser Kundendaten zur Nachweisführung der Nichtbenutzung oder teilweisen Nutzung der Fahrkarte ist daher unzulässig. Bei den Daten über den Kfz-Halter/Zeugen handelt es sich um die Daten eines Dritten, der nicht zu den Vertragsparteien gehört. Unabhängig davon haben sich die Datenmenge und die Intensität der Datenverarbeitung am Vertragszweck und seiner Bedeutung zu orientieren. Für die Rückabwicklung des Personenbeförderungsvertrages sind die von der Deutschen Bahn AG mit dem Vordruck „Antrag Fahrpreiserstattung" erhobenen Daten ausreichend. Weitere Daten des Kunden sind dafür nicht erforderlich und unter Zugrundelegung des Vertragszweckes auch nicht verhältnismäßig.

Auch § 28 Abs. 1 Nr. 2 BDSG kann nicht als Rechtsgrundlage herangezogen werden. Unstreitig kann die von der Deutschen Bahn AG vorgetragene beabsichtigte Reduzierung von Einnahmeverlusten durch Schwarz- und Graufahrer als ein berechtigtes (wirtschaftliches) Interesse der Deutschen Bahn AG angesehen werden. Es ist jedoch davon auszugehen, dass die betrügerische Rückgabe nicht entwerteter Fahrscheine nach Inanspruchnahme der Fahrt (Graufahrer) gegenüber dem Fahren ohne Fahrausweis (Schwarzfahrer) eher die Ausnahme darstellt. Hinzu kommt, dass die Erklärung des Kunden zur Nachweisführung, die dieser mit Vor- und Zunamen abzugeben und zu unterschreiben hat, als „psychologische Hürde" dazu führen kann, dass Kunden auf die Rückerstattung des Fahrpreises verzichten, obwohl sie die Fahrt tatsächlich nicht angetreten haben und einen Anspruch auf Rückerstattung des Fahrpreises hätten.

Die Datenerhebung im Vordruck zur Nachweisführung der Nicht- bzw. teilweisen Nutzung des Fahrscheins konnte somit weder auf die Einwilligung des Kunden noch auf eine Rechtsgrundlage gestützt werden und war unzulässig. Entsprechend unserer Empfehlung hat die Deutsche Bahn AG das Verfahren geändert. Der Vordruck zum Nachweis der Nichtnutzung oder teilweisen Nutzung der Fahrkarte wurde unverzüglich eingezogen und vom Markt genommen. Der Kunde hat auf dem Fahrpreiserstattungsantrag zukünftig lediglich pauschal zu bestätigen, dass er die Fahrkarte nicht nutzen konnte, weil er mit dem PKW gefahren, weil er erkrankt oder aus anderen Gründen gehindert gewesen sei. Weitere Nachweise bzw. zusätzliche Einzelangaben des Kunden werden von der Deutschen Bahn AG zukünftig nicht mehr verlangt.

Auch die Bestimmungen des „Gemeinsamen Internationalen Tarifs", dem die Deutsche Bahn AG neben anderen Eisenbahnunternehmen in der EU und in Dritt-

[95] vgl. 3.1

staaten unterliegt, rechtfertigen nicht die Erhebung und Übermittlung von Krankheitsbescheinigungen und Angaben Dritter (Fahrzeughalter). Der „Gemeinsame Internationale Tarif" benennt Krankheitsbescheinigungen nur beispielhaft und lässt dem Anwender den Spielraum für andere Nachweise für den Nichtantritt der Bahnfahrt bei Fahrpreiserstattung. Die Deutsche Bahn AG muss die internationalen Bestimmungen „im Lichte" des BDSG auslegen und darf Krankheitsbescheinigungen und Daten Dritter nicht an ausländische Eisenbahnunternehmen zu dem Zweck weitergeben, die Zahlung des für die ausländische Bahnstrecke bereits an den Kunden erstatteten Fahrpreises nachzuweisen.

bahn.comfort, das Serviceprogramm für Vielfahrer

Jeder Bahncard-Kunde hat die Möglichkeit, zusätzlich am bahn.comfort-Service teilzunehmen. Wer sich in einem bestimmten Zeitraum als „Vielfahrer" qualifiziert, erhält von der Bahn bestimmte Incentives, wie bessere Sitzplatzreservierungsmöglichkeiten, Zugang zu den Erste-Klasse-DB-Lounges usw. Bei jeder einzelnen Fahrkarte kann der Kunde auswählen, ob er diese Fahrt für den bahn.comfort-Service verwenden will. Bei Kunden des Vielfahrerprogramms werden von der Bahn neben den gesammelten Punkten zusätzlich die personenbezogenen Reisedaten auf der Fahrkarte (Ticketart, Kaufdatum und -ort, Gültigkeitsbeginn, Start- und Zielbahnhöfe) erhoben und gespeichert.

Der von der Deutschen Bahn AG gespeicherte Datensatz ist nicht unproblematisch, da er die Erstellung von Bewegungsprofilen von einzelnen *bahn.comfort-Kunden* ermöglicht. Da die bahn.comfort-Kunden keine spezielle Einwilligungserklärung unterschreiben, darf die Deutsche Bahn AG beim bahn.comfort-Programm die personenbezogenen Daten der Kunden nur in dem Umfang erheben, speichern und nutzen, in dem dies zur Umsetzung des Bonussystems erforderlich ist. Ein Kunde, der bewusst an einem Bonussystem teilnimmt, muss damit rechnen, dass die bonusgewährende Stelle alle bonusrelevanten Daten speichert.

Wir haben gegenüber der Deutschen Bahn AG durchgesetzt, dass die im Rahmen des bahn.comfort-Programms erhobenen Daten ausschließlich zur Durchführung des Rabattsystems sowie für Clearing-Zwecke verwendet werden. Demgegenüber werden diese Daten nur in anonymisierter Form für Marketingzwecke verwendet, nicht jedoch zum Aufbau eines personenbezogenen Data-Warehouse/Data-Mining-Programms[96].

Nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG sind personenbezogene Daten zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr

[96] JB 2000, 4.6.3

erforderlich ist. Wenn die Daten nach Ablauf eines noch zu bestimmenden Zeitraums nicht mehr benötigt werden, etwa weil der Kunde über die angesparten Bonuspunkte informiert wurde und innerhalb eines bestimmten Zeitraumes keinen Einspruch eingelegt hat, können die Reisedaten gelöscht werden.

Aushang über „Schwarzfahrer"

Ein Bürger informierte uns darüber, dass im „Weisungsraum" eines Bahnhofsgebäudes die Kopie einer Fahrpreisnacherhebung ausgehängt war. Der Aushang enthielt Angaben zu Namen, Vornamen, Geschlecht, Geburtsdatum, Personalausweisnummer und Wohnort des Betroffenen. Beigefügt war die Anmerkung: „Bei Antreffen der Person ohne gültigen Fahrschein ist der BGS zu verständigen. Wiederholungstäter!"

Datenschutzrechtlich handelt es sich bei einem derartigen Aushang mit personenbezogenen Daten um eine Übermittlung der Daten an diejenigen Personen, die durch Ansicht Kenntnis von den Daten nehmen können. Wir haben die Deutsche Bahn AG darüber informiert, dass eine derartige Datenübermittlung unzulässig ist. Der Aushang wurde umgehend entfernt und vernichtet. Die MitarbeiterInnen wurden auf die datenschutzrechtliche Unzulässigkeit dieser Maßnahme hingewiesen und es erging eine Anweisung, derartige Aushänge über *„Schwarzfahrer"* in der Zukunft nicht mehr anzubringen.

Auch andere Verkehrsunternehmen haben Datenschutzprobleme.

Identität von „Schwarzfahrern"

Immer wieder erreichen uns Eingaben, in denen sich Betroffene über die Datenerhebungen der Berliner Verkehrsbetriebe (BVG) zu „Schwarzfahrern" bei Fahrscheinkontrollen beschweren. Der konkrete Anlass der Beschwerden ist vielfach das Verfahren der Identitätsfeststellung durch die Mitarbeiter der BVG bzw. der Polizei. Wir haben dies zum Anlass genommen, die bestehende Praxis umfassend datenschutzrechtlich zu überprüfen.

Nach den Tarifregelungen hat die BVG einen Anspruch auf die Entrichtung eines erhöhten Beförderungsentgeltes, wenn der Fahrgast keinen gültigen Fahrausweis besitzt oder ihn bei einer Kontrolle nicht vorzeigen kann. Der Kontrolleur nimmt in diesem Fall die personenbezogenen Daten des „Schwarzfahrers" in den dafür vorgesehenen Vordruck auf. Führt der Betroffene keine Ausweispapiere mit sich, werden die von ihm angegebenen Personalien regelmäßig telefonisch mit den Angaben im Melderegister des Landeseinwohneramtes Berlin abgeglichen.

Der Kontrolldienst der BVG informiert den Bereichsleiter auf dem BVG-Stützpunkt mittels Handy und lässt die Angaben des Fahrgastes durch diesen beim Landeseinwohneramt überprüfen. Auf die telefonische Anfrage des Bereichsleiters, ob die Angaben des Fahrgastes zu Namen, Vornamen, Geburtsdatum und vollständiger Anschrift im Melderegister registriert sind, teilt das Landeseinwohneramt als Antwort lediglich ein „Ja" oder „Nein" mit. Der Bereichsleiter setzt den Mitarbeiter des Kontrolldienstes vor Ort telefonisch über das Ergebnis seiner Nachfrage in Kenntnis.

Die Übermittlung der Daten vom Landeseinwohneramt an die BVG ist datenschutzrechtlich zulässig. Nach § 25 Abs. 1 MeldeG darf das Landeseinwohneramt einer anderen Behörde oder sonstigen öffentlichen Stelle (der BVG als Anstalt des öffentlichen Rechts) die in § 2 Abs. 1 MeldeG genannten Daten aus dem Melderegister übermitteln. Dazu zählen auch Angaben zum Familiennamen, Vornamen, Tag und Ort der Geburt und zu den gegenwärtigen und früheren Anschriften von Haupt- und Nebenwohnung. Die Bestätigung des Landeseinwohneramtes auf die telefonische Anfrage der BVG geht nicht über den in § 2 Abs. 1 MeldeG genannten Datenkatalog hinaus und ist damit zulässig.

Weigert sich der angetroffene „Schwarzfahrer", seine Personalien anzugeben oder wird die telefonische Nachfrage vom Landeseinwohneramt – aufgrund von falschen Angaben des „Schwarzfahrers" - zweimal negativ beantwortet, wird zur Identitätsprüfung die Polizei gerufen.

Der Polizei obliegt nach § 1 Abs. 4 ASOG der Schutz privater Rechte, wenn gerichtlicher Schutz nicht rechtzeitig zu erlangen ist und wenn ohne polizeiliche Hilfe die Verwirklichung des Rechts vereitelt oder wesentlich erschwert würde. Diese Voraussetzungen sind hier erfüllt. Ohne die Kenntnis der Identität des Schwarzfahrers ist eine Beitreibung des erhöhten Beförderungsentgeltes ebenso wenig möglich wie die Entscheidung darüber, ob ein Strafantrag gegen den Betroffenen wegen wiederholter Beförderungserschleichung gestellt wird. Soweit zum Schutz dieser Rechte erforderlich, darf die Polizei nach § 21 Abs. 2 Nr. 2 ASOG die Identität des Betroffenen feststellen. Die zur Identitätsfeststellung erhobenen Daten darf die Polizei nach § 44 Abs. 1 ASOG an andere öffentliche Stellen übermitteln, soweit das zur Erfüllung polizeilicher Aufgaben – hier zum Schutz privater Rechte in dem oben beschriebenen Umfang - erforderlich ist.

Rechtsgrundlage für die Datenerhebung und -verarbeitung durch die BVG ist § 3 Abs. 1 der Verordnung über die Verarbeitung von personenbezogenen Daten bei den Berliner Verkehrsbetrieben (BetriebeVO). Danach darf die BVG von Fahrgästen, die ohne gültigen Fahrausweis angetroffen werden, zur Beitreibung des erhöhten Beförderungsentgeltes sowie zur Erfassung von Wiederholungsfällen Angaben zu Na-

men, Geburtsdatum und -ort, Geschlecht, Anschrift, Namen und Anschrift der gesetzlichen Vertreter, Zeit, Ort und sonstigen für die Rechtsverfolgung erheblichen Umständen des Vorfalles erheben und verarbeiten. Die Daten können auch durch Privatfirmen im Rahmen einer Auftragsdatenverarbeitung nach § 3 Abs. 1 BlnDSG erhoben werden. Die datenschutzrechtliche Verantwortung für die Datenverarbeitung liegt weiterhin bei der BVG (§ 3 Abs. 1 BetriebeVO).

Nach § 3 Abs. 4 BetriebeVO hat die BVG die erhobenen Daten ein Jahr nach Abwicklung der auf den Vorfall gegründeten Rechtswirkung, spätestens zwei Jahre nach dem letzten einschlägigen Vorfall zu löschen. Die BVG macht von dieser zweijährigen Speicherbefugnis in der Praxis keinen Gebrauch, sondern löscht die Daten bereits ein Jahr nach dem Vorfall – es sei denn, es wird innerhalb dieses Jahres eine weitere Schwarzfahrt entdeckt.

Besonderer Service für Diabetiker auf Flugreisen

Auf ihre Anfrage, ob sie als Diabetikerin für das Einchecken am Flughafen für einen Urlaubsflug nach Griechenland ein ärztliches Attest benötige, wurde einer Reisenden vom Serviceteam einer Berliner Fluggesellschaft Folgendes mitgeteilt: „Als Diabetikerin benötigen Sie nur Ihren ganz normalen Diabetiker-Pass. Sollten Sie allerdings Spritzbesteck in die Flugkabine nehmen wollen, so muss dies angemeldet werden. Dazu benötigen wir den Veranstalter, dessen Buchungsnummer, genaue Flugtage, -strecke und -nummern und natürlich die Namen der Personen, die dies betrifft. Gleichzeitig werden wir gerne für Sie auf beiden Strecken Diabetikeressen anmelden."

Die von der Petentin verlangten Angaben zum Reiseveranstalter, dessen Buchungsnummer, die genauen Flugtage, -strecken und -nummern stehen im Zusammenhang mit ihrer Diabeteserkrankung. Die Daten über den Gesundheitszustand einer natürlichen Person sind sensitive Daten (§ 3 Abs. 9 BDSG). Wird die Datenverarbeitung auf die Einwilligung des Betroffenen gestützt, muss sich diese nach § 4 a Abs. 3 BDSG ausdrücklich auch auf diese besonderen personenbezogenen Daten beziehen. Die Verarbeitung dieser Daten für eigene Geschäftszwecke ist nach § 28 Abs. 6 BDSG nur unter sehr eingeschränkten Voraussetzungen zulässig.

Nachdem wir die *Fluggesellschaft* auf diese Umstände hingewiesen hatten, erklärte diese überraschend, dass es sich bei der Auskunft an die Kundin um ein Versehen handeln würde. Die vom Serviceteam verlangten Daten seien für die Durchführung des Fluges unerheblich und würden grundsätzlich auch nicht erhoben. Durch interne Vorkehrungen sei dafür Sorge getragen worden, dass diese Daten in Zukunft in keinem Fall mehr bei den Kunden abgefragt werden.

4.6.5 Was wir sonst noch geprüft haben ....

Aufgrund von Eingaben und Pressemeldungen, aber auch von Amts wegen wurde eine Vielzahl von Privatunternehmen geprüft. Hier drei Beispiele:

Pizza-Bringservice

Bei einer Werbeaktion für Internet-Besteller mailte ein Pizza-Bringservice nicht nur das Werbeschreiben, zusätzlich zur eigenen E-Mail-Adresse wurden den Betroffenen im Adressfeld auch die E-Mail-Adressen aller anderen Internet-Besteller des Unternehmens mitgeteilt. Der Inhaber meldete sich auf unsere Anfrage nicht, deshalb führten wir eine Prüfung vor Ort durch. Dort mussten wir hören, dass er den Datenschutzbeauftragten für einen der „üblichen Wegelagerer" hielt.

Bei den E-Mail-Adressen handelt es sich um Bestandsdaten im Sinne des § 5 Teledienste-datenschutzgesetz (TDSG). Danach darf der Diensteanbieter personenbezogene Daten eines Nutzers erheben, verarbeiten und nutzen, soweit dies für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses mit ihm über die Nutzung von Telediensten erforderlich ist. Hierzu gehört nicht die Mitteilung von Bestandsdaten eines Kunden an andere Kunden des Unternehmens, soweit dies nicht Inhalt oder Bestandteil der Dienstleistung ist oder der Betroffene eingewilligt hat. Die Übermittlung der E-Mail-Adressen an die anderen Kunden des Unternehmens war somit rechtswidrig.

Darüber hinaus stellten wir zahlreiche weitere Verstöße gegen datenschutzrechtliche Vorgaben fest:

Die Mitarbeiter des *Pizza-Bringservices* waren nicht bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis verpflichtet worden (§ 5 Satz 2 BDSG). Der Pizza-Bringservice hatte keinen Datenschutzbeauftragten bestellt, obwohl mehr als vier Mitarbeiter mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt waren (§ 4 f. Abs. 1 Satz 4 BDSG). Die Lohnsteuerkarten einiger Mitarbeiter befanden sich auf dem Schreibtisch und waren für andere Mitarbeiter frei zugänglich.

Bei einer Pizzabestellung wird die Telefonnummer gespeichert, diese stellt gleichzeitig die Kundennummer bei zukünftigen Bestellungen dar. Gegen die Verwendung der Telefonnummer als Kundennummer bestehen zwar keine grundsätzlichen datenschutzrechtlichen Bedenken, wir haben dem Unternehmen allerdings empfohlen, Kunden bei einer Erstbestellung auf die Verwendung der Telefonnummer als Kundennummer aufmerksam zu machen.

Neben der Speicherung von erforderlichen Daten wie Name, Vorname, Straße, Hausnummer, Postleitzahl

und Lage der Wohnung speichert das Unternehmen das Datum der ersten Bestellung, das Datum der letzten Bestellung sowie kumuliert alle bisher vorgenommenen Bestellungen (z. B. 5 x Pizza Tonno, 3 x Pizza Salami, 2 gemischte Salate etc.). Die Speicherung dieser Daten wurde damit begründet, dass das von dem Unternehmen verwendete Computerprogramm dies so vorsieht. Da aber die Speicherung dieser Daten nicht zur Zweckbestimmung des Vertragsverhältnisses mit dem Betroffenen erforderlich ist, ist die kumulierte Speicherung der bestellten Waren rechtswidrig (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Eine Datenspeicherung kann nicht damit begründet werden, dass das EDV-System die Daten automatisch speichert (Grundsatz der Datenvermeidung und Datensparsamkeit, vgl. § 3a BDSG).

