Abgeordnetenhaus von Berlin **Drucksache 15 / 591**

15. Wahlperiode

Vorlage – zur Kenntnisnahme –

über **Stellungnahme des Senats zum Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2001**

Der Senat legt nachstehende Vorlage dem Abgeordnetenhaus zur Besprechung vor:

Gemäß § 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 18. Juni 2002

Der Senat von Berlin

Wowereit
Regierender Bürgermeister

Die Veröffentlichungen 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 2001

(gemäß § 29 Abs. 2 Berliner Datenschutzgesetz)

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

1. Rechtliche Rahmenbedingungen

1.1 Deutschland

Fortschritte und Rückschläge

Aus der Sicht des Datenschutzes stand das Jahr 2001 zunächst unter einem guten Stern: Kurz vor Jahresbeginn war das Grundrecht auf Datenschutz in die am 7. Dezember 2000 proklamierte Europäische Charta der Grundrechte aufgenommen worden. Seither ist europaweit unumstößlich, dass jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht (Art. 8).

Über zwei Jahre nachdem die Europäische Datenschutzrichtlinie[1] in deutsches Recht hätte umgesetzt werden müssen, ist am 23. Mai das neue Bundesdatenschutzgesetz (BDSG) in Kraft getreten[2]. Auch die überwiegende Mehrheit der Länder hat inzwischen ihr Datenschutzrecht an die Europäische Richtlinie angepasst, das Berliner Abgeordnetenhaus verabschiedete das neue Berliner Datenschutzgesetz (BlnDSG) am 12. Juli[3].

Als die derzeitige Bundesregierung 1998 entschied, den vorgefundenen Gesetzentwurf zur Grundlage des künftigen Gesetzes zu machen, war ihr, der in der Fachöffentlichkeit einhellig vertretenen Meinung folgend, klar, dass dieser Entwurf weder die Europäische Richtlinie optimal umsetzt noch den Erfordernissen der modernen Informationsgesellschaft gerecht wird. Um die Umsetzungsfrist nicht noch weiter zu überschreiten, wurde der Entwurf überarbeitet und ergänzt, aber trotz seiner Mängel dem Parlament zugeleitet und nach relativ ruhiger Debatte verabschiedet. Gleichzeitig wurde ein Gutachterausschuss eingesetzt mit dem Auftrag, Grundzüge für die Modernisierung des Datenschutzrechts[4] zu erarbeiten. Obwohl das Gutachten bereits im September 2001 fertiggestellt war, wurde es erst am 12. November dem Bundesinnenministerium übergeben: Der Terroranschlag vom 11. September 2001 hatte sofort eine Debatte über die Rolle des Datenschutzes ausgelöst, die es zunächst inopportun erscheinen ließ, die Modernisierung des Datenschutzes öffentlich zu thematisieren.

Der Bericht enthält umfangreiche Darstellungen der Rechtsentwicklung des Datenschutzes auf Bundesebene und in Europa, hinsichtlich derer der Senat je nach Erfordernis im Einzelfall Stellung nimmt.

[1] 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 Nr. L 281
[2] Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18. Mai 2001, BGBl. S. 904–928
[3] Gesetz zur Änderung des Berliner Datenschutzgesetzes und anderer datenschutzrechtlicher Regelungen vom 30. Juli 2001, GVBl. S. 305–312
[4] Roßnagel, Alexander; Pfitzmann, Andreas; Garstka, Hansjürgen: Modernisierung des Datenschutzrechts. Berlin: Bundesministerium des Innern, 2001

Obwohl niemand die Unfähigkeit der Sicherheitsbehörden, dieses monströse Verbrechen vorauszusehen oder gar zu verhindern, mit datenschutzrechtlichen Schwierigkeiten belegen konnte, wurde der Datenschutz zu einem der Sündenböcke gestempelt. Bereits wenige Tage nach dem Anschlag ließ der Bundesinnenminister verkünden, der Datenschutz sei zu überprüfen und „dort zu lockern, wo Datenschutz zu Terroristenschutz“ werde[5] – eine Äußerung, die selbst die Polemik der Sicherheitspolitiker in den Anfangstagen des Datenschutzes übertraf, in denen die Terroranschläge der RAF die Schlagzeilen beherrschten.

Die Folge war die in kürzester Zeit durchgepeitschte Verabschiedung des Terrorismusbekämpfungsgesetzes am 7. Dezember[6], mit dem eine Vielzahl neuer, bisher nicht für möglich gehaltener Eingriffe in die informationelle Selbstbestimmung vorgenommen wurde, ohne dass ein großer Teil davon auch das mindeste mit dem aktuellen Anlass zu tun hatte. „Jetzt weht der Wind, jetzt gehen wir segeln“, hat der Staatsrechtler Prof. Michael Kloepfer von der Humboldt-Universität das auf den Nenner gebracht, was geschehen war: In der dem rechtsstaatlichen Denken zutiefst zuwiderlaufenden Überzeugung, auf nicht beherrschte Situationen müsse sofort der Gesetzgeber tätig werden, statt dass Mängel bei der Nutzung der bestehenden Befugnisse analysiert werden, wurde eine Vielzahl von Gesetzgebungsvorschlägen im Bereich der Sicherheits- und Ausländerbehörden aus den letzten Jahren herausgekramt und dem Gesetzgeber vorgelegt. Dass das Bundesjustizministerium den Entwurf in weitgehenden Passagen für verfassungswidrig hielt, beeindruckte offensichtlich weder Bundesregierung noch Parlament.

Das neue Bundesdatenschutzgesetz

Primärer Anlass für die nunmehr dritte grundsätzliche Novellierung des Bundesdatenschutzgesetzes war die Verpflichtung zur Anpassung des deutschen Datenschutzrechtes an die Europäische Datenschutzrichtlinie. Ob dies gelungen ist, muss sich erst noch erweisen. Bisher liegt hierzu noch keine Äußerung der Europäischen Kommission vor, die im Rahmen des Notifizierungsverfahrens eine entsprechende Bewertung vornimmt. In einer Vorabmitteilung zeichnet sich allerdings schon ab, dass die Aufrechterhaltung der Möglichkeit, die Aufsichtsbehörde für den privaten Bereich in den Innenministerien anzusiedeln und diesen damit keine „völlige Unabhängigkeit“ (Art. 28 Abs. 1 Europäische Datenschutzrichtlinie) zu gewähren, mit den europäischen Vorgaben nicht vereinbar ist. Auch andere Bestimmungen lassen Zweifel über die Konformität aufkommen, etwa die unterschiedliche Behandlung des Datenschutzes im öffentlichen und nicht-öffentlichen Bereich, die von der Richtlinie teilweise stark abweichenden Begriffsbestimmungen, von denen auch der Geltungsbereich des Gesetzes abhängt, die Einschränkungen von Informations- und Auskunftsrechten ge-

[5] Besonnene Entschlossenheit: In: FAZ vom 18. September 2001, S. 4
[6] Gesetz zur Bekämpfung des internationalen Terrorismus vom 9. Januar 2002, BGBl. I. S. 361-395

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

genüber der Richtlinie oder das Fehlen von „wirksamen Einwirkungsbefugnissen“ der Kontrollstellen.