Bei Werbeaktionen hat das Unternehmen versäumt, den Betroffenen bei der Ansprache darauf hinzuweisen, dass er nach § 28 Abs. 4 Satz 1 BDSG das Recht hat, der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung zu widersprechen (§ 28 Abs. 4 Satz 2 BDSG). Kunden, die gegen Werbung Widerspruch einlegten, wurden aus der Kundendatei gelöscht. Sobald diese allerdings eine neue Bestellung aufgaben, wurden sie wieder in die Kundendatei aufgenommen und erhielten auch wieder Werbung. Wir haben dem Unternehmen empfohlen, ein Verfahren zu wählen, das sicherstellt, dass Werbewidersprüche dauerhaft eingehalten werden. Hierzu muss das Unternehmen eine interne Robinsonliste führen, in der alle Personen aufgeführt sind, die ein Werbeverbot verhängt haben. Bei jeder Mailing-aktion ist durch einen Abgleich sicherzustellen, dass niemand beworben wird, der in der internen Robinsonliste eingetragen ist.

Den Vorwurf der Wegelagerei haben wir nicht weiterverfolgt.

Videoüberwachung eines Kaufhauses

Aufgrund eines Zeitungsartikels überprüften wir die Videoüberwachungspraxis eines Kaufhauses. Wir stellten fest, dass nicht nur im Innern des Kaufhauses in allen Verkaufsetagen Kameras installiert worden waren; auch die im Eigentum des Kaufhauses stehenden Arkaden wurden überwacht. Da der Bürgersteig durch die Arkaden führt, müssen Passanten, die nicht videoüberwacht werden möchten, die Straßenseite wechseln. Eine Kamera erfasst sogar einen wesentlichen Teil der Fahrbahn sowie Bürgersteigteile, die an die Arkaden grenzen. Eine weitere Kamera überwacht den Ausgang einer Tiefgarage sowie das angrenzende öffentliche Straßenland, damit das Wachpersonal schnell reagieren kann, wenn ein Auto den Parkplatz versperrt

.

Die Kameraüberwachung im Außenbereich läuft im durchgehenden 24-Stunden-Betrieb, während sie im Kaufhaus nur während der Geschäftszeiten aktiv ist. Die *Videoüberwachung* erfolgt nach dem Kamera-

Monitor-Prinzip, d. h., alle von den Kameras erfassten Daten laufen auf Monitoren in der Leitzentrale auf. Falls es zu keinen Zwischenfällen kommt (Diebstahl, Sachbeschädigung etc.), werden die Aufzeichnungen nach 24 Stunden wieder gelöscht.

Alle von dem Kaufhaus durchgeführten Videoüberwachungen waren schon deshalb rechtswidrig, weil der Umstand der Beobachtung und die verantwortliche Stelle nicht durch geeignete Maßnahmen erkennbar gemacht wurden (§ 6 b Abs. 2 BDSG). Ein Schild, welches am Eingang des Kaufhauses befestigt war, erfüllte nicht die Vorgaben des § 6 b Abs. 2 BDSG, da es so hoch aufgehängt wurde, dass Kunden auf dieses Schild nicht aufmerksam werden konnten. Wenn das Kaufhaus diesen Mangel behebt, bestehen gegen die Videoüberwachung des Kaufhausinneren keine datenschutzrechtlichen Bedenken.

Auch wenn die Arkaden im Eigentum des Kaufhauses stehen, ist eine Videoüberwachung zur Wahrung des Hausrechts oder zur Wahrung berechtigter Interessen der verantwortlichen Stelle nur dann zulässig, wenn keine Anhaltspunkte bestehen, dass das schutzwürdige Interesse des Betroffenen überwiegt (§ 6 b Abs. 1 BDSG). Da das Kaufhaus in einer der am besten geschützten Gegenden Berlins liegt und eine besondere Gefährdung des Kaufhauses nicht zu erkennen ist, ist das Interesse der Passanten, die derzeit nur durch einen Wechsel der Bürgersteigseite der Videoüberwachung durch das Kaufhaus „entgehen" können, höher zu gewichten als das Interesse des Kaufhauses. Ein berechtigtes Interesse zur Überwachung öffentlichen Straßenlandes durch das Kaufhaus ist nicht zu erkennen, jedenfalls überwiegen hier erst recht die schutzwürdigen Interessen des Betroffenen, so dass die Videoüberwachung des öffentlichen Straßenlandes ebenfalls rechtswidrig ist.

Wirtschaftsgut Kundendaten

Ein Berliner Energieversorger schrieb die Kunden eines Hamburger Konkurrenten, der Insolvenz beantragt hatte, an und empfahl ihnen, ihren Strom zukünftig bei ihm zu kaufen.

Das Berliner Unternehmen hatte die *Kundendaten* des Hamburger Unternehmens aufgekauft, um die Kunden des Hamburger Unternehmens zu bewerben. Zwischen den Vertragspartnern wurde vereinbart, dass nicht nur die in der Werbewirtschaft üblichen und durch § 28 Abs. 3 Nr. 3 BDSG gestatteten Daten wie Name, Anschrift, Zugehörigkeit zu einer Personengruppe übermittelt wurden, sondern eine Vielzahl von Daten, durch die der Datenaufkäufer in die Lage versetzt wurde, bei den einzelnen potenziellen Neukunden auch festzustellen, ob es sich um „interessante Akquiseobjekte" handelte. Im Einzelnen wurden folgende Daten übermittelt: Lieferadressennummer, Kundennummer, Zähler-

nummer, Liefername, Lieferstraße, Lieferort, Adressenabnahmestelle, Rechnungsadresse, Telefon-/Faxnummer, E-Mail-Adresse, Bankverbindung, Kontoinhaber, Zahlungsart, Kundenart, Besteuerung, Lieferbeginn und Verbrauch.

Wir haben das Berliner Energieunternehmen darauf hingewiesen, dass es für den Kauf eines derartigen Datensatzes keine Rechtsgrundlage im Bundesdatenschutzgesetz gibt und somit die Erhebung und Speicherung dieser Daten rechtswidrig war und nach § 43 Abs. 2 Nr. 1 BDSG auch als Ordnungswidrigkeit geahndet werden könnte. Das Unternehmen hat die Daten inzwischen gelöscht (§ 35 Abs. 2 Satz 2 Nr. 1 BDSG). Da das Unternehmen uns zusagte, zukünftig beim Kauf von Werbedaten nur Datensätze zu kaufen, die dem Listenprivileg nach § 28 Abs. 3 Nr. 3 BDSG unterliegen, haben wir auf die Einleitung eines Ordnungswidrigkeitsverfahrens verzichtet.

Eine originelle Idee

Ein Bürger erhielt einen Anruf von einer Mitarbeiterin eines Finanzdienstleistungsunternehmens, die ihm bestimmte Finanzprodukte anbot. Da der Anruf erfolgte, ohne dass der Betroffene hierzu einen Anlass gegeben hatte, hatte die betreffende Mitarbeiterin schon gegen wettbewerbsrechtliche Vorgaben verstoßen (cold call). Eine unter wettbewerbsrechtlichen Gesichtspunkten rechtswidrige Datennutzung ist auch datenschutzrechtlich zu beanstanden.

Zu der Frage, wie die Anruferin an die Daten des Petenten gelangt ist, konnte folgender Sachverhalt ermittelt werden: Der Vater der Mitarbeiterin arbeitete in einem Möbelgeschäft. Nach seinem Ruhestand verbesserte er seine Rente dadurch, dass er in Heimarbeit Kundenbetreuung für seinen Arbeitgeber durchführte und die für diese Arbeit erforderlichen Kundendaten in seiner Wohnung verwaltete. Seine Tochter ging davon aus, dass insbesondere die Käufer teurer Möbelstücke auch für Finanzdienstleistungsunternehmen von Interesse sein könnten. Bei einem Besuch ihres Vaters bat sie diesen, ihr einen Kaffee zu kochen. Die Abwesenheit ihrs Vaters benutzte sie, um den Namen und die Telefonnummer einiger ihr interessant erscheinender Kunden aufzuschreiben.

Das Möbelhaus nahm den Vorfall zum Anlass, dem Vater ein verschlossenes Behältnis zu besorgen, in welches er die Akten mit personenbezogenen Daten während seiner Abwesenheit legen kann. Seine Tochter gelobte Besserung...

4.7 Europäischer und internationaler Datenschutz

4.7.1 Safe Harbor

Wir haben in den letzten Jahren kontinuierlich über die Hintergründe und den aktuellen Sachstand zu den *Safe-Harbor-Prinzipien* berichtet[97], die der Gewährleistung eines angemessenen Datenschutzniveaus in den USA dienen. Nach wie vor ist den deutschen Aufsichtsbehörden kein Fall bekannt geworden, in dem sich ein Bürger über das Nichtfunktionieren der Vereinbarung beschwert hätte. Dennoch sah sich die nach Art. 29 Europäische Datenschutzrichtlinie eingesetzte „Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten" (Art. 29-Datenschutzgruppe) gehalten, über die Effizienz von Safe Harbor nachzudenken. Der Grund liegt in der in Art. 4 der Kommissionsentscheidung[98] genannten dreijährigen Frist zur Überprüfung der Umsetzung durch die Kommission sowie der Option der Datenschutzbehörden, die Vereinbarung vor Ablauf des Zeitraums zu überprüfen (FAQ 5).

So erfolgte nach einem im März 2002 durchgeführten Besuch einer Delegation der Datenschutzgruppe in Washington nach Gesprächen mit verschiedenen US-Behörden, Nichtregierungsorganisationen und Streitbeilegungsinstanzen eine erste gründliche Analyse der Erfahrungen mit Safe Harbor. Die Datenschutzgruppe hat es sich hiernach zum Ziel gesetzt, Diskrepanzen zwischen den vereinbarten Grundsätzen und der Umsetzungspraxis zu überbrücken, und in ihrem „Arbeitspapier über die Effizienz der Safe Harbor-Vereinbarung"[99] alle betroffenen Behörden, Organisationen und Verbände in der EU aufgefordert, über bestimmte Erkenntnisse zu informieren. Dazu gehören solche über die Möglichkeit der Einführung zusätzlicher Prüfmechanismen in Bezug auf die Prozedur zum Beitritt zu Safe Harbor, über praktische Maßnahmen für den Fall, dass eine Beitrittserklärung nicht von einer angemessenen Datenschutzpolitik begleitet ist, und über Möglichkeiten für verfeinerte Streitbeilegungs- und Veröffentlichungsmechanismen.

4.7.2 Weitere Ergebnisse aus Brüssel

Die Art. 29-Datenschutzgruppe hat ein Arbeitspapier zur internationalen *Anwendbarkeit des EU-Datenschutzrechts* angenommen, wenn Websites, die außerhalb der EU angesiedelt sind, personenbezogene Daten verarbeiten und insbesondere erheben[100]. Eine

---

[97] JB 1999, JB 2000, JB 2001, jeweils 4.7

[98] Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglich „häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. EG, L 215/7, vgl. Anlagenband „Dokumente zum Datenschutz 2000", S. 23

[99] WP 62 vom 2. Juli 2002

[100] Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU (WP 56 vom 30. Mai 2002)

der Kernaussagen des Papiers besteht darin, dass das europäische nationale Recht durch einen im Drittland befindlichen Anbieter dann zu beachten ist, wenn er Mittel einsetzt, mit denen er aktiv auf den PC im EU-Mitgliedstaat einwirkt (z. B. durch Cookies oder JavaScript-Software, die es ermöglicht, auf dem Nutzer-PC Anwendungen durchzuführen). Nicht geklärt werden konnte dagegen der so genannte „Fall C": Hierbei geht es um die Frage, welches Recht gilt, wenn der in der EU ansässige Nutzer eine Website eines Anbieters im Drittland nutzt und sich veranlasst sieht, personenbezogene Daten dorthin zu übermitteln. Deutschland hat die Auffassung vertreten, dass die Europäische Datenschutzrichtlinie für den Anbieter im Drittland nicht gilt, weil er keine Verfügungsgewalt über den PC des Betroffenen hat. Die gleiche Auffassung haben u. a. die britische und die österreichische Delegation vertreten, während insbesondere Frankreich für die Anwendung der Richtlinie auch im Drittland eintrat. Andere Delegationen sind in dieser Frage unentschlossen oder meinen, dass der Fall nicht im Rahmen eines Arbeitspapiers der Art. 29-Datenschutzgruppe entschieden werden sollte. Im Ergebnis ist zu dieser Frage keine Entscheidung gefallen.

In einem weiteren Arbeitspapier wurden Empfehlungen gegeben zum Datenschutz bei der *Überwachung von E-Mail-Nachrichten* und bei der Kontrolle des Internetzugriffs im Arbeitsverhältnis[101]. Die aus der Europäischen Datenschutzrichtlinie hergeleiteten Grundsätze wie Erforderlichkeit, Zweckbindung, Transparenz gegenüber den Arbeitnehmern bzw. den Kontrollstellen, Auskunftsrechte des Betroffenen, Verhältnismäßigkeit und Datensicherheit müssen beachtet werden, wenn eine Überwachung oder Kontrolle rechtmäßig und gerechtfertigt sein soll.

Vor dem Hintergrund der Verpflichtung der Europäischen Kommission, über die Umsetzung der Europäischen Datenschutzrichtlinie in den Mitgliedstaaten zu berichten (Art. 33 Europäische Datenschutzrichtlinie), hat sie im Herbst eine Konferenz veranstaltet, an der Experten (Wissenschaftler, Unternehmensvertreter, Verbraucherverbände und Datenschutzbehörden) aus der EU und Drittländern teilnahmen. Präsentiert wurden die Ergebnisse einer „Online-Konsultation", die sich an Verarbeiter und Bürger richtete. Etwa 9.000 Bürger und 1.000 Datenverarbeiter haben sich EU-weit an der dreimonatigen Aktion beteiligt. Die Beteiligten waren aufgerufen, ihre Erfahrungen und Erwartungen in Bezug auf den Datenschutz in einem Fragebogen mitzuteilen. Die Ergebnisse haben durchweg bestätigt, dass Datenschutz für den Einzelnen gerade im Zusammenhang mit E-Commerce und sonstigen Internetanwendungen bedeutsam ist und dass die Wirtschaft Datenschutzerfordernisse als wichtig einstuft. Sie hat

[101] Arbeitsdokument zur Überwachung der elektronischen Kommunikation von Beschäftigten (WP 55 vom 29. Mai 2002), vgl. 4.4.1

aber auch Bedarf angemeldet an einer Harmonisierung und einer einheitlicheren Interpretation der bestehenden Gesetze in Europa. In der Abschlussrede resümierte der für den Binnenmarkt zuständige Kommissar Frits Bolkestein, dass die unterschiedlichen Regelungen im nationalen Datenschutzrecht der Mitgliedstaaten offenbar tatsächliche Probleme für den freien Datenfluss schaffen. Die Schwierigkeiten seien geeignet, die Wettbewerbsfähigkeit der Unternehmen zu beeinträchtigen, weil sie an einer effektiven wirtschaftlichen Entfaltung im europäischen Raum gehindert sind. Als Ziele, die nach Auffassung des Kommissars im Bericht über die Umsetzung der EU-Datenschutzrichtlinie enthalten sein sollen, sind neben Vereinfachungen der Registrierungspflichten ausdrücklich Selbstregulierungsbemühungen der Wirtschaft genannt, hier insbesondere Codes of Conduct *(Unternehmensregelungen)* für den internationalen Datentransfer. Auch sei die Idee weiterzuverfolgen, dass die Genehmigung eines Drittlandtransfers durch eine Aufsichtsbehörde in Europa die Anerkennung der Entscheidung in allen anderen Mitgliedstaaten zur Folge hat.

Dieser Vorschlag wurde umgehend von der Art. 29-Datenschutzgruppe aufgegriffen. In dem Entwurf eines Arbeitspapiers werden Aussagen zur Rechtsnatur und zum wesentlichen Inhalt von verbindlichen unternehmensinternen Vorschriften getroffen. Auch wird ein Verfahren für die Zusammenarbeit der nationalen Aufsichtsbehörden skizziert, das bei der Überprüfung von Unternehmensregelungen greifen soll. Es geht dabei davon aus, dass trotz des Notifizierungsverfahrens auf europäischer Ebene nach Art. 26 Abs. 3 Europäische Datenschutzrichtlinie zusätzliche Bemühungen um Zusammenarbeit zwischen den nationalen Datenschutzbehörden ergriffen werden sollten (Art. 28 Abs. 6). Die Diskussionen hierüber sind noch nicht abgeschlossen.

Damit wird ein „Vorschlag für eine Verfahrensregelung zur Koordinierung von Entscheidungen der europäischen Datenschutzbehörden zu grenzüberschreitenden Datenflüssen" aufgegriffen, der angesichts des von der Wirtschaft geäußerten Bedarfs unter Beteiligung Berlins erarbeitet worden ist. Grundgedanke dabei war, dass die Koordinierung nur die Entscheidungen der jeweiligen Aufsichtsbehörde über ausreichende Garantien (Verträge und Unternehmensregelungen nach § 4 c Abs. 2 BDSG), „die 2. Stufe", betrifft. Die Prüfung der materiellen Zulässigkeit der Datenübermittlung nach nationalem Recht („1. Stufe") einschließlich der verfahrensrechtlichen Fragen (wie z. B. das Erfordernis einer Genehmigung für die Datenübermittlung) sollte von dieser Regelung nicht berührt und von jeder nationalen Aufsichtsbehörde selbst zu prüfen sein[102]. Die Teilnahme an dem koordinierten Verfahren durch die europäischen Aufsichtsbehörden ist freiwillig und

[102] zu den Prüfungen „1. und 2. Stufe" vgl. JB 2001, 4.7

sollte auch Beitrittskandidaten und Nicht-EWR-Mitgliedern freigestellt werden.

4.7.3 AG Internationaler Datenverkehr

Verbindliche Unternehmensregelungen

Die Arbeitsgruppe „Internationaler Datenverkehr" des Düsseldorfer Kreises hat sich unter unserem Vorsitz vornehmlich mit dem Inhalt von verbindlichen *Unternehmensregelungen* (§ 4 c Abs. 2 BDSG) befasst[103]. Zunächst hatte die DaimlerChrysler AG (mit Konzernhauptsitz in Stuttgart und einer für den Vertrieb zuständigen Niederlassung in Berlin) einen Code of Conduct (Unternehmensregelung) für Kundendaten einerseits und Arbeitnehmerdaten andererseits zur Überprüfung auf ausreichende Garantien nach § 4 c Abs. 2 BDSG bei den Aufsichtsbehörden eingereicht. Der Düsseldorfer Kreis hat die Regelungen verabschiedet und dem Unternehmen mitgeteilt, dass sie ausreichende Datenschutzgarantien im Sinne von § 4 c Abs. 2 BDSG vorsehen. Auf der Grundlage dieser Unternehmensregelungen konnten nunmehr bei den zuständigen Aufsichtsbehörden die Anträge auf Genehmigung der konkreten Datenübermittlung gestellt werden, die zwischenzeitlich von uns positiv beschieden wurden. Damit ist DaimlerChrysler weltweit das erste Unternehmen, das mit Aufsichtsbehörden abgestimmte verbindliche Unternehmensregelungen[104] nutzt, auf deren Grundlage es Datenübermittlungen aus in der EU ansässigen Konzernteilen in Drittländer vornehmen darf.

Die Arbeitsgruppe hat sich darüber hinaus mit dem „Muster einer Unternehmensrichtlinie für die Datenweitergabe innerhalb international tätiger Versicherungsunternehmen" des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) mit Sitz in Berlin befasst. Auch diese Regelung ist verabschiedet worden. Da es sich um ein Muster[105] handelt, gilt diese Richtlinie (im Gegensatz zu den Codes of Conduct von DaimlerChrysler) nicht unmittelbar, sondern muss von den einzelnen Versicherungen übernommen werden.

Die inhaltliche Überprüfung beider Unternehmensregelungen hat eine Vielzahl von Fragen aufgeworfen, die das Verfahren bei den deutschen Aufsichtsbehörden betreffen. So ist unter ihnen umstritten, ob Unternehmensregelungen nur zu dem Zweck genutzt werden können, ausreichende Datenschutzgarantien nach § 4 c Abs. 2 BDSG zu schaffen, und die Grundlage für eine hiernach zu beantragende Genehmigung zur Datenübermittlung bilden. Dies ist unsere Auffassung. Andere Aufsichtsbehörden meinen, dass eine Unterneh-

---

[103] vgl. 3.2

[104] vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2002", S. 38

[105] vgl. Anlagenband, a. a. O., S. 49

mensregelung als selbstregulierende Maßnahme der Wirtschaft für Datenübermittlungen in Unternehmensteile in Drittländern ohne angemessenes Datenschutzniveau herangezogen werden kann, wenn sie ein angemessenes Datenschutzniveau im Drittland gewährleisten. Da die Verantwortung für die Zulässigkeit der Übermittlung die übermittelnde Stelle trage (§ 4 b Abs. 5 BDSG), sei eine Unternehmensregelung der Aufsichtsbehörde nicht zur Überprüfung vorzulegen. Gestützt werde diese Auffassung auf den Wortlaut des § 4 b Abs. 2 Satz 2 BDSG, nach dem von einem angemessenen Datenschutzniveau die Rede ist, wenn dies bei den Stellen im Drittland vorliegt. Insofern sei die Regelung vergleichbar mit Art. 25 Europäische Datenschutzrichtlinie, der keine Genehmigungspflicht vorsieht .

Diese Auffassung ist europarechtswidrig, weil damit die Genehmigungspflicht für Tatbestände des Art. 26 Abs. 2 Europäische Datenschutzrichtlinie umgangen würde. Die „§ 4 b-Befürworter" befürchten unumwunden eine Flut von Genehmigungsanträgen. Dieselben Befürworter sind andererseits nicht willens, an anderer Stelle in Betracht kommende Verfahrensvereinfachungen zu nutzen. So hatten wir vorgeschlagen, nach einmal ergangener Entscheidung zu den Datenschutzgarantien in einer Unternehmensregelung für die Genehmigung der Datenübermittlung nach § 4 c Abs. 2 BDSG auf die Angaben im ohnehin zu führenden Verfahrensverzeichnis zurückzugreifen. Nach § 4 e Satz 1 Nr. 8 BSDG sind Angaben zu geplanten Datenübermittlungen in Drittstaaten zu machen. Dies hätte einen zweifachen Vorteil: Wenn der Genehmigungsgegenstand exakt auf die Ausführungen im Verfahrensverzeichnis bezogen würde, wäre einerseits das Unternehmen gezwungen, das Verfahrensverzeichnis korrekt zu führen. Erfolgen dann Datenübermittlungen in Drittländer, die sich nicht aus dem Verfahrensverzeichnis ergeben, stellt dies wegen der insoweit fehlenden Genehmigung einen Datenschutzverstoß dar, der bußgeldbewährt ist (§ 43 Abs. 2 Ziff. 1 BDSG). Andererseits muss bei der Genehmigung von der Aufsichtsbehörde die materielle Zulässigkeit („1. Stufe") nicht geprüft werden. Vielmehr kann sie lediglich mitteilen, dass sich die nach § 4 c Abs. 2 Satz 1 BDSG zu erteilende Genehmigung auf die Angaben i. S. v. § 4 e Satz 1 Nr. 8 BDSG bezieht. Den Bedenken einiger Aufsichtsbehörden vor einer Überflutung mit Genehmigungsanträgen könnte darüber hinaus dadurch Rechnung getragen werden, dass die Genehmigung als erteilt gilt, wenn die Aufsichtsbehörde nicht binnen einer bestimmten Frist widerspricht.

Diesen Vorschlag zur Verfahrensvereinfachung hat der Düsseldorfer Kreis nicht angenommen. Zur Begründung wurde vorgetragen, dass das Verfahrensverzeichnis zum einen zu oberflächlich ist und zum anderen nichts darüber aussage, ob Übermittlungen nicht unter den (keine Genehmigung erfordernden) Tatbestand des § 4 c Abs. 1 BDSG fallen. Im Übrigen sei dem deut-

schen Verwaltungsverfahrensrecht die Fiktion einer Genehmigung fremd. Die Entwicklung derart unterschiedlicher Rechtsauffassungen bei den Aufsichtsbehörden ist natürlich misslich und dürfte in der Wirtschaft zu Verunsicherungen und – was nicht auszuschließen ist – zu „Bundeslandfluchten" führen.

Letztlich wird sich wohl die Europäische Kommission mit der Frage beschäftigen müssen, ob mit § 4 b BDSG die Europäische Datenschutzrichtlinie sachgerecht umgesetzt worden ist. Die Kommission prüft bei allen Bestrebungen nationaler Aufsichtsbehörden im Hinblick auf die Überprüfung von verbindlichen Unternehmensregelungen derzeit, ob sie entsprechend dem Verfahren bei den Standardvertragsklauseln auch in Bezug auf Unternehmensregelungen eine Entscheidung nach Art. 26 Abs. 4 Europäische Datenschutzrichtlinie treffen kann. Folge wäre, dass – entsprechend der Verfahrensweise bei Anwendung der Standardvertragsklauseln – ein nach nationalem Recht zu betreibendes Genehmigungsverfahren wegen der auf europäischer Ebene ergangenen Entscheidung entfallen würde.

Betriebsvereinbarungen zur Übermittlung in Drittländer

Die AG hat sich auch mit der Frage beschäftigt, welche Rolle *Betriebsvereinbarungen* bei der Datenübermittlung in Drittländer spielen. Anerkannt ist, dass Betriebsvereinbarungen als andere Rechtsvorschriften im Sinne des BDSG die Datenübermittlung ins Drittland legitimieren, wenn sie gleichartige Schutzvorkehrungen wie das BDSG treffen („1. Stufe"). Was die „2. Stufe" (ausreichende Garantien) angeht, so ist unstrittig, dass nach deutschem Recht geschlossene Betriebsvereinbarungen nicht im Ausland gelten können. Sie sind deshalb nicht ohne weiteres für die „2. Stufe" relevant. Dies wäre nur dann der Fall, wenn sie in einem Vertrag oder in einer Unternehmensregelung für verbindlich erklärt werden. Das bedeutet, dass eine Datenübermittlung in Drittländer (in der „2. Stufe") nach § 4 c Abs. 1 Satz 1 Ziff. 2 BDSG in Verbindung mit der Betriebsvereinbarung zulässig sein kann, wenn die Datenübermittlung für die Erfüllung des Arbeitsvertrages erforderlich ist. Ist dies nicht der Fall, so kann die Datenübermittlung nach § 4 c Abs. 2 BDSG zulässig sein, wenn die Betriebsvereinbarung in den Vertragsklauseln oder verbindlichen Unternehmensregelungen für verbindlich erklärt worden ist. Betriebsräten ist zu empfehlen, Betriebsvereinbarungen im Zusammenhang mit der Datenübermittlung in Drittländer nur abzuschließen, wenn die Unternehmen bereit sind, für ausreichende Datenschutzgarantien im Drittland zu sorgen.

4.8 Organisation und Technik

4.8.1 Transparenz der Datenverarbeitung

Zu den Grundprinzipien des Datenschutzes gehört es

Durch die Möglichkeit mit Hilfe der Datenverarbeitung

weltweit, dass die Einhaltung der Bestimmungen kontrolliert werden muss. Voraussetzung ist die Kontrollierbarkeit der Verwendung personenbezogener Daten in Wirtschaft und Verwaltung, namentlich die automatisierte Datenverarbeitung. Aus diesem Grunde sehen die Datenschutzgesetze vor, dass ein Mindestmaß an Transparenz für die Kontrolle durch die Betroffenen selbst, die internen Kontrollinstanzen wie innere Revision und betriebliche bzw. behördliche Datenschutzbeauftragte sowie durch unabhängige externe Kontrollinstitutionen wie Aufsichtsbehörden und die Datenschutzbeauftragten des Bundes und Länder gewährleistet werden muss. Den Betroffenen selbst stehen Auskunfts- und Benachrichtigungsrechte zu, die sie zu einer gewissen Kontrolle des Umgangs mit den eigenen Daten befähigen.

Mit der Novellierung des Bundesdatenschutzgesetzes und des Berliner Datenschutzgesetzes im Jahre 2001 sind die für die interne und externe Kontrolle vorgesehenen Transparenzregelungen von bürokratischen Übertreibungen befreit worden.

Nach dem alten Bundesdatenschutzgesetz waren alle Unternehmen, für die das Gesetz vorsah, dass die Aufsichtsbehörde sie ohne bestimmte Anlässe kontrollieren durfte, dazu verpflichtet, sich bei der Aufsichtsbehörde mit bestimmten Angaben zum *Firmenregister* zu melden. Dies war notwendig, weil sonst die Aufsichtsbehörde nicht wissen konnte, in welchen Unternehmen sie ihre Kontrollbefugnisse uneingeschränkt wahrnehmen konnte. Das neue Datenschutzgesetz sieht vor, dass alle privatrechtlichen Organisationen ohne Anlass kontrolliert werden können, der Zweck des Registers entfällt damit. Das Register der Aufsichtsbehörde ist damit zwar nicht abgeschafft worden, erfasst aber nur noch einen Bruchteil der vorher schon meldepflichtigen Firmen, nämlich die Unternehmen, die personenbezogene Daten zum Zwecke der Übermittlung (z. B. Auskunfteien, Detekteien) oder anonymisierten Übermittlung (z. B. Markt- und Meinungsforschungsinstitute) speichern. Ferner sind Unternehmen meldepflichtig, die von der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten entbunden sind, dies auch nicht freiwillig getan haben, jedoch Daten nicht aufgrund „harter" Rechtsgrundlagen (das wäre die Einwilligung der Betroffenen oder die Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses) erheben, verarbeiten oder nutzen.

Das alte Dateien- und Geräteregister, das die Meldungen der öffentlichen Stellen Berlins beim Berliner Beauftragten für Datenschutz und Informationsfreiheit zusammenführte und auch bei optimaler Gesetzestreue Berliner Behörden nicht hinreichend aktuell und vollständig geführt werden konnte, ist abgeschafft worden. Sein Nutzen war gering, zumal auch die Einsichtsrechte der Bürger kaum in Anspruch genommen wurden. Das neue Berliner Datenschutzgesetz beschränkt sich

Datensammlungen anzulegen, erschließen sich diverse Möglichkeiten der automatisierten Auswertung. Der Ansatz die klassische Datenbank zu betrachten greift zu kurz. Bei den heute verfügbaren Rechnerleistungen können auch unstrukturierte Daten in kurzer Zeit überprüft werden. Anstelle von Strukturspeicherungen sollte der Datenschutz eine Transparenz der Datenauswertungen fordern. Nur so sind Möglichkeiten von Fehlinterpretationen zu vermeiden.
Ein Verfahrensverzeichnis besteht in der Senatsverwaltung für Wissenschaft, Forschung und Kultur nicht.

darauf, dass die behördlichen Datenschutzbeauftragten für die automatisierten Verfahren *Dateibeschreibungen* in einem Verfahrensverzeichnis führen, um damit die eigenen Kontrollaufgaben durchführen zu können, sie dem Berliner Beauftragten für Datenschutz und Informationsfreiheit zur Verwendung für seine Kontrolltätigkeit bereitzuhalten und das den Bürgern zustehende Recht zur Einsichtnahme zu gewährleisten (§§ 19, 19 a BlnDSG).

Zuständigkeit für die Dateibeschreibung nach § 19 Berliner Datenschutzgesetz (BlnDSG)

Die Neuordnung der Transparenzregelungen im Berliner Datenschutzgesetz hat bei vielen Daten verarbeitenden Stellen in der Berliner Verwaltung zu Verwirrungen geführt. Nach dem Wegfall der Meldepflicht zum Dateienregister bei unserer Behörde und mit der Verlagerung der Führung der neuen Dateibeschreibungen zu den Daten verarbeitenden Stellen wurden Fragen nach der Zuständigkeit zur Erstellung der Dateibeschreibungen aufgeworfen. Das Gesetz gibt zwar vor, dass der behördliche Datenschutzbeauftragte die Dateibeschreibungen zur Einsichtnahme bereithalten muss, es präzisiert aber nicht, wer diese zu erstellen hat. In § 19 BlnDSG wird nur allgemein gefordert, dass für automatisierte Verarbeitungen die Daten verarbeitende Stelle die in Abs. 2 aufgeführten Angaben schriftlich festzulegen hat.

In der Regel füllen die für den Einsatz der Informationstechnik zuständigen Stellen oder die Fachabteilungen die von der Senatsverwaltung für Inneres empfohlenen Musterformulare aus und reichen sie dann an die behördlichen Datenschutzbeauftragten weiter.

Dabei gibt es drei Fallkonstellationen:

- Bei bezirkseigenen Fachverfahren, also den ganz für eine spezielle Aufgabe eingerichteten automatisierten Anwendungen, sind die Daten vom Fachamt als der verfahrensverantwortlichen Stelle zur Verfügung zu stellen.

- Bei bezirksübergreifenden Verfahren, also Verfahren, die in allen oder in vielen Bezirksämtern zum Einsatz kommen sollen und meist unter Koordination von KoBIT (Geschäftsstelle zur Koordinierung und Beratung von IT-Verfahren im Bezirksamt Neukölln)[106] eingeführt werden, ist es sinnvoll, dass das Fachamt desjenigen Bezirks, der den Test- und Probe-Echtbetrieb durchführt, die Dateibeschreibung einheitlich den bezirklichen Datenschutzbeauftragten zur Verfügung stellt.

[106] vgl. 3.4

- Für die landesweiten, verwaltungsübergreifenden Großverfahren, die sowohl in den Senats- als auch in den Bezirksverwaltungen eingesetzt werden, z. B. IPV, ProFISKAL, sollte die fachlich zuständige Senatsverwaltung (und hier in der Regel die Projektleitung) eine Musterbeschreibung zur Verfügung stellen und diese an die anwendenden Stellen weiterleiten, damit sie dort ergänzt bzw. an die örtlichen Gegebenheiten angepasst werden können. Die vollständige und angepasste Dateibeschreibung wird dann an die zuständigen behördlichen Datenschutzbeauftragten weitergeleitet.

4.8.2 Behördliche und betriebliche Datenschutzbeauftragte

Mit der Novellierung des Berliner Datenschutzgesetzes hat sich eine Verschiebung der Datenschutzkontrolle von der externen zur internen Kontrolle ergeben. Den *behördlichen Datenschutzbeauftragten* sind wichtige Aufgaben zugewachsen, die ihre Position wesentlich verstärken sollten. Wenn die Voraussetzungen für besonders schutzbedürftige Verfahren gegeben sind (§ 5 Abs. 3 Satz 2 BlnDSG), haben sie nach § 19 a Abs.1 Satz 3 Nr.1 BlnDSG Vorabkontrollen durchzuführen. Nach § 19 a Abs.1 Satz 4 BlnDSG sind die Beschreibungen der automatisierten Verarbeitungen (Dateibeschreibung, § 19 BlnDSG) zu führen und jeder Person, die es wünscht, Einsicht zu gewähren.

Des Weiteren fordert das neue BlnDSG Sicherheitskonzepte auf der Grundlage von Risikoanalysen und enthält Regelungen zur Organisation der Wartung der DV-Systeme. Diese Änderungen des Datenschutzgesetzes erweitern im Vergleich zum alten Datenschutzrecht den Aufgabenbereich der behördlichen Datenschutzbeauftragten und verbessern die Voraussetzungen für das Wirksamwerden einer internen Datenschutzkontrolle.

Im Berichtsjahr wurde der gesetzlichen Verpflichtung zur Bestellung von stellvertretenden behördlichen Datenschutzbeauftragten nur zögerlich Folge geleistet. Wir haben mehrfach auf die gesetzliche Verpflichtung hingewiesen, dem behördlichen Datenschutzbeauftragten für den Fall seiner Abwesenheit einen Stellvertreter an die Seite zu geben.

Gesprächskreis der behördlichen Datenschutzbeauftragten der Bezirke

Seit fünf Jahren treffen sich die *bezirklichen Datenschutzbeauftragten* zu regelmäßigen Koordinierungsgesprächen in unserem Hause, um sich über aktuelle und relevante Datenschutzthemen in ihrem Geschäftsbereich auszutauschen. Zwar gibt es nach wie vor bezirkliche Datenschutzbeauftragte, die sich nicht an diesen Abstimmungsgesprächen beteiligen, dennoch

führt die engagierte Mitarbeit der übrigen bezirklichen Datenschutzbeauftragten zu nutzbringenden Erkenntnissen.