Dessen ungeachtet ist die überwiegende Mehrzahl der Richtlinienvorgaben, die im deutschen Recht bisher fehlten oder abweichend geregelt waren, eingearbeitet worden. Dies betrifft insbesondere die herausgehobene Stellung „besonderer Arten personenbezogener Daten“ über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben (§ 3 Abs. 9), verschärfte Anforderungen an die Einwilligung (§ 4 a), den internationalen Datenverkehr (§§ 1 Abs. 5, 4 b, 4 c), das eingeschränkte Verbot automatisierter Einzelentscheidungen (§ 6 a) und die Verpflichtung der verantwortlichen Stellen zu Vorabkontrollen bei besonders sensiblen Verfahren (§ 4 d Abs. 5,6).

Der deutsche Gesetzgeber hat von der Möglichkeit Gebrauch gemacht, die von der Richtlinie grundsätzlich vorgesehenen weitgehenden Registrierungspflichten, die einen hohen bürokratischen Aufwand bedeuten, durch eine Stärkung der betrieblichen und behördlichen Datenschutzbeauftragten auf ganz wenige Fälle zu beschränken[7]. Diese werden künftig eine erheblich größere Rolle bei der Beratung und Kontrolle spielen (§§ 4 e-g). Die Aufsichtsbehörden erhielten die Befugnis, künftig auch im privaten Bereich von Amts wegen tätig zu werden, was zu einer deutlichen Ausweitung der Datenschutzkontrollen bei Privatunternehmen führen muss (§ 38). Gestärkt werden die Aufsichtsbehörden durch die Möglichkeit, Verstöße gegen das BDSG als Ordnungswidrigkeiten zu ahnden und mit Bußgeldern bis zu 250 000 € zu belegen (§ 43).

Die Novelle des BDSG beschränkt sich nicht auf die Anpassung an die Europäische Richtlinie, sondern sie greift die Tendenz der aktuellen Datenschutzdebatte auf, deutlich mehr Gewicht auf die datenschutzgerechte Ausgestaltung der Technik und der Verfahren selbst zu legen („Systemdatenschutz“). So wurde aus dem Tele- und Mediendiensterecht der Grundsatz der Datenvermeidung und Datensparsamkeit einschließlich der Verpflichtung zum Angebot anonymer oder pseudonymer Verfahren übernommen (§ 3 a), die Videoüberwachung öffentlicher Räume wird erstmals (allerdings auf zweifelhafte Weise) geregelt (§ 6 b), für Chipkarten werden neue Transparenzverpflichtungen geschaffen (§ 6 c) und der Katalog der technisch-organisatorischen Maßnahmen wird einerseits gestrafft, andererseits um Verfügbarkeitskontrolle und Trennungsgebot ergänzt (§ 9 mit Anlage).

Modernisierung des Datenschutzrechts

Ausgangspunkt des Gutachtens zur Modernisierung des Datenschutzrechts („2. Stufe“ der BDSG-Novellierung) war die Feststellung, dass das bisherige Datenschutzrecht in Deutschland den Gegebenheiten der modernen Datenverarbeitung nicht mehr gerecht wird. Insbeson-

Das umfangreiche Gutachten zur Modernisierung des Datenschutzrechts stellt einen wichtigen Beitrag für die Diskussion über die sogenannte 2. Stufe der BDSG-Novellierung dar, die aufgrund der rasanten technologischen Entwicklung und zur Vereinfachung des Da-

[7] vgl. 4.8.2

dere werden die Gefahren und die Chancen neuer Techniken nur ungenügend berücksichtigt. Die Anwendung datenschutzrechtlicher Regelungen wirft angesichts widersprüchlicher Bestimmungen und der Unübersichtlichkeit durch die Normierung in Hunderten von bereichsspezifischen Gesetzen große Schwierigkeiten auf. Daher steht auch eine Vereinfachung dieses Rechtsbereiches im Mittelpunkt der Überlegungen.

Diese kann dem Gutachten zufolge zunächst durch einen Paradigmenwechsel in der Gesetzessystematik zum Datenschutzrecht erfolgen. Im Mittelpunkt sollte ein allgemeines Gesetz stehen, das grundsätzliche und präzise Regelungen der Verarbeitung personenbezogener Daten enthält und in dem sich möglichst wenige offene Abwägungsklauseln finden. In diesem Gesetz sollten sich auch Regelungen zur Technikgestaltung, zur Datensicherung, zur Datenschutzorganisation, zur Datenschutzkontrolle und zur Selbstregulierung finden. Nur für die Bereiche, die aufgrund ihrer besonderen Aufgaben oder der besonderen Sensitivität der Daten spezifischer Bestimmungen zum Datenschutz bedürfen – z. B. Sicherheitsbereich - sollten bereichsspezifische Ausnahmen gelten. Die eigenständige Regelung des Telekommunikations- und Teledienstedatenschutzrechts sollte aufgegeben und auch diese Bereiche in das Bundesdatenschutzgesetz integriert werden, wobei das in diesen Bereichen erreichte hohe Niveau des Datenschutzes maßgebend für ein künftiges Bundesdatenschutzgesetz sein muss.

Angesichts der vielfältigen Verarbeitung personenbezogener Daten lediglich für das Erbringen technischer Leistungen wird vorgeschlagen, in einem neuen Datenschutzrecht zwei Kategorien der Datenverarbeitung zu unterscheiden: Zum einen die Verarbeitung mit gezieltem Personenbezug zum Zweck der personenbezogenen oder personenbeziehbaren Verwendung (z. B. Personalakten, Vertragsdaten, Bestandsdaten), zum anderen die Verarbeitung ohne gezielten Personenbezug zu anderen Zwecken als der personenbezogenen oder personenbeziehbaren Verwendung, welche sich insbesondere auf die Erbringung technischer Dienstleistungen oder die Kommunikation von Maschine zu Maschine bezieht. Unter der Voraussetzung, dass diese Daten auf das erforderliche Minimum begrenzt werden, sie einer strikten Zweckbindung unterliegen und nach der Verarbeitung sofort gelöscht werden, könnten dann für die Datenverarbeitung ohne gezielten Personenbezug geringere Anforderungen gelten.