Zum Verfahren BASIS I (PROSOZ) wurde von einem Bezirksamtsvertreter die Frage aufgeworfen, inwieweit der Datenschutz und vor allem die Datensicherheit bei der Datenübermittlung für die *Zahlbarmachung von Sozialleistungen* aus dem PROSOZ-Verfahren an die Bezirkskasse gewährleistet sind. Dabei wurden zwei Verfahrensweisen diskutiert: Die Übertragung von Daten auf freigegebene Netzwerkverzeichnisse oder die Übertragung mittels elektronischer Post. In beiden Fällen kann auf die Verschlüsselung der Daten nicht verzichtet werden. Der Aufwand dafür ist jedoch bei der elektronischen Post sehr viel geringer, da hier Zusatzprogramme für den E-Mail-Client verwendet werden können und keine Abhängigkeit von den Verschlüsselungsverfahren im Berliner Landesnetz besteht, die nur zögerlich eingeführt werden.

Bei komplizierten Rechtsfällen sucht der behördliche Datenschutzbeauftragte Unterstützung im Rechtsamt seines Bezirks. Allerdings kommt es gelegentlich vor, dass er mit der dort erhaltenen Rechtsauffassung nicht einverstanden ist und sich, gestützt auf § 19 a Abs. 4 BlnDSG, zusätzlichen Rat beim Berliner Beauftragten für Datenschutz und Informationsfreiheit holt. In diesem Fall ist er frei, sich der einen oder der anderen Rechtsauffassung anzuschließen. Folgt er der Meinung des Berliner Beauftragten für Datenschutz und Informationsfreiheit, sollte es die zukünftige vertrauensvolle Zusammenarbeit mit seinem eigenen Rechtsamt nicht beeinträchtigen, weil verschiedene Rechtsmeinungen zum juristischen Alltag gehören. Im Übrigen ist der behördliche Datenschutzbeauftragte bei der Anwendung seiner Sachkunde weisungsfrei.

4.8.3 Sicherheitsrisiken mit universellen Schnittstellen

USB für *„Universal Serial Bus*" und IEEE1394 stehen für neue Schnittstellen, die nach den Vorstellungen der Hersteller den chaotischen Kabelsalat vermeiden sollen. Die Entwicklung neuer Schnittstellensysteme für PCs wurde erstmals vom Betriebssystem MS Windows 98 unterstützt. Die aktive Nutzung dieser Schnittstellen setzte allerdings erst in den letzten Jahren ein.

Am PC-Gehäuse stehen an der Rück- und Vorderseite meist mehrere Einsteckbuchsen bereit (oft bis zu 6-mal USB und 2-mal IEEE1394), die von beliebigen kompatiblen Geräten genutzt werden können. Wahlweise können Peripheriegeräte – Tastatur, Maus, Spielkonsolen, Speichermedien, Festplatten in entsprechenden Gehäusen, digitale Kameras usw. - angeschlossen werden, sofern auch sie über die entsprechende Schnittstelle verfügen. Auch die Möglichkeit der Hot-Plug&Play-Kompabilität, mit der Geräte während des laufenden Betriebs des PC-Systems angeschlossen und entfernt werden können, bietet Vorteile, weil ein Gerät auch

Der Senat ist sich der Risiken bewusst, die mit der Nutzung der aufgeführten universellen Schnittstellen am PC entstehen. Die vom Berliner Beauftragten für Datenschutz und Informationsfreiheit aufgeführten möglichen Sicherheitsmaßnahmen werden bei der Erstellung und Umsetzung der entsprechenden Sicherheitskonzepte berücksichtigt.

während der Arbeit am PC nachträglich und ohne zeitraubenden Neustart funktionstüchtig angeschlossen werden kann.

Als weiterer Vorteil ist die gesteigerte Datenübertragungsrate gegenüber den älteren seriellen bzw. parallelen Schnittstellen zu erwähnen. Mit einem Hub kann ein einzelner Anschluss um weitere gleichartige Anschlüsse (entsprechend einer Stromverteilerdose) erweitert werden. Auch die Stromversorgung kann teilweise vom Schnittstellensystem wahrgenommen werden. Bei neueren Notebooks findet man häufig nur noch eine USB-Schnittstelle vor, die in Verbindung mit entsprechenden Adaptern andere Schnittstellen ersetzen kann.

Auch die Installation bzw. Erkennung neu angeschlossener Geräte funktioniert sehr einfach. Nach dem Anschluss eines USB-Gerätes an das USB-System des PCs erfolgt meist die automatische Erkennung und anschließende Treiberinstallation. So ist es ohne weiteres auch möglich, externe Speichermedien (z. B. einen Memory Stick mit einer Speicherkapazität von bis zu 2 GB) anzuschließen.

Doch gerade hier beginnen die Probleme für den Datenschutz und die informationstechnische Sicherheit, die schon von den bisherigen genutzten seriellen und parallelen Schnittstellen bekannt sind, sich aber durch die neue Kompatibilität verstärken:

Die neu gewonnene Flexibilität macht es möglich, mit der Kapazität des Speichermediums für den PC-Nutzer verfügbare Daten auf externe Datenträger zu exportieren. War bisher der PC dadurch geschützt, dass keine Laufwerke für die Datenweitergabe existierten, so lässt sich dieser Schutz jetzt leicht durchbrechen, indem sensible personenbezogene Daten aus einem geschützten Bereich – z. B. einem geschütztem Netz – in einen ungeschützten Bereich exportiert werden.

Eine denkbare weitere Gefahr wäre, dass die so erhaltenen Daten auf einem entsprechenden Gerät manipuliert und somit verfälscht in das kompromittierte System zurückgespeichert werden.

Eine große Gefahr besteht auch darin, dass Daten und Programme über die Schnittstelle importiert werden können. So können Programme auf die lokale Platte oder ein Netzlaufwerk kopiert und installiert werden, mit denen sich der normale Nutzer erweiterte Rechte im Netz verschaffen kann, z. B. um auf die Datenbereiche lesend oder ändernd zugreifen zu können, für die er keine Zugriffsbefugnisse hat.

Bei einem Datenimport besteht jedoch auch die Gefahr der bewussten oder unbewussten Einschleusung von *Schadprogrammen* wie z. B. Viren. In diesen Fällen könnte in einem entsprechend geschützten Netz die Entdeckung des Virus möglicherweise schnell erfol-

gen, die Suche nach der Ursache einer solchen Infektion könnte sich jedoch schwierig gestalten, weil das Peripherie-Gerät schon längst entfernt sein kann und seine Spuren mit entsprechenden Tools verschleiert worden sein können.

Welche Gegenmaßnahmen stehen dem Netz-Administrator zur Verfügung, um eine Unterwanderung eines geschützten Systems zu verhindern?

Zunächst ist festzuhalten, dass die gleichen Maßnahmen zu empfehlen sind, die auch zuvor schon gegen die Schnittstellenproblematik getroffen werden konnten. Soweit die USB-Schnittstellen gebraucht werden, hilft nur ihre physische Absicherung am Rechnergehäuse, ersatzweise organisatorische Regelungen, die das Anschließen unautorisierter Geräte an die Rechner untersagen und einer strikten Kontrolle unterwerfen, die im Falle einer Zuwiderhandlung zu notwendigen Sanktionen führen müssen. Speziell für die Systemumgebungen, die in der Berliner Verwaltung noch gängig sind, ist zusätzlich festzustellen, dass das hier verbreitete Netzbetriebssystem Windows NT 4 USB-Schnittstellen nur unterstützt, wenn spezielle Treiber dafür installiert sind.

Sofern die USB-Schnittstellen nicht gebraucht werden, können sie im BIOS des Motherboards deaktiviert werden, falls sie Bestandteil des Motherboards sind. Wurde jedoch eine zusätzliche Schnittstellenkarte eingebaut, so ist zu prüfen, ob eine Deaktivierung per Jumpereinstellung auf der Einsteckkarte oder durch die Einstellung spezieller BIOS-Parameter der Einsteckkarte erfolgt.

Wir wissen aus eigenen Erfahrungen, dass die Deaktivierung im BIOS nicht immer ausreicht, da sich in bestimmten Fällen Peripherie-Geräte an dem BIOS vorbei anmelden können. Hier kann nur ein Eingriff in das Betriebssystem (Deaktivierung z. B. in der Windows Registry) helfen.

4.8.4 Videoüberwachung

Immer größere Bedeutung erlangt auch bei uns die *Videoüberwachung*. Im öffentlichen Bereich steht im Vordergrund die Frage, in welchem Umfang die Polizei diese Technik zur Gefahrenabwehr und zur vorbeugenden Straftatenbekämpfung nutzen darf. Der Berliner Gesetzgeber hat durch eine Novellierung des ASOG eine Rechtsgrundlage zur Überwachung gefährdeter Objekte geschaffen[107], die deutlich zurückhaltender ist als in anderen Bundesländern.

Gerade aber auch in der Privatwirtschaft wird in großem Umfang videoüberwacht, z. B. in Kaufhäusern,

[107] vgl. 4.2.1

Tankstellen oder Bahnhöfen. Hierzu enthält das BDSG 2001 in § 6 b erstmals datenschutzrechtliche Regelungen.

Diese Bestimmung ist unter zwei Aspekten ein Fremdkörper im Bundesdatenschutzgesetz. Sie setzt keine Erhebung oder Speicherung von Daten voraus, schon die bloße Beobachtungsmöglichkeit (Videoüberwachung ohne Aufzeichnung, Überwachungsraum nicht besetzt) erfüllt den Tatbestand. Außerdem knüpft sie anders als alle anderen Normen des Bundesdatenschutzgesetzes nicht an § 3 Abs. 1 BDSG an. § 6 b BDSG gilt auch dann, wenn die erfassten Bilddaten nicht personenbeziehbar sind, weil die Betroffenen zwar erkannt werden können, aber unbekannt sind. Wenn allerdings Aufnahmen etwa bei einer Webcam nicht oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten Person zugeordnet werden können (etwa kleine Punkte bei Luftaufnahmen), ist der § 6 b nicht erfüllt.

§ 6 b BDSG gilt nur für Raumbeobachtungen mit festinstallierten Kameras, nicht jedoch für die Beobachtung von (beweglichen) Zielpersonen. Wenn etwa ein Detektiv eine bestimmte Person videoüberwacht, fällt dies nicht in den Regelungsbereich, es gilt vielmehr allgemeines Datenschutzrecht bzw. Zivilrecht (allgemeines Persönlichkeitsrecht). Die Bestimmung gilt außerdem nur für *öffentlich zugängliche* Räume. Damit fällt insbesondere die Videoüberwachung von Arbeitnehmern, die sich nicht in öffentlich zugänglichem Raum aufhalten (Fabrik), nicht darunter, auch hier gelten weiterhin die allgemeinen Datenschutzbestimmungen sowie Arbeitsrecht. Eine öffentliche Zugänglichkeit wird man demgegenüber annehmen können in den Fällen „relativer Zugänglichkeit", wie etwa beim Zuschauerraum eines Theaters (Öffentlichkeit trotz Eintrittskarte).

Der in der Praxis bedeutendste Zweck der Videoüberwachung ist die Wahrnehmung des Hausrechts nach Abs. 1 Nr. 2. Hier geht es insbesondere darum, Diebstähle (Kaufhäuser, Tankstellen), Sachbeschädigungen (Bahnhöfe) oder sonstige Straftaten zu verhindern oder zumindest die Aufklärung von Straftaten zu erleichtern. Auf die Wahrnehmung des Hausrechts kann sich der Hausrechtsinhaber nur „innerhalb seiner vier Wände" berufen, eine Überwachung des öffentlichen Straßenlandes, um Steinwürfe gegen die Fensterscheiben zu erschweren, scheidet aus.

In der Regel werden gegen die Videoüberwachung zur Wahrnehmung des Hausrechts keine überwiegenden schutzwürdigen Interessen der Betroffenen vorliegen. Eine Kamera aber, bei der mittels Zoom die Betroffenen sehr genau gesehen werden können (Mimik), würde über die Erfordernisse zur Hausrechtswahrung hinausgehen und wäre damit rechtswidrig. Eine Videokamera in Umkleideräumen, die nicht auf die Kleider-

schränke begrenzt ist, könnte zwar Diebstähle verhindern, hier würden jedoch überwiegende schutzwürdige Interessen der Betroffenen die Videoüberwachung rechtswidrig machen.

Eine Videoüberwachung zur Wahrung berechtigter Interessen liegt vor (Abs. 1 Nr. 3), wenn Banken - auch zum Schutz ihrer Kunden - die Benutzer von Bankautomaten überwachen. Ein Sicherheitsunternehmen, das öffentliches Straßenland überwacht, handelt zwar zur Wahrnehmung berechtigter Interessen, in der Regel dürfte jedoch das schutzwürdige Interesse der Betroffenen überwiegen. Soweit die Beobachtung öffentlich zugänglicher Räume durch die Medien erfolgt, ist das Medienprivileg zu beachten (§ 41 BDSG).

Die in § 6 b Abs. 2 BDSG geforderte Erkennbarmachung der Videoüberwachung erfolgt in der Regel durch ein Hinweisschild, das gut erkennbar (Augenhöhe) auf die Videoüberwachung hinweist. Das Schild ist so anzubringen, dass der Betroffene in die Lage versetzt wird, der Videoüberwachung (durch Nichtbetreten) auszuweichen. Zusätzlich sollten Symbole (Piktogramme) verwendet werden, in Gegenden mit hohem ausländischem Bevölkerungsanteil auch ein Text in der entsprechenden Sprache. Auf dem Hinweisschild muss die verantwortliche Stelle ausdrücklich benannt werden. Das Deutsche Institut für Normung (DIN) bereitet derzeit eine Normierung eines entsprechenden Piktogramms vor.

Nach § 6 b Abs. 3 BDSG dürfen die mittels Videoüberwachung erhobenen Daten nur verarbeitet oder genutzt werden, wenn dies zur Erreichung des verfolgten Zwecks erforderlich ist und für überwiegende schutzwürdige Interessen des Betroffenen keine Anhaltspunkte bestehen. Beschränkt sich der Zweck der Videoüberwachung auf die Verhinderung von Straftaten, so reicht die Videoüberwachung als verlängertes Auge aus. Sollen demgegenüber Beweise mit Hilfe der Videoüberwachung gesichert werden, so ist eine Speicherung erforderlich.

Soweit die Videoüberwachung zu personenbezogenen Daten geführt hat, ist der Betroffene zu benachrichtigen (vgl. § 6 b Abs. 4). Die Löschung hat ohne schuldhaftes Verzögern zu erfolgen. Nicht nur die Löschung nach Auswertung hat unverzüglich zu erfolgen, auch die Auswertung selbst darf nicht zu lange verzögert werden, bei einer schuldhaften Verzögerung stehen die schutzwürdigen Interessen der Betroffenen einer weiteren Speicherung entgegen.

Ansonsten gelten die allgemeinen Regelungen des Bundesdatenschutzgesetzes. Auch die Vorschriften des Kunsturhebergesetzes bleiben unberührt, die eine Verbreitung der Bilder nur mit Einwilligung der Betroffenen zulassen (§§ 22, 23 KunstUrhG). Die Löschungsverpflichtung nach Zweckerreichung ist z. B. gegeben, wenn bei einer Videoaufnahme keine Strafta-

ten erkennbar sind, da in diesem Fall eine Beweissicherung nicht erforderlich ist.

4.9 Informationsfreiheit

4.9.1 Bundes- und Europarecht

Bundesinformationsfreiheitsgesetz

Die im letzten Jahresbericht geäußerte Skepsis zu den Chancen eines *Informationsfreiheitsgesetzes* auf Ebene des Bundes war leider berechtigt. Trotz einer Vereinbarung im Koalitionsvertrag zur 14. Wahlperiode des Bundestages schlug dieses Projekt fehl. Ein letzter Versuch, insbesondere aus den Reihen der Bundestagsfraktion von Bündnis 90/Die Grünen, ein solches Gesetz doch noch in die parlamentarische Debatte einzubringen, scheiterte im Frühsommer 2002 an massiven Vorbehalten sicherheitsrelevanter, außenpolitischer, (außen)wirtschaftlicher sowie fiskalischer Art aus verschiedenen Fachministerien, die sich im Nachgang zum 11. September 2001 noch verstärkt hatten, letztlich wohl auch an der mangelnden verbleibenden Zeit der Wahlperiode. Es bleibt nunmehr die Hoffnung, dass die erneute Vereinbarung im *Koalitionsvertrag*[108], ein Informationsfreiheitsgesetz für die Bundesbehörden einzubringen, in der 15. Wahlperiode tatsächlich erfüllt wird.

Auch in Bundesländern, die noch nicht über ein Informationsfreiheitsgesetz verfügen, ist ein entsprechendes Gesetz in nächster Zeit nicht zu erwarten. Zwar haben in verschiedenen Ländern parlamentarische sowie Anhörungen durch Stellen von Landesregierungen stattgefunden, jedoch zeichnen sich keine parlamentarischen Mehrheiten ab. Der Gesetzgebungsprozess ist in keinem dieser Länder so weit fortgeschritten, dass mit der Verabschiedung eines Gesetzes zu rechnen ist. Sollte ein Bundes-IFG Wirklichkeit werden, so könnte dieses ein entscheidender Impuls für erfolgversprechende Gesetzgebungsinitiativen und parlamentarische Mehrheiten in weiteren Bundesländern sein.

Verbraucherinformationsgesetz

Auch ein zweites Gesetzesvorhaben der Bundesregierung im Bereich der Informationsfreiheit scheiterte, jedoch nicht bereits im Anfangsstadium des Gesetzgebungsprozesses, sondern nachdem es bereits vom Bundestag verabschiedet worden war, an der mangelnden Zustimmung des Bundesrates: Im Zuge der BSE-Krise hatte die Bundesministerin für Verbraucherschutz und Landwirtschaft ein *Verbraucherinformationsgesetz* initiiert, das den Verbrauchern Zugang zu den bei Be-

[108] Koalitionsvertrag vom 16. Oktober 2002: „Erneuerung-Gerechtigkeit-Nachhaltigkeit", Kapitel VIII: „Sicherheit, Toleranz und Demokratie; Demokratische Beteiligungsrechte und Datenschutz"

hörden vorhandenen Informationen über Produkte und Dienstleistungen verschaffen und den Behörden das Recht einräumen sollte, unter bestimmten Voraussetzungen die Öffentlichkeit über marktrelevante Sachverhalte zu informieren. Zunächst war überdies vorgesehen, den Verbrauchern auch gegenüber Unternehmen ein Auskunftsrecht einzuräumen. Allerdings wurde diese Überlegung aufgrund des massiven Widerstands aus der Wirtschaft sehr schnell ad acta gelegt. Im Zuge der weiteren Entwicklung kam es dann zu einer zusätzlichen Einschränkung des Anwendungsbereichs, der sich nur noch auf Informationen zu Erzeugnissen nach dem Lebensmittel- und Bedarfsgegenständegesetz, dem Fleischhygienegesetz, dem Geflügelfleischhygienegesetz und dem Weingesetz erstrecken sollte. Trotz Anrufung des Vermittlungsausschusses scheiterte letztlich auch dieses Gesetz.

Am 5. Juni 2002 veröffentlichte die Europäische Kommission den Vorschlag für eine „Richtlinie des Europäischen Parlaments und des Rates über die Weiterverwendung und *kommerzielle Verwertung von Dokumenten des öffentlichen Sektors*"[109]. Nach Art. 1 dieses Vorschlags soll die Richtlinie einen Mindestbestand an Regeln festlegen, der die kommerzielle und anderweitige Verwertung vorhandener allgemein zugänglicher Dokumente öffentlicher Stellen der Mitgliedstaaten durch alle Bürger der Union und jede natürliche oder juristische Person mit Wohnsitz oder Sitz in einem Mitgliedsstaat gewährleistet.

Des Weiteren verabschiedete der Ministerausschuss des Europarats am 21. Februar 2002 eine Empfehlung zum Zugang zu amtlichen Dokumenten[110]. Danach sollen die Mitgliedstaaten garantieren, dass jedermann auf Antrag ein Recht auf Zugang zu offiziellen Dokumenten der öffentlichen Stellen erhält. Dieses Prinzip soll ohne Diskriminierung und ohne Rücksicht auf die Nationalität der Antragsteller gelten.

4.9.2 Informationsfreiheit in Berlin

Verbraucherinformationsgesetz

Um eine Rechtsgrundlage zu schaffen, die es nach dem Scheitern des Bundesverbraucherinformationsgesetzes Berliner Behörden ermöglicht, die Öffentlichkeit über Gefahren, die von Lebensmitteln, Kosmetika und Bedarfsgegenständen ausgehen, zu informieren, hat der Berliner Senat am 31. Oktober 2002 den Entwurf eines *Berliner Verbraucherinformationsgesetzes*[111] in das Der Entwurf des Berliner Verbraucherinformationsgesetzes hat nicht zum Inhalt, die Öffentlichkeit vor Gefahren zu warnen. Das ist schon jetzt nach dem Produktsicherungsgesetz möglich. Das Gesetz soll vielmehr die Tatbestände für eine Information der Öffentlichkeit über Verstöße gegen Bestimmungen des Lebensmittel- und Bedarfsgegenständerechts schaffen,

[109] KOM (2002) 207

[110] Rec (2002) 2, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2002", S. 86

[111] Gesetz zur Information der Verbraucherinnen und Verbraucher im Lebensmittelverkehr im Land Berlin, Abghs.-Drs. 15/838

Abgeordnetenhaus eingebracht. Dieses Gesetz könnte zumindest einen Teil der Lücke schließen, die das Scheitern des Bundesverbraucherinformationsgesetzes hinterlässt. Ein Informationsanspruch der Verbraucher, wie es das Bundesgesetz vorsah, würde damit allerdings nicht begründet werden.

wenn hieran ein besonderes öffentliches Interesse besteht.

Gebühren

Mehrere Anwohner eines Berliner Kneipenkiezes, deren Nachtruhe durch die Restaurantbesucher erheblich gestört wurde, hatten beim zuständigen Bezirksamt um Akteneinsicht in die Gewerbeakten der Gaststätten nachgesucht. Das Bezirksamt erwog, für jeden Vorgang eine eigenständige Gebühr zu erheben. Angesichts der Vielzahl der beantragten Akten hätte der Gesamtbetrag der Gebühren weit höher ausfallen können, als die in Tarifstelle 1004 a) des Gebührenverzeichnisses festgesetzte oberste Rahmengebühr von 511,29 €.

Nach § 16 Berliner Informationsfreiheitsgesetz (IFG) ist die Akteneinsicht oder Aktenauskunft gebührenpflichtig, das Gesetz über *Gebühren und Beiträge* (GebBeitrG) in der jeweils geltenden Fassung entsprechend anzuwenden. Verwaltungsgebühren sind nach § 2 Abs. 1 GebBeitrG für die Vornahme von Amtshandlungen zu erheben. Nicht jede von der öffentlichen Stelle vorzunehmende Tätigkeit stellt allerdings eine eigenständige Amtshandlung dar, für die eine gesonderte Gebühr erhoben werden kann, vielmehr fällt diese nur einmalig für den jeweiligen in sich abgeschlossenen Gesamtvorgang an. Die Amtshandlung bemisst sich grundsätzlich nach dem Antrag, der sich auch auf mehrere bei der öffentlichen Stelle geführte Akten beziehen kann, soweit er zumindest thematisch oder nach bestimmten Sachverhalten oder Zeiträumen eingegrenzt wird, ihm somit ein konkreter einheitlicher Lebenssachverhalt zugrunde liegt.

Allein dieses Ergebnis lässt sich auch mit dem Sinn und Zweck der Regelung einer Rahmengebühr vereinbaren. Ihr Ziel ist es, einerseits eine prohibitive Wirkung zu vermeiden[112] und andererseits die durch den Informationszugang entstehenden Kosten nicht allein den öffentlichen Stellen anzulasten. Die im Gebührenverzeichnis festgelegte Rahmengebühr lässt insoweit genügend Raum für eine Bemessung der Gebührenhöhe unter Beachtung des Kostendeckungs- und des Äquivalenzprinzips. Insbesondere in Fällen, in denen das berechtigte Informationsinteresse der Antragsteller nur durch Einsichtnahme in eine größere Anzahl von Akten befriedigt werden kann, käme die mehrfache Gebührenfestsetzung einer faktischen Beschränkung ihres umfassend gewährten Informationsanspruchs gleich.

[112] vgl. EuGH, Urteil vom 9. September 1999. In: NVwZ 1999, S.1209 (1211)

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Die Gebührenerhebung ist auch kein tauglicher Ansatzpunkt, um einem möglichen Missbrauch der Informationszugangsfreiheit durch Pauschalanträge zu begegnen. Zu unbestimmte Anträge sind vielmehr als unzulässig abzulehnen. Bei hinreichend bestimmten und damit zulässigen Anträgen, die aber eine größere Anzahl von Akten umfassen, reduziert sich der Verwaltungsaufwand der öffentlichen Stelle, da diese sich nur mit einem spezifischen Lebenssachverhalt zu befassen hat. Dies wird auch im vorliegenden Fall deutlich: Die Prüfung von Ausschlussgründen der Akteneinsicht nach §§ 6 – 12 IFG, die üblicherweise den größten Aufwand bei der öffentlichen Stelle erfordert, kann einem einheitlichen Muster folgen, da es sich bei den beantragten Unterlagen jeweils um die Gewerbeakten von Gaststätten handelte.

Antragsteller und Bezirksamt haben sich gütlich geeinigt. Ob das zugrunde liegende Problem der Lärmbelästigung damit gelöst werden konnte, wird spätestens mit Beginn der Biergartensaison 2003 in der Presse zu verfolgen sein.

Ein Petent hatte bei der Aufsicht führenden Senatsverwaltung Einsicht in Niederschriften von Delegiertenversammlungen einer Kammer beantragt, was die Senatsverwaltung ablehnte. Zur Begründung wurde angegeben, dass die Sitzungen der Delegiertenversammlung nicht öffentlich seien und durch die Akteneinsicht Betriebs- oder Geschäftsgeheimnisse der Kammer offenbart würden. Im Übrigen könne sich der Petent an die Kammer direkt wenden. Die Bescheidung des daraufhin eingelegten Widerspruchs zog sich trotz mehrfacher Intervention von uns über mehrere Monate hin. Schließlich wurde dem Petenten mitgeteilt, dass seinem Widerspruch stattgegeben würde, er aber mit einer Gebühr für die Akteneinsicht von rund 360 € zu rechnen habe. Der Petent zog daraufhin seinen Antrag zurück. Er teilte uns mit, dass er zwar nach wie vor Interesse an der Information habe, die zu erwartende Gebühr ihn aber von einer weiteren Verfolgung seines Anspruchs abhalte.

Die Senatsverwaltung hat trotz unserer Aufforderung noch nicht dargelegt, aufgrund welcher Erwägungen sie diese – auch im Verhältnis zu vergleichbaren Akteneinsichtsvorgängen – außerordentlich hohe Gebühr verlangen will. Ganz offensichtlich widerspricht die Entscheidung aber dem Urteil des EuGH vom 9. September 1999, wonach die Gebühr für eine Akteneinsicht eine angemessene Höhe nicht überschreiten und insbesondere nicht prohibitiv sein darf[113]. Dass im vorliegenden Fall die Höhe der angekündigten Gebühr aber eine abwehrende Wirkung entfaltete, liegt auf der Hand. Im Hinblick auf den relativ geringen Umfang der Unterlagen (zwei konkret benannte Niederschriften von Sitzungen) wird überdies die Unverhältnismäßig-

Wie im Bericht des BlnBDI selbst angegeben, ist die Erörterung mit der zuständigen Senatsverwaltung noch nicht abgeschlossen. Eine inhaltliche Stellungnahme zu den spekulativen Vermutungen der für die überschlägige Gebührenhöheentscheidung verwandten Berechnungsparameter bleibt daher dieser bilateralen Erörterung vorbehalten.

[113] ebenda

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

keit der in Betracht gezogenen Gebühr deutlich. Sollten für deren Berechnung auch die Arbeitszeiten juristischer Mitarbeiter in Ansatz gebracht worden seien, die für die Einarbeitung in die Rechtsmaterie aufgewandt werden mussten, so wäre dies unzulässig. Die antragstellenden Bürgerinnen und Bürger müssen davon ausgehen können, dass die öffentlichen Stellen die rechtlichen Grundlagen ihrer Aufgaben beherrschen. Soweit – wie dies bei dem noch immer neuen IFG häufig der Fall sein dürfte – diese sich in die Materie zunächst noch einarbeiten müssen, kann dieser Aufwand dem Antragsteller oder der Antragstellerin nicht in Rechnung gestellt werden.

Im Übrigen ging auch der Hinweis an den Antragsteller, sich mit seinem Anliegen an die betreffende Kammer zu wenden, fehl. Nach § 3 IFG besteht ein Recht auf Einsicht in oder Auskunft über den Inhalt der von der öffentlichen Stelle geführten Akten. Maßgeblich ist somit für den Informationsanspruch die Tatsache, dass Akten bei einer öffentlichen Stelle vorhanden sind. Ob darüber hinaus auch eine andere Stelle über diese verfügt oder einzelne Dokumente dort entstanden sind, ist irrelevant.

Privat oder dienstlich?

Eine Petentin hatte Einsicht in eine Akte des Gesundheitsamtes eines Bezirksamtes genommen. Ihre Bitte um Anfertigung von Kopien auch der handschriftlichen Aufzeichnungen der Sachbearbeiterin wurde mit der Begründung abgelehnt, dass es sich dabei um eigene Notizen der Sachbearbeiterin handele, die nicht herauszugeben seien.

Das Recht auf Herausgabe von Kopien nach § 13 Abs. 5 IFG bezieht sich grundsätzlich auf alle Unterlagen, die dem Akteneinsichts- bzw. Aktenauskunftsanspruch unterliegen. Eine Ausnahme besteht nur dann, wenn Urheberrechte des Verfassers der Anfertigung von Kopien entgegenstehen. Nach § 3 Abs. 2 IFG unterfallen dem Informationsanspruch alle Akten(teile), die amtlichen Zwecken dienen. Die Art und Weise, in der die Aufzeichnungen gefertigt wurden, spielt dabei keine Rolle. Insoweit gehören hierzu auch *handschriftliche Aufzeichnungen* von Beschäftigten, wenn sie im Rahmen der Aufgabenerfüllung entstanden sind oder hierfür verwendet werden. Auch unterliegt die Handschrift eines Beschäftigten nicht dem Urheberrecht. Ebenso ist es für die Frage, welche Akten amtlichen Zwecken dienen, unerheblich, ob ihr Inhalt mit Hilfe eines PC erstellt wurde oder die Informationen handschriftlich von den Beschäftigten festgehalten wurden. Lediglich tatsächlich persönliche Unterlagen, wie die eigenen Gehaltsabrechnungen, private Adressbücher oder Familienfotos, die Beschäftigte an ihrem Arbeitsplatz aufbewahren, unterfallen nicht dem IFG.

Der Senat teilt die Auffassung, dass gemäß § 3 Abs. 2 IFG auch handschriftliche Aufzeichnungen von Beschäftigten grundsätzlich dem Aktenbegriff des IFG unterfallen, wenn sie amtlichen Zwecken dienen. Allerdings ist hier im Einzelfall genau zu differenzieren, wann etwas amtlichen Zwecken dient und wann nicht. So können im Einzelfall bestimmte Notizen oder Entwürfe unter Umständen auch dann, wenn sie noch einen Bezug zur Aufgabenerledigung aufweisen, dennoch keinen „amtlichen Zwecken“ dienen. Beispielhaft seien etwa erste Vorentwürfe von Verfügungen, auf denen keine Zeichnung erfolgen soll, Lösungsskizzen, Memos oder ähnliches genannt, die vom Bearbeiter nie zur „Veraktung“ vorgesehen wurden und denen daher – obwohl ein dienstlicher Bezug vorliegt – kein amtlicher Charakter i.S. von § 3 Abs. 2 IFG zukommt. § 3 Abs. 1 Satz 1 IFG verdeutlicht, dass sich der Informationsanspruch auf die „von der öffentlichen Stelle geführten Akten“ erstreckt.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Informationsfreiheit beim Rechnungshof

Zwei Eingaben betrafen Anträge auf Einsicht in Unterlagen des Rechnungshofs von Berlin. Der Rechnungshof hatte beide mit der Begründung abgelehnt, dass seine Unterlagen nur insoweit dem IFG unterlägen, als sie Tätigkeiten betreffen, die Verwaltungsaufgaben im Sinne von § 2 Abs. 1 Satz 2 IFG darstellen.

Dies ergebe sich zum einen aus der richterlichen Unabhängigkeit der Prüftätigkeit des *Rechnungshofs*, weshalb die für die Gerichte normierte Ausnahme auch für ihn gelte. Zum anderen beträfe die Prüftätigkeit den „Kernbereich der exekutiven Eigenverantwortung", der einer außenstehenden Kontrolle nicht unterliege. Überdies stünde einem Informationsanspruch nach dem IFG § 12 Abs. 2 Rechnungshofgesetz (RHG) entgegen, wonach die Mitglieder und Prüfer des Rechnungshofs von den durch ihre Tätigkeit bekannt gewordenen Tatsachen und Urteilen nur zur Erfüllung ihrer Aufgaben im Rahmen dieses Gesetzes Gebrauch machen dürfen.

Die Prüfung des Informationsanspruchs der Petenten gegenüber dem Rechnungshof durch uns hat zur gegenteiligen Auffassung geführt:

Zunächst fehlt es an einer ausdrücklichen gesetzlich Ausnahme hinsichtlich des Geltungsbereichs des IFG für den Rechnungshof, wie sie für die Gerichte und die Behörden der Staatsanwaltschaft in § 2 Abs. 1 IFG normiert ist. Für diese gilt das Gesetz nur, solange sie Verwaltungsaufgaben erledigen. Hätte der Gesetzgeber eine solche Ausnahme auch für den Rechnungshof gewollt, so wäre dies im Gesetzestext verankert worden wie in Nordrhein-Westfalen (§ 2 Abs. 2 IFG NRW) und Brandenburg (§ 2 Abs. 2 AIG i. V. m. § 1 Abs. 2 Landesorganisationsgesetz des Landes Brandenburg).

Dem Kernbereich exekutiver Eigenverantwortung trägt bereits § 10 IFG Rechnung, der den Schutz des behördlichen Entscheidungsprozesses vorsieht (als Ausnahme jedoch eng auszulegen ist). Unabhängig davon unterliegen Behörden aber gleichwohl grundsätzlich dem IFG. Nur im *Einzelfall* kann die Vertraulichkeit der Beratungen oder der Kernbereich exekutiver Eigenverantwortung berührt sein. Dann könnte ein Anspruch auf Informationszugang ausgeschlossen sein. Im Rahmen dieses Rechtsinstituts wird – wie seine Formulierung nahe legt – überdies nur der *Kernbereich* der exekutiven Eigenverantwortlichkeit, nicht jedoch die exekutive Eigenverantwortlichkeit an sich geschützt.

Nach § 12 Abs. 2 RHG dürfen die Mitglieder und Prüfer des Rechnungshofs von den durch ihre Tätigkeit bekannt gewordenen Tatsachen und Urteilen nur zur Erfüllung ihrer Aufgaben im Rahmen dieses Gesetzes Gebrauch machen. Zweck dieser Bestimmung ist der Geheimnisschutz. Diesem Zweck dienen auch die in §§ 5 – 12 IFG enthaltenen Bestimmungen. Für die An-

nahme, dass § 12 Abs. 2 RHG lex specialis gegenüber den Bestimmungen des IFG ist, sind Anhaltspunkte nicht ersichtlich. Insbesondere ist im IFG keine Subsidiaritätsklausel wie in § 2 Abs. 5 Satz 2 BlnDSG zu finden.

1. Telekommunikation und Medien

5.1 Telekommunikationsnetze und –dienste

Überwachung des Telekommunikationsverkehrs und der Internetnutzung

Während sich in den vergangenen Jahren die Bemühungen der Sicherheitsbehörden auf den Zugriff auf bei den Anbietern von *Telekommunikations- und Internetdienstleistungen* zu Abrechnungszwecken vorhandene Bestands-, Verbindungs- und Nutzungsdaten der Kunden konzentrierten, war das vergangene Jahr davon bestimmt, den Umfang der bei den Anbietern vorhandenen Daten zu vergrößern. Entsprechende Bemühungen gab es sowohl auf nationaler Ebene als auch in der Europäischen Union.