Dem Wesen der heutigen Informationsgesellschaft widerspricht es, die Verarbeitung personenbezogener Daten weiterhin einem Verbot mit Erlaubnisvorbehalt zu unterstellen. Daher sollte künftig ein genereller Erlaubnistatbestand die Datenverarbeitung für zulässig erklären, wenn offenkundig keine Beeinträchtigung der betroffenen Person zu erwarten ist und die normierten Grundsätze der Datenverarbeitung berücksichtigt werden. Damit einhergehen muss die Stärkung der Selbstbestimmung der betroffenen Person. Einwilligung oder tenschutzrechts dringend geboten erscheint. Der Bund und die Länder sind aufgefordert, die in dem Gutachten unterbreiteten Vorschläge zu prüfen und zu bewerten. Der sich daran anschließende Diskussions- und Abstimmungsprozess zwischen Bund und Ländern wird zeigen, in welchem Umfang sich die unterbreiteten Vorschläge realisieren lassen und Eingang in einen Referentenentwurf auf Bundesebene zur Novellierung des BDSG finden werden. Eine Bewertung der Vorschläge im einzelnen kann und soll vor diesem Hintergrund hier nicht erfolgen.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Einwilligungssurrogate, etwa in Form eines Vertrages oder eines Antrags gegenüber einer Behörde, sollten grundsätzlich die Voraussetzung einer rechtmäßigen Datenverarbeitung sein. Ein besonderes Augenmerk muss dabei der Freiwilligkeit der Einwilligung gelten, die immer dann gefährdet ist, wenn der Betroffene in einem Abhängigkeitsverhältnis zum Datenverarbeiter steht, wie dies beispielsweise in einem Arbeitsverhältnis immer der Fall sein wird.

Spiegelbild der Einwilligung ist die strikte Zweckbindung der Datenverarbeitung. Die zur Datenverarbeitung verwendeten Produkte und die eingerichteten Datenverarbeitungsprozesse sollten so gestaltet werden müssen, dass sie nur die Maßnahmen zulassen, die dem Zweck der Datenverarbeitung entsprechen (Systemdatenschutz).

Datenverarbeitungstechnik ist nicht nur eine Gefahr für die missbräuchliche Nutzung personenbezogener Daten, sondern kann dem Anliegen des Datenschutzes weitaus mehr dienen, als dies bisher der Fall ist. Der Gesetzgeber sollte daher Regelungen vorsehen, die die Entwicklung und Herstellung datenschutzgerechter Technik fordert und fördert. Diesem Anliegen können Produktanforderungen sowie die Möglichkeit, datenschutzgerechte Technik zertifizieren zu lassen, dienen. Durch eine Verpflichtung öffentlicher Stellen, datenschutzgerechte Technik vorrangig zu verwenden, könnte der öffentliche Bereich eine Vorreiterrolle spielen.

Die Konkretisierung des gesetzlichen Rahmens könnte durch branchen- oder unternehmensspezifische Selbstregulierung erfolgen. Dies würde es der Wirtschaft ermöglichen, schneller als es im Gesetzgebungsverfahren möglich ist, passgerechte branchen- oder unternehmensbezogene verbindliche Regelungen zu entwickeln. Selbstregulierung muss aber den gesellschaftlichen Konsens im Auge behalten und daher nicht einseitig auf die Durchsetzung der Interessen eines Verbandes zielen. Anerkannte Datenschutz- und Verbraucherverbände müssten daran beteiligt werden. Darüber hinaus sollten für die Datenverarbeitung verantwortliche Stellen die Möglichkeit haben, die Datenschutzfreundlichkeit ihrer Verarbeitungen durch ein Datenschutzaudit bewerten zu lassen. Die Umsetzung dieses Vorhabens, das ein eigenes Gesetz voraussetzt und durch § 9 a BDSG bereits vorgezeichnet ist, sollte und könnte unabhängig von der Verabschiedung eines neuen Bundesdatenschutzgesetzes in Kürze erfolgen.

Die Datenschutzkontrolle könnte effektiver erfolgen, wenn auch im Bund und in den Ländern, die dies bisher noch nicht vorgesehen haben, die Kontrollstellen für den öffentlichen und nicht-öffentlichen Bereich vereinheitlicht würden. Ebenso müssen im Hinblick auf die von Art. 28 der Europäischen Datenschutzrichtlinie geforderte völlige Unabhängigkeit der Kontrollstellen die landes- und bundesgesetzlichen Regelungen zur Rechtsaufsicht über die Kontrollstellen überdacht werden. Berlin spielt in beiden Bereichen mit seinen Regelungen zur Stellung und zu den Aufgaben des Berli-

Zur Frage der Rechtsaufsicht vertritt der Senat die Auffassung, dass die von Art. 28 Abs. 1 der Europäischen Datenschutzrichtlinie geforderte völlige Unabhängigkeit der Kontrolle lediglich „Unabhängigkeit von den zu Überprüfenden“ bedeutet. Jede andere Auslegung wäre verfassungsrechtlich bedenklich, da der Berliner Beauftragte für Datenschutz und Informationsfreiheit mit der Kontrolle der Privatwirtschaft Exekutivfunktionen wahrnimmt und bei der Aufsicht über nicht öffentliche Stellen subjektive Rechte des Bürgers beeinträchtigt werden können. Somit muss er

ner Beauftragten für Datenschutz und Informationsfreiheit bereits jetzt eine Vorreiterrolle. Effektivere Datenschutzkontrolle setzt auch größere Durchsetzungskompetenzen der Kontrollstellen voraus. Auch im nicht-öffentlichen Bereich sollten die Datenschutzbeauftragten mit der Befugnis ausgestattet werden, die Sperrung, Löschung oder Vernichtung von Daten, die widerrechtlich verarbeitet wurden, durch Verwaltungsakt anzuordnen. Formen der gesellschaftlichen Kontrolle könnten den Datenschutz weiter stärken. Konkurrentenklagen und ein Verbandsklagerecht im Datenschutz wären hierzu wünschenswert.

Auch auf Bundesebene sollte das informationelle Selbstbestimmungsrecht als Grundrecht der Informationsgesellschaft in die Verfassung aufgenommen werden. Art. 8 der Europäischen Grundrechtecharta und eine Vielzahl von Landesverfassungen, die wie die Verfassung von Berlin in Art. 33 dieses Grundrecht normiert haben, können dem Bundesgesetzgeber als Vorbild dienen.

Terrorismusbekämpfungsgesetz

Statt zunächst besonnen auszuloten, ob es bei Ausschöpfung der vorhandenen Befugnisse möglich gewesen wäre, die Ereignisse vom 11. September 2001 zu verhindern, und daraus entsprechende Schlüsse für die Organisation der Sicherheitsbehörden zu ziehen, wurde weltweit nach dem Gesetzgeber gerufen. In den USA selbst[8], aber auch in anderen Staaten und in Deutschland wurde vieles aus den Schubläden der Innenministerien geholt, was als Gesetzgebungsidee jemals vorgebracht wurde, aber nicht durchsetzbar schien. Bereits wenige Tage nach dem Anschlag lag neben Vorschlägen zur Änderung des Vereins- und Sicherheitsüberprüfungsrechtes ein über 150-seitiges Papier des Bundesministeriums des Innern mit Vorschlägen für Gesetzesänderungen vor, das alsbald die durchaus treffende Spottbezeichnung „Otto-Katalog“ erhielt. Angesichts der weitreichenden Vorschläge forderte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf einer Sonderkonferenz am 1. Oktober 2001 in Bonn, später auch auf der 62. Konferenz vom 24.-26. Oktober 2001 in Münster, die Freiheits- und Persönlichkeitsrechte dürften bei der Terrorismusbekämpfung nicht verloren gehen[9]. Im Laufe der vorgesehenen Beratungen, insbesondere der Koalitionsfraktionen, wurden zwar Beschränkungen der Befugnisse sowie eine begrenzte Geltungsdauer einiger Teile des Paketes erreicht, grundsätzlich wurde das Gesetzgebungspaket jedoch in vollem Umfang durch die parlamentarischen Gremien gepeitscht und am 7. Dezember 2001 vom Bundestag beschlossen[10]. Eine Vielzahl von Einwendungen des Bundesjustizministeriums, die die Verfassungswidrigkeit erheblicher Teile des Gesetzes belegen, wurde ignoriert.

mindestens der Rechtsaufsicht des Senats unterstellt sein. Seine völlige Unabhängigkeit im Sinne eines Verzichts auf die Rechtsaufsicht würde einen unzulässigen Eingriff in das Prinzip der parlamentarischen Verantwortlichkeit darstellen. Der Unterausschuss Datenschutz hat sich aus eben diesen Gründen den in der Sitzung am 3. Juli 2001 vom Berliner Beauftragten für Datenschutz und Informationsfreiheit geäußerten Wunsch auf Streichung der Rechtsaufsicht nicht zu eigen gemacht. Der Senat erachtet ein Verbandsklagerecht im Datenschutz für nicht zweckmäßig.

[8] USA Patriot Act vom 24. Oktober 2001, H.R. 3162
[9] vgl. Anlagenband „Dokumente zum Datenschutz und Informationsfreiheit 2001“, I.2.-3.
[10] vgl. oben

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Das Terrorismusbekämpfungsgesetz zielt im Wesentlichen in drei Richtungen: Eingriffsbefugnisse der Sicherheitsbehörden werden erweitert, die Ausweispapiere der deutschen Staatsbürger und -bürgerinnen sollen mit biometrischen Merkmalen versehen und die Rechte der Ausländer sollen deutlich beschnitten werden.

Schon seit Jahren gibt es Tendenzen, die verfassungsrechtlich gebotene Trennung zwischen Polizeibehörden auf der einen und Nachrichtendiensten auf der anderen Seite aufzuweichen. Die Polizeibehörden arbeiten darauf hin, bereits im Vorfeld von Straftaten und Gefahrenlagen auf Vorrat Daten sammeln zu können (und dabei auch nachrichtendienstliche Mittel verwenden zu können), die Nachrichtendienste andererseits streben nach mehr exekutiven Befugnissen; erheblicher politischer Druck besteht dahingehend, die Nachrichtendienste in die Bekämpfung der organisierten Kriminalität einzubinden.

Das sogenannte Trennungsgebot bezieht sich lediglich auf die organisatorische Trennung von Polizei und Nachrichtendiensten. Es enthält keine Aussagen darüber, welche Einsatzmittel diese Behörden jeweils nutzen dürfen. Daraus lässt sich demnach keine Sperre für die Polizei herleiten, auf solche Mittel zu verzichten, derer sich die Nachrichtendienste bedienen. Die von der Polizei eingesetzten - auch technischen - Mittel sind deshalb keine nachrichtendienstlichen, sondern polizeiliche Einsatzmittel.

Unabhängig davon ist der Polizei ebenso wie dem Berliner Beauftragten für Datenschutz und Informationsfreiheit bekannt, dass eine Datenspeicherung auf Vorrat gegen verfassungsrechtliche Grundsätze verstieße. Sie arbeitet deshalb auch nicht darauf hin, „... im Vorfeld ... auf Vorrat Daten zu sammeln ...“. Vielmehr speichert sie im Rahmen ihrer gesetzlichen Aufgaben nach § 1 Abs. 3 ASOG auch Daten zum Zweck der vorbeugenden Bekämpfung von Straftaten.

Das Terrorismusbekämpfungsgesetz gibt beiden Trends nach. Auf der einen Seite werden das Bundesamt für Verfassungsschutz und in unterschiedlichem Umfang auch die anderen Dienste ermächtigt, Daten bei Finanzdienstleistern, Postunternehmen, Luftfahrtunternehmen und Telekommunikations- und Teledienstleistern Daten „einzuholen“. Damit wird zwar nur eine Befugnis, noch nicht unmittelbar eine Verpflichtung der angesprochenen Unternehmen festgelegt; da diese aber nach allgemeinem Datenschutzrecht befugt sind, zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten Daten zu übermitteln (§ 28 Abs. 3 Ziff. 2 BDSG), und sich im Zweifel dem Ansinnen der Sicherheitsbehörden nicht entziehen werden, werden hier faktisch exekutive Datenerhebungsbefugnisse begründet. Der lange gehegte Wunsch, mit „IMSI-Catchern“ die Identifikationsnummern von Handys zu ermitteln, wurde nebenbei erfüllt.

Das Bundeskriminalamt erhält auf der anderen Seite die Befugnis, Daten zu erheben, ohne dass das Amt ein Ermittlungsverfahren übertragen bekommen hat. Diese ursprünglich sehr weit gefasste Befugnis wurde zwar darauf beschränkt, Daten zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung zu sammeln, im Endeffekt werden die Befugnisse aber dahin führen, dass das BKA ohne konkreten Anlass Daten über bestimmte Personengruppen sammeln kann – eine Aufgabe, die bisher den Diensten überlassen war.