Sie richten sich darauf, die Anbieter dazu zu verpflichten, *Bestands- und Nutzungsdaten* ihrer Kunden „vorbeugend" für Zwecke der Strafverfolgung und der Nachrichtendienste zu speichern. Diese Speicherung soll unabhängig davon erfolgen, ob die Anbieter diese Daten selbst für die Abrechnung in Anspruch genommener Dienstleistungen mit ihren Kunden benötigen. Demgegenüber sieht das bisher geltende Datenschutzrecht vor, dass Verbindungs- bzw. Nutzungsdaten über in Anspruch genommene Telekommunikations- oder Internetdienstleistungen von den Anbietern nur dann gespeichert werden dürfen, wenn diese die Daten für die Abrechnung der Dienste gegenüber dem Nutzer benötigen.

Am 13. November 2001 hatten die Freistaaten Bayern und Thüringen einen Gesetzesantrag im Bundesrat eingebracht, der die Einführung einer *Vorratsdatenspeicherung* für Anbieter von Telekommunikationsdienstleistungen und von Telediensten vorsah[114]. Dieser Antrag wurde jedoch von der damaligen Bundesratsmehrheit im März 2002 abgelehnt.

Am 27. März 2002 brachte das Land Niedersachsen den Entwurf eines „Gesetzes zur Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Missbrauchs von Kindern und der Vollstreckung freiheitsentziehender Sanktionen" im Bundesrat ein. Dieser Entwurf[115] beschränkte sich zunächst darauf, § 100 a Strafprozessordnung, der eine Aufzählung von

[114] BR-Drs. 1014/01

[115] BR-Drs. 275/02

Straftaten enthält, in denen die Überwachung des Telekommunikationsverkehrs angeordnet werden kann, um Bestimmungen zu erweitern, die den sexuellen Missbrauch von Kindern und die Verbreitung entsprechender pornographischer Schriften enthalten. Im Rechtsausschuss des Bundesrates wurde der Gesetzentwurf um Vorschriften ergänzt, die eine Verpflichtung von Anbietern von Telekommunikations- und Telediensten enthielten, unabhängig von Abrechnungserfordernissen für Zwecke der Strafverfolgung bzw. für geheimdienstliche Zwecke Verbindungs- bzw. Nutzungsdaten ihrer Kunden zu speichern. Die Dauer der Vorratsspeicherung sollte in beiden Fällen durch die Bundesregierung durch Rechtsverordnung bestimmt werden können. Der Gesetzesantrag wurde durch den Bundesrat angenommen. Der Gesetzentwurf wurde im Juli 2002 in den Deutschen Bundestag eingebracht[116]. Die Bundesregierung lehnte in ihrer Stellungnahme die Vorschläge des Bundesrates zur Einführung einer Vorratsdatenspeicherung ab[117]. Mit dem Ablauf der Legislaturperiode verfiel der Gesetzentwurf der Diskontinuität. Es ist jedoch damit zu rechnen, dass der Bundesrat auch in der neuen Legislaturperiode wiederum entsprechende Gesetzesanträge einbringen wird.

Auch auf europäischer Ebene entfalteten die Sicherheitsbehörden Aktivitäten zur Einführung einer Regelung zur Vorratsdatenspeicherung: Nachdem durch die Datenschutzrichtlinie für elektronische Kommunikation[118] in Art. 15 Abs. 1 eine Öffnungsklausel zur Speicherung von Verbindungsdaten für Sicherheitszwecke eingefügt worden war (vgl. unten), gelangten im August 2002 weitere Planungen an die Öffentlichkeit: Die britische Bürgerrechtsorganisation „Statewatch" berichtete über Pläne des Rats der Justiz- und Innenminister, im Rahmen der „dritten Säule" durch einen Rahmenbeschluss die vorbeugende, flächendeckende Speicherung von Verbindungsdaten für einen Zeitraum zwischen 12 und 24 Monaten bindend vorzuschreiben.
Die dänische Ratspräsidentschaft in der zweiten Jahreshälfte dementierte umgehend in einer Presseerklärung, dass sie einen Entwurf für bindende Regeln für die Vorratsdatenspeicherung vorgelegt hätte, und verwies auf den von ihr vorgelegten „Entwurf für Schlussfolgerungen des Rates zur Informationstechnologie und zur Ermittlungsarbeit und Verfolgung im Bereich der organisierten Kriminalität" vom Juni 2002. Dieser Vorschlag werde gegenwärtig in der zuständigen Ratsarbeitsgruppe beraten, werde aber wohl kaum vor November 2002 fertig gestellt sein. Darüber hinaus gebe es keine weiteren Vorschläge zur Vorratsdatenspeicherung von Verbindungsdaten und die dänische Ratsprä-

---

[116] BT-Drs. 14/9801

[117] a. a. O., S. 15 f.

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

sidentschaft sei auch nicht mit dem Entwurf solcher Vorschläge befasst.

Zu einer Beschlussfassung kam es auf der Sitzung des Europäischen Rates am 13. Juni 2002 nicht. Soweit dies aus öffentlich zugänglichen Dokumenten ersichtlich ist, befasste sich die zuständige Arbeitsgruppe des Rates der Europäischen Union (die multidisziplinäre Gruppe "Organisierte Kriminalität" (MDG)) zunächst damit, den gegenwärtigen Stand der Regelungen in den Mitgliedstaaten und deren Haltung zur Einführung einer Verpflichtung zur Vorratsdatenspeicherung in Erfahrung zu bringen. Dazu erstellte der Vorsitz der Arbeitsgruppe im August 2002 zunächst einen Fragebogen. Unterdessen kursieren im Internet Dokumente, die die Antworten der Delegation der Arbeitsgruppe auf die einzelnen Fragen dokumentieren. Daraus ergibt sich, dass in den meisten Mitgliedstaaten bisher keine Regelungen getroffen worden sind, die über die Erforderlichkeit zur Abrechnung oder zur Verhinderung betrügerischer Inanspruchnahme von Diensten Anbieter dazu verpflichten, Verbindungs- bzw. Nutzungsdaten allein für Zwecke der Strafverfolgung für einen bestimmten Zeitraum aufzuheben.

Entsprechende Vorschläge werden jedoch in vielen Mitgliedstaaten diskutiert. Die überwiegende Mehrzahl der Vertreter der Mitgliedstaaten in der Arbeitsgruppe befürwortet die Einführung von verbindlichen Mindestfristen zur Vorratsdatenspeicherung.

Gegen die Pläne zur Vorratsdatenspeicherung haben sich im zurückliegenden Berichtszeitraum wiederum Datenschutzbehörden und -organisationen sowohl auf nationaler als auch auf internationaler Ebene entschieden ausgesprochen: So hat die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25. Oktober 2002 darauf hingewiesen, dass eine verdachtslose routinemäßige Speicherung sämtlicher bei der Nutzung von Kommunikationsnetzen anfallenden Daten auf Vorrat mit dem deutschen Verfassungsrecht nicht zu vereinbaren ist[119]. Bereits die 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. März 2002 hatte in einer weiteren Entschließung darauf hingewiesen, dass nach dem geltenden Recht in Deutschland Anbieter von Tele-, Medien- und Telekommunikationsdiensten weder berechtigt noch verpflichtet sind, generell Daten auf Vorrat zu erheben, zu speichern oder herauszugeben, die sie zu keinem Zeitpunkt für eigene Zwecke benötigen[120].

Auch die Konferenz der Europäischen Datenschutzbe-

[119] Entschließung zur systematischen verdachtslosen Datenspeicherung in der Telekommunikation und im Internet, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2002", S. 27

[120] Entschließung zum Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien und Telekommunikationsdiensten, vgl. Anlagenband, a. a. O., S.10

auftragten hat in einer Erklärung vom 11. September 2002 gravierende Zweifel hinsichtlich der Legitimität und Legalität von weitreichenden Maßnahmen zur Vorratsdatenspeicherung angemeldet und unter Bezugnahme auf die Rechtsprechung des Europäischen Menschenrechtsgerichtshofs betont, dass eine solche Vorratsdatenspeicherung ein unzulässiger Eingriff in die Grundrechte des Einzelnen nach Art. 8 der Europäischen Menschenrechtskonvention sei[121]. Die Art. 29-Datenschutz-gruppe hat sich am 11. Oktober in einer Stellungnahme der Erklärung der europäischen Datenschutzbeauftragten angeschlossen[122].

Identifikationszwang für Inhaber von Prepaid-Karten

Im März 2002 veröffentlichte das Bundesministerium für Wirtschaft und Technologie „Eckpunkte zur Anpassung der Regelung des § 90 Telekommunikationsgesetz (TKG)". Diese Vorschrift verpflichtet seit ihrem In-Kraft-Treten im Jahr 1996 geschäftsmäßige Anbieter von Telekommunikationsdiensten zur Führung von Kundendateien mit Namen und Anschriften der Inhaber von Rufnummern und Rufnummernkontingenten, die den Strafverfolgungsbehörden und Nachrichtendiensten in einem automatisierten Verfahren zum Abruf bereitgestellt werden müssen. Hierzu hatte bereits in der Vergangenheit die Regulierungsbehörde für Telekommunikation und Post (RegTP) die Auffassung vertreten, die Verpflichtung zur Führung von Kundendateien im Rahmen des § 90 Abs. 1 TKG gelte auch für den Vertrieb von *Prepaid-Produkten*. Gegen diese Verpflichtung hatte ein Anbieter von Telekommunikationsdienstleistungen vor dem Verwaltungsgericht Köln Klage erhoben und Recht bekommen. Das Verwaltungsgericht Köln hat in seinem Urteil[123] insbesondere ausgeführt, dass Anbieter von Telekommunikationsdienstleistungen nach § 90 TKG nur zur Aufnahme von Kundendaten verpflichtet seien, die auf der Grundlage des § 89 Abs. 2 TKG i. V. m. § 3 TDSV (alt) im Rahmen der Erforderlichkeit zur betrieblichen Abwicklung erhoben werden dürfen.

Die Initiative zielte darauf, dass Anbieter von Telekommunikationsdienstleistungen zur Aufnahme von Kundendaten in den nach § 90 TKG zu führenden Kundendateien verpflichtet werden sollten, und zwar unabhängig davon, ob sie die Daten für die Vertragsabwicklung benötigen. Zur Begründung wurde ausgeführt, die Verwendung anonym oder pseudonym erworbener Prepaid-Karten erschwere die Ermittlungstä-

---

[121] Erklärung zur zwangsweisen systematischen Speicherung von Verkehrsdaten der Telekommunikation, vgl. Anlagenband, a. a. O., S. 63

[122] Stellungnahme 5/2002 zur Erklärung der Europäischen Datenschutzbeauftragten auf der Internationalen Konferenz in Cardiff (9. - 11. September 2002) zur obligatorischen systematischen Aufbewahrung von Verkehrsdaten der Telekommunikation

[123] Urteil vom 22. September 2000, Az.: 11 K 240/00

tigkeit der Sicherheitsbehörden. Die Erfahrungen der Behörden zeigten, dass die gesetzliche Regelungslücke unter Straftätern bekannt sei und in nahezu allen Deliktsbereichen mit steigender Tendenz genutzt werde, um eine Beweisführung der Ermittler unmöglich zu machen.

Diesem Vorhaben ist die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 24. Mai 2002 zum geplanten Identifikationszwang in der Telekommunikation entschieden entgegengetreten[124]. Die Konferenz hat insbesondere darauf hingewiesen, dass auch durch die geplante Gesetzesänderung nicht verhindern wird, dass Straftäterinnen und Straftäter bewusst und gezielt in kurzen Zeitabständen neue Prepaid-Karten erwerben, Strohleute zum Erwerb einsetzen, die Karten häufig – teilweise nach jedem Telefonat – wechseln oder die Karten untereinander austauschen. In der Begründung werde auch nicht plausibel dargelegt, dass mit dem geltenden Recht die Ermittlungstätigkeit tatsächlich behindert und durch die geplante Änderung erleichtert wird. Darüber hinaus wird durch die geplanten Regelungen die gesetzliche Verpflichtung, sich an dem Ziel von Datenvermeidung und Datensparsamkeit auszurichten, konterkariert. Gerade die Prepaid-Karten seien ein gutes Beispiel für den Einsatz datenschutzfreundlicher Technologien, da sie anonymes Kommunizieren auf unkomplizierte Weise ermöglichen. Die Nutzung dieser Angebote dürfe deshalb nicht von der Speicherung von Bestandsdaten abhängig gemacht werden.

Im Mai 2002 hob das Oberverwaltungsgericht Münster überraschend das Urteil des Verwaltungsgerichts Köln auf[125]. In seinem Beschluss vertritt das OVG Münster die Auffassung, § 90 Abs. 1 TKG sei eine hinreichende Rechtsgrundlage zur Verpflichtung der Anbieter von Telekommunikationsdienstleistungen, beim Verkauf von Prepaid-Produkten Kundendaten zu erheben, zu überprüfen und eine Identifizierung des Kunden anhand der amtlichen Ausweispapiere vorzunehmen. Es bleibt abzuwarten, ob das Bundesministerium für Wirtschaft und Arbeit vor diesem Hintergrund das oben genannte Gesetzgebungsvorhaben weiterbetreiben wird.

Auch in der Europäischen Union steht die Frage der Identifizierung von Nutzern von Guthabenkarten auf der Tagesordnung: So hat die Ratsarbeitsgruppe „Drogenhandel" in einem Papier, das für den Rat der Europäischen Union erarbeitet wurde, empfohlen, dass die Mitgliedstaaten „ein Bündel angemessener rechtlicher Anforderungen für die Identifizierung von Guthaben-

[124] Anlagenband a. a. O., S. 25

[125] Beschluss vom 17. Mai 2002, Az.:13 A 5293/00. In: MMR 8/2002, S. 563

kartenbenutzern" prüfen sollen[126].

Datenschutzrichtlinie für elektronische Kommunikation verabschiedet

Die Europäische *Datenschutzrichtlinie für die elektronische Kommunikation*[127] ist am 31. Juli 2002 in Kraft getreten. Über die Vorarbeiten hatten wir bereits in unserem Jahresbericht 2000 ausführlich berichtet[128]. Die Richtlinie ersetzt die Telekommunikations-Datenschutzrichtlinie 97/66/EG aus dem Jahre 1997[129]. Für die Umsetzung der Bestimmungen ist eine Frist bis zum 31. Oktober 2003 vorgesehen (Art. 17 Abs. 1).

Während die Regelungen der ursprünglichen Richtlinie auf das Angebot von Telekommunikationsdienstleistungen im Festnetz und in Mobilfunknetzen beschränkt waren, ist der Anwendungsbereich der neuen Richtlinie weiter gefasst und bezieht sich allgemein auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation. Neu eingefügt wurde insbesondere eine Vorschrift, die die Verarbeitung von „anderen Standortdaten als Verkehrsdaten" regelt (Art. 9). Damit sind Standortdaten gemeint, deren Genauigkeit über das für den Netzbetrieb erforderliche Maß hinausgeht. Diese Informationen werden insbesondere für solche Dienste verwendet, die auf der Kenntnis des Standortes z. B. eines Mobilfunknutzers basieren[130]. Diese Daten dürfen nach den Bestimmungen der Richtlinie nur im zur Bereitstellung von Diensten mit Zusatznutzen (beispielsweise die Beratung hinsichtlich der billigsten Tarifpakete, Navigationshilfen, Verkehrsinformationen, Wettervorhersage oder touristische Informationen) erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Nutzer oder Teilnehmer seine Einwilligung gegeben hat (Erwägungsgrund 18). Der Diensteanbieter ist verpflichtet, die Nutzer vor Einholung ihrer Einwilligung darüber zu informieren, welche Arten von Standortdaten verarbeitet werden, für welche Zwecke und für wie lange das geschieht und ob die Daten zum Zwecke der Bereitstellung des Dienstes an einen Dritten weitergegeben werden (Art. 9 Abs. 1). Auch wenn eine solche Einwilligung erteilt wird, müssen die Nutzer weiterhin die Möglichkeit haben, die Verarbeitung der Daten für jede Netzverbindung oder für jede Übertragung einer Nachricht auf einfache Weise und gebührenfrei zeitweise zu

---

[126] Dok-Nr. 5157/2/02 STUP 3 REV 1

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

[128] JB 2000, 5.1

[129] Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, ABl. EG L 24/1 vom 30. Januar 1998

[130] Location based services, vgl. 5.2 und JB 2001, 5.1

untersagen (Art. 9 Abs. 2).

Die Regelung über *unerbetene Nachrichten*, die sich bisher nur auf automatische Anrufsysteme und Faxgeräte für Zwecke der Direktwerbung bezog, ist auf elektronische Post ausgeweitet worden. Auch hier ist die Nutzung für Zwecke der Direktwerbung nur bei vorheriger Einwilligung der Teilnehmer gestattet (Art. 13 Abs. 1). Im Rahmen einer bestehenden Geschäftsbeziehung kann ein Anbieter jedoch mittels elektronischer Post Direktwerbung betreiben, wenn die Werbung auf eigene ähnliche Produkte oder Dienstleistungen beschränkt ist und die Kunden die Möglichkeit erhalten, eine solche Nutzung ihrer elektronischen Kontaktinformationen bei deren Erhebung und bei jeder Übertragung gebührenfrei und problemlos abzulehnen (Art. 13 Abs. 2).

Ausdrücklich verboten wird das Versenden elektronischer Nachrichten zu Zwecken der *Direktwerbung*, wenn dabei die Identität des Absenders, in dessen Auftrag die Nachricht übermittelt wird, verschleiert oder verheimlicht wird oder wenn keine gültige Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann (Art. 13 Abs. 4).

Darüber hinaus werden Regelungen zu einigen spezifischen Aspekten des Internet getroffen: So soll der Einsatz von Instrumenten, die von Anbietern ohne Wissen des Nutzers auf dessen Endgerät platziert werden, um Zugang zu Informationen zu erlangen oder die Nutzeraktivität zurückzuverfolgen (z. B. „Spyware", Web-Bugs", „Hidden Identifiers"), nur für rechtmäßige Zwecke mit dem Wissen der betreffenden Nutzer gestattet sein (Erwägungsgrund 24). Hinsichtlich des Einsatzes von „Cookies" und ähnlichen Instrumenten wird bestimmt, dass die Nutzer klare und genaue Informationen über deren Zweck und die Gelegenheit erhalten müssen, die Speicherung in ihrem Endgerät abzulehnen (Erwägungsgrund 25).