Die weitreichendsten Folgen könnte der grundsätzliche Beschluss haben, in Pässe und Personalausweise deutscher Staatsangehöriger zusätzliche biometrische Merkmale von Fingern, Händen oder Gesicht aufzunehmen. Zusammen mit anderen Merkmalen dürfen sie auch in verschlüsselter Form in die Papiere eingebracht werden, was bisher verboten war. Die Einführung dieser Merkmale muss zwar durch ein besonderes Gesetz

Mit einer im Rahmen des Terrorismusbekämpfungsgesetzes beschlossenen Änderung des Passgesetzes und des Gesetzes über Personalausweise hat der Bundesgesetzgeber die Möglichkeit eröffnet, neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von Fingern oder Händen oder Gesicht in das jeweilige Personaldokument aufzunehmen.

11 JB 1998, 3.5

12 Grosse, Hans: Handbuch für Untersuchungsrichter als System der Kriminalistik. 4. Aufl. München 1904, S. 278

geregelt werden, mit seiner grundsätzlichen Zustimmung hat das Parlament allerdings zum Ausdruck gebracht, dass die Entwicklung dorthin gehen soll.

Biometrische Merkmale lassen sich grundsätzlich zu zwei verschiedenen Zwecken verwerten:

- zur Authentifizierung, d. h. zur Feststellung, ob der Dokumenteninhaber tatsächlich

derjenige ist, für den das Dokument ausgestellt ist,

- zur Identifizierung unbekannter Personen oder von diesen hinterlassener Spuren.

Wenig problematisch, ja geradezu erwünscht zur Erhöhung der Informationssicherheit ist die Verbesserung von Authentifikationsmerkmalen mit Hilfe biometrischer Methoden[11]. Hierfür reicht es allerdings aus, die Merkmale der Ausweisinhaber mit denjenigen auf dem Ausweispapier zu vergleichen. Eine Speicherung der Merkmalsdaten außerhalb des Dokuments ist nicht erforderlich.

Jede Speicherung biometrischer Daten außerhalb des Dokuments in zentralen oder auch dezentralen Dateien ermöglicht allerdings, die Merkmale über die Authentifizierung hinaus auch zur Identifikation zu benutzen. Die Speicherung von Fingerabdrücken ermöglicht die Identifikation von Tatspuren, der Einsatz von Gesichtsgeometrie erlaubt in Verbindung mit geeigneter Software und entsprechender Videotechnik selbst die Identifizierung vorbeigehender Personen. Eine derartige Speicherung identifizierender Daten aller Bürgerinnen und Bürger wäre allerdings verfassungswidrig.

Bereits bei der Einführung der Daktyloskopie an der Wende vom 19. zum 20. Jahrhundert waren Vorschläge gemacht worden, eine „Volksdaktyloskopie“ einzuführen. Der Autor eines berühmten kriminalistischen Lehrbuches schlug vor, „die gesamte männliche (!) Bevölkerung über 20 Jahre“ zu erfassen[12]. Dieser Vorschlag wurde bereits in der damaligen Zeit als rechtsstaatswidrig empfunden, vielmehr bestand allgemeiner Konsens darin, dass die Sammlung von Fingerabdrücken nur bei Personen zulässig sein sollte, die bereits auffällig geworden waren. Das Bundesverwaltungsgericht hat in einer berühmten Entscheidung im Jahr 1967[13] diese „Delinquenzprophylaxe“ zum entscheidenden Kriterium für die Aufbewahrung erkennungsdienstlicher Unterlagen gemacht. Wörtlich stellte das Gericht fest, „daß nach dem Menschenbild des Grundgesetzes die Polizeibehörde nicht Jedermann als potentiellen Rechtsbrecher betrachten und auch nicht jeden, der sich irgendwie verdächtig gemacht hat ... ohne weiteres erkennungsdienstlich behandeln darf“. Eine umfassende Registrierung der Bürger widerspräche den Prinzipien des freiheitlichen Rechtsstaates[14].

Das Terrorismusbekämpfungsgesetz geht den ersten Schritt weg von diesem Verfassungsgrundsatz. Die Grundsatzentscheidung für die Aufnahme biometri-

Mit der Aufnahme von biometrischen Merkmalen in die Pass- und Ausweisdokumente soll die Möglichkeit verbessert werden, dass die Sicherheitsbehörden mittels eines computergestützten Verfahrens sofort feststellen können, ob die Identität des Dokumenteninhabers mit den im Dokument abgespeicherten Originaldaten übereinstimmt. Dadurch soll insbesondere verhindert werden, dass Personen sich mit fremden Papieren, die für ähnlich aussehende Personen ausgestellt wurden, ausweisen können.

Da dies einen wesentlichen Beitrag zur Verbesserung der öffentlichen Sicherheit und Ordnung darstellen wird, begrüßt der Senat vor dem Hintergrund der Ereignisse vom 11. September 2001 dieses Vorhaben.

Die in diesem Zusammenhang vom Bundesgesetzgeber ebenfalls neu getroffenen Regelungen, die eine Verschlüsselung von Angaben zur Person des Dokumenteninhabers erlauben, sollen der Verbesserung der Fälschungssicherheit und der maschinellen Echtheitsprüfung der Dokumente mit Hilfe nicht für jedermann auslesbarer Individualmerkmale dienen. Den Belangen des Datenschutzes hat der Bundesgesetzgeber dadurch Rechnung getragen, dass die im Pass bzw. im Personalausweis enthaltenen verschlüsselten Merkmale und Angaben nur zur Identitätsprüfung des Dokumenteninhabers ausgelesen und verwendet werden dürfen und auf Verlangen dem Dokumenteninhaber über den Inhalt der verschlüsselten Merkmale und Angaben Auskunft zu erteilen ist.

Zur Umsetzung des Gesamtvorhabens bedarf es noch einer besonderen bundesgesetzlichen Regelung, in der die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung zu regeln sind. Die hierzu geeigneten Konzepte und Techniken werden derzeit vom Bundesministerium des Innern in Zusammenarbeit mit dem Bundeskriminalamt und der Bundesdruckerei geprüft. In diese Prüfung einbezogen werden auch die Möglichkeiten einer gemeinsamen Lösung im Rahmen der Europäischen Union.

Unabhängig davon, wie der Bundesgesetzgeber das Verfahren für die Überprüfung biometrischer Merkmale künftig auch abschließend regeln wird, hat er jedoch bereits durch die jetzige im Terrorismusbekämpfungsgesetz getroffene Regelung datenschutzrechtlichen Belangen dadurch Rechnung getragen, dass er in § 4 Abs. 4 Satz 2 Passgesetz und § 1 Abs. 5 Satz 2 des Gesetzes über Personalausweise die Einrichtung einer bundesweiten (Referenz-) Datei ausgeschlossen hat.

---

[13] BVwGE 26, S. 170
[14] ebd. S. 171

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

scher Merkmale in Pässe und Ausweise ist gefallen; der Druck der Sicherheitsbehörden dürfte so groß sein, dass die konkrete gesetzliche Ausgestaltung bald folgen wird. Zwar sehen die Neuregelungen noch das Verbot bundesweiter Dateien vor, zur Spurenidentifikation werden die Daten nicht zugelassen. Der Weg zur „Volksbiometrisierung“ zeichnet sich allerdings schon ab: Das nächste große Verbrechen könnte schon zum Anlass genommen werden, die bisherigen Beschränkungen zu beseitigen.

Deutliche Einschränkungen ihrer informationellen Selbstbestimmung müssen künftig Ausländerinnen und Ausländer hinnehmen. Auch in deren Dokumente, wie z. B. Aufenthaltsgenehmigungen oder Ausweisersatzpapiere, sollen biometrische Merkmale aufgenommen werden, die allerdings vom Bundesministerium des Innern durch Rechtsverordnung festgelegt werden können. Zur Bestimmung des Herkunftsstaates oder der Herkunftsregion kann künftig das gesprochene Wort von Ausländerinnen und Ausländern aufgezeichnet und ausgewertet werden. In die Ausländerdateien der Ausländerbehörden sollen künftig „freiwillig gemachte Angaben zur Religionszugehörigkeit“ aufgenommen werden.

Einen Auskunftsanspruch über die verschlüsselt gespeicherten Daten in den Dokumenten erhalten Ausländerinnen und Ausländer im Gegensatz zu den Deutschen nicht.

Es ist sehr zu bezweifeln, ob diese diskriminierende Ungleichbehandlung von Ausländerinnen und Ausländern einer verfassungsrechtlichen Prüfung standhalten wird.

Die Darstellung der durch das Terrorismusbekämpfungsgesetz erfolgten Änderungen im Ausländerrecht ist zutreffend, wenn auch sehr gestrafft. Soweit der Berliner Beauftragte für Datenschutz und Informationsfreiheit moniert, der fehlende Auskunftsanspruch über die verschlüsselt in den Dokumenten gespeicherten Daten stelle eine diskriminierende Ungleichbehandlung im Vergleich zu Deutschen dar, bleibt abzuwarten, ob die Frage ggf. vom Bundesverfassungsgericht genauso gesehen wird.

Andere Entwicklungen

Fortschritt und Stillstand, wenn nicht Rückschritt, waren auch beim bereichsspezifischen Datenschutz zu verzeichnen.

Die ökonomischen Möglichkeiten des E-Commerce (aber auch des E-Government) prägten auch in diesem Jahr trotz des Endes des finanziellen Höhenflugs des „Neuen Marktes“ die politischen Debatten. Der Bundesgesetzgeber hat die juristische Absicherung weiter vorangetrieben. Als Ergebnis der Evaluierung der IuK-Gesetzgebung aus dem Vorjahr[15] sowie als Umsetzung der Europäischen E-Commerce-Richtlinie[16] wurde das Elektronische Geschäftsverkehr-Gesetz[17] verabschiedet. Die Regelungen sind vor allem rechtstechnischer Natur und halten den hohen Standard des deutschen Teledienste-Datenschutzes aufrecht, privilegieren allerdings künftig die kommerzielle Kommunikation (international: B2B = Business to Business), indem in diesem Bereich nur noch das allgemeine Datenschutz-

[15] JB 2000, 5.2

[16] 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

[17] Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr vom 14. Dezember 2001, BGBl S. 3761-3727

recht, nicht aber die strengeren Regelungen des Teledienstedatenschutzgesetzes gelten[18]. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte sich hierzu besonders gegen einen Antrag des Bundesrates gewandt[19], Bestands- und Nutzungsdaten bei Telediensten nicht nur an Strafverfolgungsbehörden, sondern auch an Verwaltungsbehörden zur Verfolgung von Ordnungswidrigkeiten und an Nachrichtendienste zu übermitteln[20]. Der Antrag blieb erfolglos.

Nach der kurz vor Jahresbeginn in Kraft getretenen Telekommunikations-Datenschutz-verordnung (TDSV) wurde im Berichtsjahr auch die langwierige Diskussion über die Telekommunikations-Überwachungsverordnung (TKÜV) abgeschlossen, die einerseits die Verpflichtung der Telekommunikationsdienstleister zur Bereitstellung von Abhörschnittstellen konkretisierte, andererseits aber auch weitgehende Ausnahmen von dieser Verpflichtung zulässt[21]. Auch die seit Jahren offene Frage, unter welchen Voraussetzungen Telekommunikationsdienstleister verpflichtet sind, an Sicherheitsbehörden Daten über „Umstände des Fernmeldeverkehrs“ wie z. B. Standorte von Mobiltelefonen herauszugeben, ist durch die Einfügung der §§ 100 g und 100 h in die Strafprozessordnung beantwortet worden[22]. Diese Bestimmungen ersetzen den letzten noch bestehenden Paragrafen des alten Fernmeldeanlagengesetzes (§ 12).

Die Finanzbehörden erhielten mit In-Kraft-Treten der Neufassung des § 147 Abgabenordnung zu Jahresbeginn neue Befugnisse, auf die automatisch geführten Buchhaltungsdaten der Unternehmen zuzugreifen. Die ebenfalls als Reaktion auf den 11. September aufgebrachte Idee, sämtliche von deutschen Banken geführten Konten zentral zu speichern, wurde fallengelassen; allerdings sollen im Rahmen des 4. Finanzmarktförderungsgesetzes den Finanzbehörden nochmals zusätzliche Befugnisse eingeräumt werden. Bewegung ist eingetreten bei der Ergänzung der Abgabenordnung um Datenschutzvorschriften, deren Fehlen von den Datenschutzbeauftragten seit vielen Jahren beanstandet wird[23].