Neu eingefügt wurde schließlich die bereits oben erwähnte Öffnungsklausel, die es den Mitgliedstaaten ermöglicht, für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen, Beschränkungen der Schutzvorschriften der Richtlinie zur Vertraulichkeit, der Verarbeitung von Verkehrsdaten, der Rechte der Nutzer im Hinblick auf die Rufnummernanzeige sowie die Verarbeitung von Standortdaten zu erlassen. Die Mitgliedstaaten können unter anderem durch Rechtsvorschriften vorsehen, dass die genannten Daten während einer begrenzten Zeit aufbewahrt werden (Art. 15 Abs. 1). Die Maßnahmen müssen im Einklang mit der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten in ihrer Auslegung durch die Urteile des Europäischen Gerichtshofs für

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Menschenrechte erfolgen und „... in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ...” sein (Art. 15 Abs. 1, Erwägungsgrund 11).

Besonders diese letztgenannte Regelung war zwischen dem Rat der Europäischen Union und dem Europäischen Parlament in dem Verfahren zum Erlass der Richtlinie äußerst umstritten. Die weitschweifig formulierten Bedingungen, an die die Maßnahmen zur Vorratsspeicherung von Verkehrs- und Standortdaten geknüpft werden, stellen einen Versuch dar zu verhindern, dass sämtliche Dämme in diesem Bereich brechen. Inwieweit dies gelungen ist, wird die Umsetzung der Richtlinie in den Mitgliedstaaten zeigen. Anders als dies verschiedentlich in der öffentlichen Debatte dargestellt wurde, stellt die Bestimmung des Art. 15 Abs. 1 der Richtlinie allerdings ausdrücklich keine Verpflichtung der Mitgliedstaaten zum Erlass von Rechtsvorschriften zur Vorratsdatenspeicherung dar, sondern ermöglicht diese lediglich.

Steter Tropfen höhlt den Stein: Der IMSI-Catcher

Bereits seit längerer Zeit bestand bei Sicherheitsbehörden und Nachrichten großes Interesse am Einsatz des *„IMSI-Catchers”*, um damit auch unbekannte, von Verdächtigen genutzte Anschlussnummern ermitteln zu können. Der IMSI-Catcher simuliert eine Basisstation eines Mobilfunknetzes, bei der sich Handys in einem bestimmten Umkreis anmelden, weil sie diese für „echt” halten. Durch den Einsatz des Geräts kann die IMSI (International Mobile Subscriber Identity) eines Mobilfunkgeräts festgestellt und zur Identifizierung des Anschlussinhabers genutzt werden. Dadurch werden allerdings nicht nur die Telefone der Verdächtigen „gefangen”, sondern alle Mobiltelefone, die sich zum Zeitpunkt des Einsatzes des IMSI-Catchers in dessen Einzugsbereich befinden. Es wird also nicht nur in das Fernmeldegeheimnis der Verdächtigen, sondern auch von Unbeteiligten eingegriffen, die sich zufällig in der entsprechenden Funkzelle befinden.

Der Einsatz des IMSI-Catchers ist im Entwurf des Gesetzes zur Änderung des Gesetzes über den Verfassungsschutz Berlin nicht vorgesehen.

Für den Einsatz des IMSI-Catchers fehlte es bisher an einer ausdrücklichen gesetzlichen Grundlage. Eine solche Grundlage ist für das Bundesamt für Verfassungsschutz durch das Gesetz zur Bekämpfung des internationalen Terrorismus[131] durch Einführung des § 9 Abs. 4 in das Bundesverfassungsschutzgesetz geschaffen worden. Der Bundesrat hatte in einem von ihm initiierten, parallel laufenden Gesetzgebungsverfahren bereits im November 2002 die Schaffung einer Regelung für den Einsatz des IMSI-Catchers auch im Strafverfahren vorgeschlagen[132]. Ähnliche Bemühun-

[131] Terrorismusbekämpfungsgesetz vom 9. Januar 2002, BGBl. I, S. 361

[132] Entwurf eines Gesetzes zur Verbesserung des strafrechtlichen Instrumentariums für die Bekämpfung des Terrorismus und der organisierten Kriminalität, BR-Drs. 1014/01

gen des Bundesrates waren schon im Jahre 1997 zu verzeichnen gewesen und wurden seinerzeit von den Datenschutzbeauftragten scharf kritisiert[133]. 1997 war die Regelung aus dem Gesetzentwurf im Laufe der Beratungen wieder gestrichen worden; auch der Gesetzesantrag des Bundesrates vom 27. November 2001 wurde am 21. März 2002 mit den Stimmen der Koalitionsfraktionen abgelehnt[134].

Im Mai 2002 wurde in das im Deutschen Bundestag beratene Gesetz zur Änderung der Strafprozessordnung (StPO) auf Initiative des Rechtsausschusses des Bundestages eine Regelung eingefügt, die die StPO um den § 100 i ergänzt und den Einsatz des IMSI-Catchers im Rahmen der Strafverfolgung regelt. Diese Regelung durchlief das weitere Gesetzgebungsverfahren ohne wesentliche Änderungen und trat am 14. August 2002 in Kraft[135].

Nunmehr darf zur Vorbereitung einer Überwachungsmaßnahme nach § 100 a StPO die Geräte- und Kartennummer eines aktiv geschalteten Mobilfunkendgeräts ermittelt werden. Die Maßnahme ist nur zulässig, wenn die Voraussetzungen des § 100 a StPO vorliegen und die Durchführung der Überwachungsmaßnahme ohne die Ermittlung der Geräte- und Kartennummer nicht möglich oder wesentlich erschwert wäre (§ 100 i Abs. 1, 2 StPO). Außerdem darf zur vorläufigen Festnahme nach § 127 Abs. 2 StPO oder zur Ergreifung eines Täters aufgrund eines Haft- oder Unterbringungsbefehls der Standort eines aktiv geschalteten Mobilfunkendgerätes ermittelt werden. Dies ist nur im Fall einer Straftat von erheblicher Bedeutung zulässig und nur dann, wenn die Ermittlung des Aufenthaltsortes des Täters auf andere Weise weniger erfolgversprechend oder erschwert wäre. Die Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes ist darüber hinaus im Falle einer Straftat von erheblicher Bedeutung auch dann zulässig, wenn die Ermittlung des Aufenthaltsortes des Täters zur Eigensicherung der zur vorläufigen Festnahme oder Ergreifung eingesetzten Beamten des Polizeidienstes erforderlich ist (§ 100 i Abs. 2 StPO).

In beiden Fällen dürfen personenbezogene Daten Dritter anlässlich der dargestellten Maßnahme nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung der entsprechenden Zwecke unvermeidbar ist. Diese Daten dürfen über den Datenabgleich zur Ermittlung der gesuchten Geräte- und Kartennummer hinaus nicht verwendet werden und sind nach Beendigung der Maßnahme unverzüglich zu löschen (§ 100 i Abs. 3 StPO).

---

[133] JB 1997, 4.7.1

[134] vgl. das Protokoll der 227. Sitzung des Bundestages vom 21. März 2002, S. 22515

[135] BGBl. I, S. 3018

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

5.2 Tele- und Mediendienste

Sechster Rundfunkänderungsstaatsvertrag

Zum 1. Juli 2002 ist der 6. *Rundfunkänderungsstaatsvertrag* in Kraft getreten[136]. Durch die Novellierung des Mediendienste-Staatsvertrages werden insbesondere die bereits im Jahre 2001 geänderten Datenschutzbestimmungen im Bereich der Teledienste[137] weitgehend unverändert auch für Anbieter von Mediendiensten übernommen.

Überschießende Erhebung von Bestandsdaten

Ein in Berlin ansässiger Anbieter eines Mediendienstes erhob als Bedingung für den – kostenlosen – Zugang zu einem Nachrichtenarchiv zwangsweise Namen und Adressen der Nutzer. Darüber hinaus wurden zahlreiche weitere personenbezogene Daten auf freiwilliger Basis erhoben.

Die zwangsweise Erhebung personenbezogener Bestandsdaten als Zugangsvoraussetzung für einen kostenlosen Dienst ist unzulässig, wenn sie nicht für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses mit dem Nutzer über die Nutzung von Mediendiensten erforderlich sind (§ 19 Abs. 1 Mediendienste-Staatsvertrag). Vorliegend konnte die Erforderlichkeit durch den Diensteanbieter nicht nachgewiesen werden. Die Erhebung der Daten war insbesondere nicht zu Zwecken der Abrechnung mit dem Nutzer erforderlich, da die Inanspruchnahme des Dienstes kostenlos war. Die Erhebung personenbezogener Bestandsdaten der Nutzer kann daher nur auf die – freiwillige – Einwilligung der Nutzer gestützt werden. Der Anbieter hat die zwangsweise Erhebung von Namen und Adresse der Nutzer des Nachrichtenarchivs eingestellt.

Nach einer Einzelbestellung bei einem Online-Versandhandelsunternehmen wurde einem Nutzer zu dessen Erstaunen eine Benutzerkennung und ein Passwort für ein Benutzerkonto bei diesem Anbieter mitgeteilt, obwohl er dies nie beantragt hatte.

Der Anbieter hatte es einerseits versäumt, den Nutzer – wie in § 4 Abs. 1 Teledienstedatenschutzgesetz (TDDSG) vorgeschrieben – über die beabsichtigte Verarbeitung und Nutzung seiner personenbezogenen Daten zu informieren. Darüber hinaus war die Einrichtung eines Benutzerkontos für die Erbringung der Dienstleistung auch nicht erforderlich. Die Erhebung

---

[136] Sechster Staatsvertrag zur Änderung des Rundfunkstaatsvertrages, des Rundfunkfinanzierungstaatsvertrages und des Mediendienste-Staatsvertrages (Sechster Rundfunkänderungsstaatsvertrag), GVBl. 2002, S. 163

[137] JB 2001, 5.2

und Verarbeitung von Bestandsdaten konnte damit nicht auf § 5 TDDSG gestützt werden, sondern bedurfte der ausdrücklichen Einwilligung des Nutzers. Der Anbieter hat das Angebot so umgestaltet, dass ein Benutzerkonto nunmehr nur noch für solche Nutzer eingerichtet wird, die dies ausdrücklich wünschen.

Mangelnde Information der Betroffenen

Anbieter von Tele- und Mediendiensten sind nach dem geltenden Recht verpflichtet, die Nutzer über Art, Umfang und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten (§ 4 Abs. 1 TDDSG; § 18 Abs. 1 Mediendienste-Staatsvertrag). Diese *Unterrichtung* hat zu Beginn des Nutzungsvorganges zu erfolgen. Eine Unterrichtung ist auch erforderlich bei automatisierten Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten vorbereiten.

Solche Unterrichtungen waren vielfach nicht oder in nicht ausreichender Form vorhanden. Vielfach herrscht Unklarheit bei den Anbietern, wie eine solche Unterrichtung sachgerecht vorgenommen werden kann. Dafür ist es jedenfalls nicht ausreichend, wenn irgendwo in einem Internet-Angebot allgemeine Geschäftsbedingungen enthalten sind, die – zum Teil an nicht eben prominenter Stelle – Informationen zum Datenschutz enthalten. Diese Information muss dem Nutzer – wie gesetzlich festgelegt – vielmehr zu Beginn des Nutzungsvorganges ausdrücklich zugänglich gemacht werden. Dies kann beispielsweise durch einen ausdrücklichen Hinweis an der Stelle des Internet-Angebots erfolgen, wo erstmals personenbezogene Daten der Nutzer erhoben werden.

Darüber hinaus sind die Informationen in vielen Fällen inhaltlich nicht ausreichend: So genügt es nicht, wenn der Anbieter den Nutzern lediglich versichert, die „geltenden datenschutzrechtlichen Bestimmungen werden eingehalten". Die Nutzer sind vielmehr darüber zu unterrichten, welche personenbezogenen Daten jeweils in dem Angebot erhoben werden und wofür diese Daten erforderlich sind. Soweit die Verarbeitung der Daten in Staaten außerhalb des europäischen Wirtschaftsraums erfolgt, sind die Nutzer auch hierüber zu unterrichten.

Datenschutz im Urheberrechts-Management

Zunehmend werden im Internet urheberrechtlich geschützte Werke in digitaler Form verbreitet. Dies betrifft Druckwerke und Musiktitel, aber auch Videofilme. Hierzu haben sich spezielle Tauschbörsen im Internet etabliert, die es den Nutzern erlauben, solche Werke im Internet zum Abruf bereitzustellen bzw. von anderen dort zur Verfügung gestellte Werke abzurufen. Die erweiterten Verbreitungsmöglichkeiten für urhe-

berrechtlich geschützte Werke im Internet haben die Rechteinhaber und deren Verwertungsgesellschaften auf den Plan gerufen, die bereits seit längerer Zeit darüber klagen, dass ihnen durch die unkontrollierbare Verbreitung von Werken im Internet Vergütungen für die Nutzung dieser Werke in erheblicher Höhe verloren gehen.

Bisher wurde die analoge Verbreitung solcher Werke überwiegend durch die Erhebung von Pauschalabgaben auf Leermedien (z. B. unbespielte Audio- oder Videokassetten, Fotokopiergeräte) abgegolten. Zur Kontrolle der digitalen Verbreitung und Nutzung urheberrechtlich geschützter Werke im Internet bemüht sich die Industrie seit einigen Jahren um die Entwicklung von Urheberrechtsmanagement-Systemen, die eine Kontrolle der Nutzung dieser Werke und deren Vergütung zum Ziel haben.

Mit der Einführung solcher *Urheberrechtsmanagementsysteme* können erhebliche Gefährdungen für die Privatsphäre der Nutzer verbunden sein, wenn personenbezogene Informationen über die Nutzung einzelner Werke zur Kontrolle dieser Nutzung und deren Vergütung durch die Rechteinhaber oder deren Beauftragte erhoben und verarbeitet werden. Wenn dies geschieht, könnte zukünftig nachvollzogen werden, wer zu welchem Zeitpunkt und mit welchen Nutzungsrechten bestimmte Inhalte aus dem Internet genutzt hat, welche Zeitungsartikel er oder sie gelesen hat, welche Musikstücke eine bestimmte Person interessieren und welche Videofilme oder Fernsehsendungen er oder sie bevorzugt. Das Ergebnis wäre ein Mediennutzungsprofil von Einzelpersonen in einem bisher nicht denkbaren Ausmaß.

Die Bundesregierung hat zur Umsetzung der EU-Urheberrechtslinie 2001/29/EG einen „Entwurf eines Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft" vorgelegt[138].

In ihrem Gesetzentwurf hält die Bundesregierung weitgehend an dem bisherigen System der Pauschalvergütung auch für digitale Privatkopien fest. Demgegenüber hatten im Gesetzgebungsverfahren Gerätehersteller, Rechteinhaber und deren Verbände wiederholt gefordert, das dort als nicht mehr zeitgemäß empfundene Pauschalvergütungssystem durch die individuelle Lizenzierung von Nutzungsrechten unter Nutzung digitaler Urheberrechtsmanagement-Systeme zu ersetzen. Auch der Bundesrat hat sich in seiner Stellungnahme zum Gesetzentwurf der Bundesregierung für den Vorrang der individuellen Lizenzierung vor einer Pauschalvergütung eingesetzt[139], aber gleichzeitig die Gewährleistung ausreichenden Schutzes der Nutzer vor

[138] BT-Drs. 15/38

[139] vgl. BR-Drs. 684/02 (Beschluss), S. 6, Nr. 3 d)

Ausspähung personenbezogener Daten über die individuelle Nutzung von Werken und die Erstellung von Nutzerprofilen betont.

Die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25. Oktober 2002 hat in einer Entschließung[140] darauf hingewiesen, dass der Bundesgerichtshof eine individuelle Überprüfung des Einsatzes von analogen Kopiertechniken durch Privatpersonen zur Durchsetzung von urheberrechtlichen Vergütungsansprüchen als unvereinbar mit dem verfassungsrechtlichen Schutz der persönlichen Freiheitsrechte der Nutzerinnen und Nutzer bezeichnet hat. Diese Feststellung behält auch unter den Bedingungen der Digitaltechnik und des Internet ihre Berechtigung. Die Konferenz hat den Gesetzgeber darin bestärkt, an diesem bewährten, datenschutzfreundlichen Verfahren festzuhalten. Wenn die Pauschalvergütung durch eine individuelle Lizenzierung abgelöst werden soll, so muss sichergestellt werden, dass die urheberrechtliche Vergütung aufgrund von statistischen und anonymisierten Angaben über die Nutzung einzelner Werke erhoben wird. Auch technische Systeme zur digitalen Verwaltung digitaler Rechte müssen datenschutzfreundlich gestaltet werden.

Bereits im August 2001 waren Fragen des Datenschutzes und des geistigen Eigentums im Internet auf einem Symposium des Berliner Beauftragten für Datenschutz und Informationsfreiheit im Rahmen der Internationalen Funkausstellung Berlin 2001 erörtert worden.

Multimedia Messaging Service – Audio- und Videoüberwachung für jedermann?

Neu auf dem Markt eingeführt wurde im zurückliegenden Berichtszeitraum der *„Multimedia Messaging Service"* (MMS). Damit können Besitzer von Mobilfunkgeräten elektronische Nachrichten verschicken, die neben Texten auch Bilder, Audio-Dateien oder sogar Videosequenzen enthalten können. Endgeräte, die die hierzu notwendigen Aufzeichnungsmöglichkeiten bieten, sind bereits am Markt erhältlich. Pressemeldungen zufolge soll die Anzahl der Benutzer im Ausland, z. B. in Japan, bereits mehrere Millionen betragen[141].

Die aufgezeichneten Bilder und Audiosequenzen können sowohl direkt vom Endgerät aus an andere Mobilfunkteilnehmer, die über ein MMS-fähiges Endgerät verfügen, verschickt oder auch per E-Mail auf Personalcomputern oder ähnlichen Geräten weiterverarbeitet werden.

Risiken für den Datenschutz können hier insbesondere

---

[140] Entschließung zur datenschutzgerechten Vergütung für digitale Privatkopien im neuen Urheberrecht, vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2002", S. 29

[141] Der Spiegel 47/2002, S. 127

dann entstehen, wenn solche Aufnahmen heimlich gefertigt werden. Immerhin hat jeder Besitzer eines MMS-fähigen Endgerät potenziell gleichzeitig auch eine Videoüberwachungsanlage und ein Abhörgerät in der Tasche. Zwar stellt die Veröffentlichung aufgezeichneter Bilder oder Videosequenzen, auf denen Personen identifiziert werden können, in vielen Fällen einen Verstoß gegen das Kunsturhebergesetz dar und die heimliche Aufzeichnung von Audiosequenzen steht unter Umständen nach § 201 Strafgesetzbuch unter Strafe. Dennoch sollten die Hersteller das ihre dazu tun, dass solche heimlichen Aufzeichnungen gar nicht erst möglich gemacht werden. Dies kann u. a. dadurch erfolgen, dass – z. B. im Falle der Videoaufzeichnung und des Fotografierens – der Aufzeichnungsvorgang durch einen Warnton signalisiert wird.