Im Gesundheitswesen gaben die Planungen des Bundesgesundheitsministeriums zur Einführung eines Arzneimittelpasses als Reaktion auf den Lipobay-Skandal Anlass zu umfangreichen Erörterungen. Dieser und andere Aspekte der Telemedizin werden in den nächsten Jahren gründliche Erörterungen erforderlich machen[24]. Die Debatten um einen datenschutzgerechten Umgang mit genetischen Daten gingen weiter; die

[18] vgl. 5.2
[19] BR-Drs. 136/1/01
[20] Entschließung zwischen der 61. und der 62. Konferenz zu „Entwurf einer Telekommunikations-Überwachungsverordnung“. In: Anlagenband, a.a.O., I.2
[21] vgl. 5.1
[22] Gesetz zur Änderung der Strafprozessordnung vom 20. Dezember 2001, BGBl. S. 3879-3880
[23] vgl. 4.3.2
[24] vgl. 3.4

Datenschutzbeauftragen haben hierzu detaillierte Vorschläge entwickelt[25].

Fehlanzeige muss nach wie vor erstattet werden bei der Schaffung eines Arbeitnehmerdatenschutzgesetzes. Trotz mehrerer Beschlüsse des Bundestages und weiterer Ankündigungen des Bundesarbeitsministeriums ist wiederum kein Gesetzentwurf vorgelegt worden – inzwischen erarbeitet die Europäische Kommission einen Richtlinienvorschlag, wohl erneut ein Motiv für künftige Untätigkeit.

Das Bundesverfassungsgericht hat Fernsehaufnahmen im Gericht nicht für generell verfassungswidrig erklärt, sondern dem Gesetzgeber hier einen Spielraum gelassen[26]. . Die Datenschutzbeauftragen hatten sich hierzu früher bereits ebenfalls geäußert. Die Regelungen zur Speicherung des genetischen Fingerabdrucks von Straftätern wurden zwar gebilligt, allerdings höhere Anforderungen gestellt, als die gerichtliche Praxis sie bisher handhabte[27].

1.2 Europa

Bereits vor dem 11. September stand das Verhältnis zwischen dem Datenschutz und den Interessen der Sicherheitsbehörden im Mittelpunkt der Diskussion in Europa. Der Entwurf für ein Übereinkommen über Datennetzkriminalität des Europarates („Cybercrime-Konvention“) wurde das ganze Jahr über auch von den Datenschutzgremien der Europäischen Union kontrovers diskutiert und am 23. November in Budapest unterzeichnet[28]. Die Anschläge in New York und Washington verstärkten die vielfältigen Bemühungen, die Befugnisse der Sicherheitsbehörden auf europäischer Ebene (insbesondere Europol) zu erweitern[29].

Im Mittelpunkt der europäischen Rechtsentwicklung standen Entscheidungen zur Untersetzung bestehender Vorschriften: Auf dem Gebiet des Datenschutzes sind von besonderer Bedeutung die Entscheidungen der Kommission über Standardvertragsklauseln zur Datenübermittlung in Drittländer[30] und zur Auftragsdatenverarbeitung in Drittländern[31]. Die Informationsfreiheit innerhalb der europäischen Gremien, die im Amsterdamer Vertrag festgelegt worden war (Artikel 25.5), wurde durch die „europäische Transparenzverordnung“ konkretisiert[32].

1.3 Berlin

Wie der Bund hat es auch das Land Berlin versäumt, die Europäische Datenschutzrichtlinie fristgemäß in

Eine Umsetzung der EU-Richtlinie im Land Berlin ohne die Berücksichtigung der Umsetzung der EU-

[25] vgl. 3.2
[26] Urteil vom 24. Januar 2001, Az.: 1 BvR 2623/95, 1 BvR 622/99
[27] Beschluss vom 14. Dezember 2000, Az.: 2 BvR 1741/99, 2 BvR 276/00, 2 BvR 2061/00
[28] vgl. 5.1
[29] vgl. 3.1
[30] Entschließung vom 15. Juni 2001, vgl. Anlagenband a.a.O., II.1
[31] Entschließung vom 27. Dezember 2001, ebd., II.2
[32] Verordnung 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 vom 30. Mai 2001, ABl. EG L 145/43, vgl. Anlagenband, a.a.O., Teil B

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

das Landesrecht umzusetzen. Vor dem Hintergrund einer von der Kommission angestrengten Klage vor dem Europäischen Gerichtshof und einer entsprechenden Mahnung des Bundesinnenministeriums legte die Senatsinnenverwaltung einen Gesetzentwurf vor, der mit uns weitgehend abgestimmt und in der letzten Sitzung der Parlaments vor dem Ende der Legislaturperiode am 12. Juli verabschiedet wurde. Das Gesetz folgt weitgehend den Vorgaben des neuen Bundesdatenschutzgesetzes, enthält allerdings insbesondere im Bereich des technischen Datenschutzes deutlich darüber hinausgehende Bestimmungen. Detailliert geregelt wird nunmehr die Wartung von Datenverarbeitungssystemen, die datenschutzrechtlich bisher schwer einzuordnen war. Vorarbeiten hierzu waren in Kooperation mit dem Land Brandenburg geleistet worden.

Richtlinie auf Bundesebene erschien wenig sinnvoll. Wie die meisten anderen Bundesländer hatte daher auch das Land Berlin entschieden, zunächst abzuwarten, bis sich die Überlegungen zur Novellierung des BDSG auf Bundesebene hinreichend konkretisiert hatten. Aufgrund der von der Kommission angestrengten Klage vor dem Europäischen Gerichtshof wurden die Anstrengungen zur zeitnahen Umsetzung der Richtlinie weiter verstärkt, so dass das Gesetz zur Änderung des Berliner Datenschutzgesetzes und anderer datenschutzrechtlicher Regelungen nicht zuletzt aufgrund der konstruktiven Zusammenarbeit mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit noch vor dem Ende der vergangenen Legislaturperiode vom Abgeordnetenhaus beschlossen werden konnte. Nachdem nunmehr die Kommission die Klage zurückgenommen und die Bundesregierung der Rücknahme zugestimmt hat, ist das Vertragsverletzungsverfahren beendet.

Die Verpflichtung zu technischen und organisatorischen Maßnahmen zur Gewährleistung der Informationssicherheit wurde an den Stand der Diskussion in der Informatikwissenschaft angepasst. Die bisherigen und im BDSG immer noch enthaltenen Vorschriften zu konkreten einzelnen Maßnahmen wurden ersetzt durch die Regelungsziele der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz. Vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung der automatisierten Datenverarbeitung sind künftig die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzepts zu ermitteln (§ 5).