Location based services

Bereits in unserem letzten Jahresbericht hatten wir über die Verwendung von Aufenthaltsinformationen in mobilen Kommunikationsdiensten *(Location based services)* berichtet[142]. Diese Dienste haben sich auch im zurückliegenden Berichtszeitraum weiter ausgebreitet. Beinahe alle Netzanbieter im Mobilfunk bieten unterdessen mobile Dienstleistungen an, bei denen der Nutzer auf Grundlage des Standorts des Mobilfunkgeräts in der Nähe gelegene Orte wie Restaurants, Geldautomaten, Apotheken, Hotels oder Pensionen auffinden kann. Die Dienste werden größtenteils unter Nutzung von SMS (Short Messaging Service) oder WAP (Wireless Access Protocol) angeboten. Darüber hinaus sind auch weitere Dienste für mobile Endgeräte am Markt erhältlich, z. B. Navigationssysteme, Stadtpläne und Landkarten sowie Fahrplanauskunftsdienste, die ebenfalls Standortinformationen nutzen.
Zusätzlich existieren Dienste, mit denen ermittelt werden kann, ob sich Freunde oder Bekannte, die diesen Dienst auf ihren Endgeräten freigeschaltet haben, in der Nähe befinden.

Notwendige Voraussetzung für die Übermittlung und Nutzung von Standortdaten zur Erbringung aufenthaltsbasierter Dienstleistungen ist in jedem Fall die vorherige Einwilligung des Nutzers. Gleichzeitig ist eine vorherige Unterrichtung des Nutzers über Art, Umfang und Zweck der Erhebung, Verarbeitung und Nutzung seiner Daten erforderlich.

Auch Anbieter aufenthaltsbasierter Dienstleistungen haben die Grundsätze zur Datenvermeidung und Datensparsamkeit (§ 3 a BDSG) zu beachten. Anbieter von Tele- und Mediendiensten müssen auch standortbezogene Dienste ihren Nutzern anonym oder unter Pseudonym anbieten, soweit dies technisch möglich

[142] JB 2001, 5.1

und zumutbar ist (§ 4 Abs. 6 TDDSG, § 13 Abs. 1 MDStV).

Eine datenarme Gestaltung aufenthaltsbasierter mobiler Dienstleistungen ist auch im Interesse der Anbieter, da dies von ihnen als Qualitätsmerkmal des Dienstes vermarktet werden kann. Die Vorstellung, mit einem Mobilfunkgerät ständig geortet werden zu können, dürfte ansonsten bei zahlreichen Nutzern zu einer eher zurückhaltenden Inanspruchnahme solcher Dienstleistungen führen.

Die bis zum 31. Oktober 2003 durch die Mitgliedstaaten der Europäischen Union umzusetzende neue Telekommunikationsrichtlinie sieht vor, dass auch in den Fällen, in denen der Nutzer eine Einwilligung zur Verarbeitung von Standortdaten gegeben hat, auch weiterhin die Möglichkeit bestehen muss, die Verarbeitung solcher Daten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise und gebührenfrei zeitweise zu untersagen (Art. 9 Abs. 2 Richtlinie). Auch diese Regelungen sollten Anbieter von aufenthaltsbasierten, mobilen Diensten bereits jetzt bei der Gestaltung ihrer Dienste beachten.

6. Aus der Dienststelle

6.1 Entwicklung

Die Stelle der Bereichsleitung Recht konnte auch im vergangenen Jahr nicht ordnungsgemäß besetzt werden, was naturgemäß die Arbeit erschwerte. Angesichts der Haushaltslage konnten die Belastungen, die in den vergangenen Jahren durch das Informationsfreiheitsgesetz und die Einführung der Amtsaufsicht bei nichtöffentlichen Stellen eingetreten waren, nicht durch zusätzliche Stellen ausgeglichen werden[143]. Die schrittweise Einführung eines Bürgeroffice mit Jahresbeginn, in dem der persönliche und schriftliche Bürgerkontakt gebündelt werden, soll zu einer Entlastung der Arbeitsgebiete führen und mehr Prüfungen von Amts wegen ermöglichen[144].

Die räumlichen Voraussetzungen hierfür werden sich deutlich verbessern, wenn die Dienststelle Mitte des Jahres in neue Diensträume (An der Urania 2 - 12, 10787) umziehen wird. Nach über 20 Jahren werden wir damit in einem landeseigenen Gebäude untergebracht, das im Übrigen vom Rechnungshof und der Landeszentrale für Politische Bildung belegt wird.

6.2 Aufgaben

Die Arbeitsgebiete Gesundheit und Soziales sowie Wirtschaft wiesen im vergangenen Jahr die meisten Vorgänge auf, gefolgt von den Arbeitsgebieten Tele-

---

[143] JB 2001, 6.1

[144] zur Neuorganisation vgl. den neuen Geschäftsverteilungsplan, Anhang 3

kommunikation und Medien sowie Wissenschaft, Forschung und Statistik. Der stärkste Anstieg war im Bereich Internationaler und Europäischer Datenschutz zu verzeichnen, in dem sich die Anzahl der Vorgänge fast verdoppelt hat. Rückläufig ist dagegen die Zahl der Vorgänge im Bereich Innere Sicherheit, obwohl mit der Gesetzgebung zur Terrorismusbekämpfung und der Durchführung der Rasterfahndung gerade in diesem Bereich Probleme des Datenschutzes in der Öffentlichkeit große Beachtung fanden.

6.3 Zusammenarbeit mit dem Parlament

Zu Beginn der Legislaturperiode konstituierte sich der nunmehr so benannte „Unterausschuss Datenschutz und Informationsfreiheit" neu. Ihm gehören unter dem Vorsitz der Abgeordneten Marion Seelig (PDS), die seit der Wiedervereinigung dem Unterausschuss angehört, sowie der Schriftführung des Abgeordneten Peter Trapp (CDU), der in der vergangenen Legislaturperiode den Vorsitz innehatte, die Abgeordneten Dr. Fritz Felgentreu (SPD), Alexander Ritzmann (FDP), Wolfgang Wieland (BÜNDNIS 90/DIE GRÜNEN), Minka Dott (PDS), Thomas Kleineidam (SPD) und Frank Zimmermann (SPD) an. Für den Abgeordneten Roland Gewalt rückte der Abgeordnete Ulrich Brinsa (CDU) nach. Im Jahr 2002 wurden elf Sitzungen abgehalten, in denen im Wesentlichen der Jahresbericht 2000 erörtert wurde. Insgesamt wurden sechs Beschlüsse zu verschiedenen Geschäftsbereichen gefasst, die in der Plenarsitzung am 12. Dezember 2002 angenommen wurden[145]. Bei dieser Gelegenheit hielten der Berliner Beauftragte für Datenschutz und Informationsfreiheit sowie die Vorsitzende des Unterausschusses Reden, die insbesondere die konstruktive Zusammenarbeit in diesem Gremium hervorhoben[146].

6.4 Kooperation mit anderen Datenschutzbehörden

Das Datenschutzgesetz verpflichtet zur Zusammenarbeit mit allen Stellen, die mit Kontrollaufgaben des Datenschutzes betraut sind (§ 24 Abs. 4 BlnDSG). In der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die im vergangenen Jahr unter dem Vorsitz des Landesbeauftragten für den Datenschutz Rheinland-Pfalz, Prof. Dr. Walter Rudolf, in Mainz (7./8.März) und Trier (24./25. Oktober) tagte, wurde erneut eine Reihe von Beschlüssen gefasst, die die Fortentwicklung des Datenschutzes fördern sollten[147]. Die Ergebnisse sind im Bericht dargestellt worden. Im laufenden Jahr hat der Sächsische Datenschutzbeauftragte, Dr. Thomas Giesen, den Vorsitz übernommen.

---

[145] vgl. Anhang 1

[146] vgl. Anhang 2

[147] vgl. Anlagenband „Dokumente zu Datenschutz und Informationsfreiheit 2002", S. 9 ff.

Die Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands, der die Datenschutz- und Informationsfreiheitsbeauftragten der Bundesländer Berlin, Brandenburg, Nordrhein-Westfalen und Schleswig-Holstein angehören, fasste Entschließung zu mehr Transparenz bei Verwaltungsvorschriften (16./17. Mai in Düsseldorf) und zur Korruptionsbekämpfung (20. November in Potsdam)[148].

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

Für den Bereich der Aufsicht über Privatunternehmen wurde die Koordinierung im „Düsseldorfer Kreis", dem Gremium der Obersten Aufsichtsbehörden für den Datenschutz, wahrgenommen. Den Vorsitz führte das Innenministerium Baden-Württemberg. Im laufenden Jahr hat Berlin den Vorsitz übernommen.

Im Düsseldorfer Kreis hat der Berliner Beauftragte für Datenschutz und Informationsfreiheit den Vorsitz in den Arbeitsgruppen „Internationaler Datenverkehr" sowie „Telekommunikation, Tele- und Mediendienste". Über die Ergebnisse wurde oben berichtet[149].

Auf europäischer Ebene ist der Berliner Beauftragte für Datenschutz und Informationsfreiheit deutscher Ländervertreter in der Artikel-29-Datenschutzgruppe, der alle europäischen Datenschutzinstitutionen angehören - seit Beginn des Jahres auch diejenigen aller Beitrittsländer - und die die Europäische Datenschutzkommission in Datenschutzfragen berät.

Die Internationale Arbeitsgruppe Datenschutz in der Telekommunikation, die im Rahmen der Internationalen Konferenz der Datenschutzbeauftragten unter unserem Vorsitz arbeitet, hatte wie immer zwei Sitzungen. In der Tagung in Auckland/Neuseeland am 26./27. März 2002 wurden Arbeitspapiere u. a. zur Überwachung im Internet, zum Schutz von Kindern bei Nutzung des Internet sowie zur Telemedizin verabschiedet[150]. Bei der Sitzung in Berlin am 11./12. November 2002 wurden die vorausgegangenen Diskussionen weitergeführt. Wie stets wurden die Arbeitsergebnisse auf der Europäischen Datenschutzkonferenz am 24./26. April 2002 in Bonn sowie der Internationalen Konferenz der Datenschutzbeauftragten am 9./11. September 2002 in Cardiff vorgestellt.

6.5 Europäische Akademie für Informationsfreiheit und Datenschutz

Seit Jahren ist im Kreis der europäischen Datenschutzinstitutionen der Wunsch geäußert worden, eine Institu-

[148] vgl. Anlagenband, a. a. O., S. 92 f.

[149] vgl. 4.7.3 sowie 5.

[150] vgl. Anlageband, a. a. O., S. 70 ff.

tion ins Leben zu rufen, die neben den regelmäßig stattfindenden Konferenzen eine beständige Plattform für Informationsaustausch, Koordinierung und Fortbildung bildet. Interesse bestand vor allem auch daran, die mittel- und osteuropäischen Institutionen einzubinden. Aufgrund der Erfahrungen, die wir in den vergangenen 20 Jahren im internationalen Bereich gewonnen haben, sowie aufgrund seiner geografischen Lage zwischen Ost und West wurde Berlin gefragt, ob nicht hier eine entsprechende Einrichtung geschaffen werden könnte.
Nach vielen Monaten der Vorbereitung ist am 9. April 2002 unter unserer Beteiligung ein Trägerverein für eine *Europäische Akademie für Informationsfreiheit und Datenschutz* (EAID) gegründet worden. Zielsetzungen sind u. a.:

- die staatenübergreifende Fortbildung der Allgemeinheit auf dem Gebiet von Informationsfreiheit und Datenschutz in Europa durch öffentliche Veranstaltungen,

- der Erfahrungsaustausch zwischen europäischen Entscheidungsträgern auf dem Gebiet von Informationsfreiheit und Datenschutz,

- die Mitwirkung bei der Rechtsangleichung in Beitrittsländern zur EU im Bereich der Informationsgesellschaft,

- der Erfahrungsaustausch über technische Aspekte von Informationsfreiheit und Datenschutz.

Mit der Europäischen Akademie Berlin, die der EAID ihre vorzüglichen Tagungseinrichtungen sowie logistische Hilfeleistung zur Verfügung stellt, wurde eine Kooperationsvereinbarung geschlossen.

Die Eröffnungsveranstaltung der Akademie am 17. Juni 2002 fand großes nationales und internationales Interesse bei der Datenschutzgemeinde. Der Senator für Inneres begrüßte die neue Aktivität in Berlin. Der Präsident der italienischen Datenschutzkommission, Prof. Dr. Stefano Rodota, der Direktor der norwegischen Datenschutzkommission, Georg Apenes, der Bundesbeauftragte für den Datenschutz, Dr. Joachim Jacob, sowie der Konzernbeauftragte der DaimlerChrysler AG, Prof. Dr. Alfred Büllesbach, sprachen Grußworte. In einem Festvortrag stellte Prof. Dr. Michael Kloepfer von der Humboldt-Universität Informationsfreiheit und Datenschutz als die beiden Säulen der Informationsgesellschaft dar.

Der Akademiebetrieb wurde am 25./26. November 2002 mit dem *Complaints Handling Workshop* der Europäischen Datenschutzkonferenz aufgenommen. Im laufenden Jahr folgen Veranstaltungen zur Informationsfreiheit, zum Identitätsmanagement im Internet und zu verbindlichen Unternehmensregelungen zum Datentransfer in Drittländer. Im November wird die Konfe-

renz der mittel- und osteuropäischen Datenschutzbeauftragten ihre halbjährliche Sitzung in der Akademie abhalten.

6.6 Öffentlichkeitsarbeit

Auch im vergangenen Berichtszeitraum konnten wir ein wachsendes Interesse der Bürgerinnen und Bürger am Thema Datenschutz beobachten. Insofern hat sich die Tendenz der vergangenen Jahre positiv fortgesetzt. Belegt wird das zunehmende Informationsbedürfnis nicht nur durch die steigende Anzahl von schriftlichen und telefonischen Anfragen, die uns erreichen, sondern auch durch die große Zahl von „Hits", die monatlich auf unser Internetprogramm zugreifen. Bedingt durch den Erfolg unserer Website rückt das Medium Internet zunehmend in den Mittelpunkt unserer Öffentlichkeitsarbeit. Insofern war es folgerichtig, diesen Ansatz auch für unser Anliegen, für die Informationsfreiheit zu werben, ihre Potenziale für ein demokratisches Gemeinwesen darzustellen und über Entwicklungen in diesem Bereich zu informieren, zu nutzen. Ein wichtiges Instrument hierfür ist unser neues Internetangebot, das am 1. November 2002 online ging. Neben Informationen zu den gesetzlichen Grundlagen des Akteneinsichtsrechts in Berlin, Hilfestellungen zur Antragstellung und Auslegungshinweisen zu den rechtlichen Vorgaben enthält es auch umfangreiche Linksammlungen zur Informationsfreiheit in Deutschland, Europa und weltweit. Rechtliche Stellungnahmen und Hinweise zur Anwendung des IFG werden stetig ergänzt.

Ergänzend zu unseren Online-Aktivitäten haben wir im vergangenen Jahr einige Broschüren selbst herausgegeben bzw. waren an der Entwicklung und Herausgabe von Gemeinschaftspublikationen mit anderen Datenschutzbeauftragten beteiligt.

In unserer Schriftenreihe *„Ratgeber zum Datenschutz"* bieten wir kurze, allgemein verständliche Informationen und Hilfe zur Selbsthilfe bei ausgewählten Datenschutzthemen an. Ein Thema, das uns immer wieder begegnet und viele interessierte Bürgerinnen und Bürger berührt, ist der Adressenhandel. Dies hat uns veranlasst, den „Ratgeber zum Datenschutz Nr. 2 - Adressenhandel und Umgang mit unerwünschter Werbung" zu überarbeiten und als Neufassung herauszugeben. In unserer Schriftenreihe „Materialien zum Datenschutz" haben wir – in Kooperation mit dem Hessischen Datenschutzbeauftragten - den Band Nr. 28 „Datenschutz in Wissenschaft und Forschung" als überarbeitete Neuauflage veröffentlicht.

Unter der Leitung des Landesbeauftragten für den Datenschutz Niedersachsen waren wir an einer Arbeitsgruppe beteiligt, die Handlungsempfehlungen für ein „Datenschutzgerechtes eGovernment" erarbeitet und herausgegeben hat. Die Handreichung soll dazu beitragen, dass bei der Entwicklung von eGovernment-Lösungen die Anforderungen von Datenschutz und

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Datensicherheit Berücksichtigung finden und praktische Anleitung dafür geben, wie diese Anforderungen in datenschutzgerechte und datenschutzfreundliche Anwendungen umgesetzt werden können.

Erstmals haben wir im Jahr 1998 in einer Gemeinschaftsarbeit mit dem Brandenburgischen Datenschutzbeauftragten über die Ergebnisse der datenschutzrechtlichen Koordinierungsgremien auf Bundes-, Europa- und internationaler Ebene berichtet. Diese Zusammenarbeit hat sich in den nachfolgenden Jahren – nicht nur aus Gründen der Kostenreduzierung – bewährt und wurde im Berichtszeitraum fortgesetzt. Als Ergänzung zum vorliegenden Bericht erscheint in der Reihe die Broschüre „Dokumente zu Datenschutz und Informationsfreiheit 2002". Sie enthält die relevanten Beschlüsse und Entscheidungen der „Konferenz der Datenschutzbeauftragten des Bundes und der Länder", der „Arbeitsgruppe der Obersten Aufsichtsbehörden für den Datenschutz („Düsseldorfer Kreis")", der „Konferenz der Europäischen Datenschutzbeauftragten", der „Konferenz der Internationalen Datenschutzbeauftragten", der „Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation", der „Arbeitsgemeinschaft der Informationsbeauftragten in Deutschland" sowie „Fragen von Datenschutzbeauftragten an die Parteien zur Bundestagswahl 2002" und die „Empfehlung des Ministerausschusses an die Mitgliedstaaten des Europarats zum Zugang zu amtlichen Dokumenten".

Berlin, den 25. März 2003

Prof. Dr. Hansjürgen Garstka
Berliner Beauftragter für Datenschutz
und Informationsfreiheit

Berlin, den 3. Juni 2003

Der Senat von Berlin
Klaus Wowereit
Regierender Bürgermeister