Nicht gelungen ist es, entsprechend unserem Vorschlag wie im Bundesrecht die Möglichkeit zu schaffen, den Stand datenschutzrechtlicher Vorkehrungen durch ein Auditierungsverfahren zertifizieren zu lassen. Der Unterausschuss Datenschutz des Innenausschusses hat in der Beratung des Gesetzentwurfes allerdings die Innenverwaltung aufgefordert, ein entsprechendes Gesetz zu erarbeiten[33].

Von einer gesetzlichen Verankerung des Datenschutzaudits im BlnDSG hat der Berliner Gesetzgeber bewusst abgesehen. Da eine entsprechende Regelung aus kompetenzrechtlichen Gründen lediglich die Datenschutzkonzepte sowie technische Einrichtungen der öffentlichen Stellen des Landes Berlin erfassen könnte – für deren Prüfung nicht zuletzt der Berliner Beauftragte für Datenschutz und Informationsfreiheit eine besondere Verantwortung besitzt – sollte zunächst abgewartet werden, bis entsprechende Erfahrungen im Bund und in den Ländern vorliegen, in denen entsprechende Auditierungsverfahren existieren oder beabsichtigt sind. Der Senat hält ein solches Verfahren zum gegenwärtigen Zeitpunkt für einen effektiven Datenschutz für nicht notwendig, aber kostenträchtig. Zudem entwertet es in gewissem Umfang die Stellung des behördlichen Datenschutzbeauftragten und könnte – da die Auditierung freiwillig erfolgen soll – dazu führen, dass einzelne datenverarbeitende Stellen ihr Datenschutzkonzept auditieren lassen, andere vergleichbare Stellen aber nicht. Die sich daraus ergebende Uneinheitlichkeit im Land Berlin erscheint bedenklich.

Ebenfalls nicht gelungen ist es, die Terminologie des Gesetzes an die des Bundes anzupassen. Die unterschiedlichen Begriffsbestimmungen auf europäischer, nationaler und Berliner Ebene werden die Rechtsanwendung sicher nicht erleichtern.

Aufgrund des erheblichen Zeitdrucks zur Umsetzung der Richtlinie stand eine terminologische Vereinheitlichung von BDSG und BlnDSG bei der Novellierung des BlnDSG nicht im Vordergrund. In Teilbereichen wurde die Terminologie des BlnDSG dennoch an die

[33] Beschlussprotokoll der Sitzung vom 3. Juli 2001, S. 2

Terminologie des Bundes angepasst (etwa bei den Regelungen zur Videoüberwachung oder zu den mobilen personenbezogenen Speicher- und Verarbeitungsmedien). Über eine weitere terminologische Angleichung sollte erst nach der „2. Stufe“ der BDSG-Novellierung nachgedacht werden, um zu verhindern, dass eventuelle Angleichungen nach vergleichsweise kurzer Zeit überholt sind und erneut angepasst werden müssten.

Von Bedeutung für das E-Government im Land Berlin wird das Gesetz zur Erprobung der digitalen Signatur in der Berliner Verwaltung sein, das es in ausgewählten Verwaltungsbereichen ermöglichen wird, auf gesicherte Weise mit der Berliner Verwaltung zu kommunizieren[34].

2. Technische Rahmenbedingungen

2.1 Entwicklung der Informationstechnik

Verfolgt man über das ganze Jahr hinweg die Angebote für Heimcomputer und Zubehör, mit denen wir in Form von Beilagen von Zeitungen und Zeitschriften überschwemmt werden, so stellt sich der Eindruck ein, als würde die Informationstechnik einer schnellen und kontinuierlich wachsenden Weiterentwicklung unterliegen. Waren zu Weihnachten 2000 Pentium-III-Rechner mit 866-MHz-Prozessoren, 128-MB-Arbeitspeicher und 40-GB-Festplatte und selbstverständlich eingebautem CD-Brenner und DVD-Laufwerk noch der Hit, so wird dieses Preissegment jetzt von Pentium-4-Rechnern mit 2-GHz-Prozessoren, 256-MB-Arbeitsspeicher, 60-GB-Festplatte und neuerdings schon eingebautem DVD-Brenner beherrscht. Welcher Fortschritt ergab sich da für Heim und Freizeit? Für die häuslichen Büroanwendungen wie Textverarbeitung, etwas Tabellenkalkulation, vielleicht die Nutzung einer kleinen Datenbank zur Organisation von Sammlungen benötigt man diese Kapazitäten nicht, ebenso wenig für das Surfen im Internet. Der Speicherung und Bearbeitung von digitalen Fotografien sind die heutigen Kapazitäten auch schon über den Kopf gewachsen. Es bleiben die grafisch immer komplexer werdenden Computerspiele und der computergestützte Umgang mit digitaler Videotechnik. Wer dies nicht macht, lässt 90 % seiner Rechenkapazität brachliegen.

Informationstechnik immer und überall

Neben dieser nicht mehr revolutionären Entwicklung von Freizeittechnik gaben sporadische Meldungen der Fachpresse Anlass, uns mit den Fantasien zu befassen, die durch die zunehmende Miniaturisierung von Informationstechnik und das Aufkommen drahtloser Kommunikation in den Labors der informationstechnischen Industrie ausgelöst wurden.

Dem folgenden Szenario sei ein Zitat des IBM-Chef Lou Gerstner vorangestellt, der seine Vision äußerte,

[34] Gesetz zur Erprobung der elektronischen Signatur in der Berliner Verwaltung vom 8. Oktober 2001, GVBl. S. 531

dass „eine Milliarde Menschen mit einer Million E-Business-Unternehmen über eine Billion vernetzter und intelligenter Geräte interagieren“ werden. Das Szenario verwendet Vorstellungen, die man bei einschlägigen Recherchen im World Wide Web nachlesen kann.

Im Jahre 2010 mag man sich den normalen Tagesablauf eines normalen Menschen, nennen wir ihn Egon Digital, wie folgt vorstellen:

Nach dem Aufstehen gibt Egons Bett einen Warnton ab, der ihn veranlasst, auf ein Display zu schauen, welches ihm mitteilt, dass er in der letzten Nacht 50 Gramm mehr gewogen habe als in der Nacht zuvor und dass dies dem Trend der letzten Wochen entspräche. Egon Digital nimmt sich vor, außerhalb seiner Wohnung etwas mit den Kalorien aufzupassen. Zu Hause braucht er es nicht, denn dort übernimmt dies der Kühlschrank für ihn. Dieser erhält nämlich dann ein Signal vom Bett, dass kalorienärmere Kost hilfreich wäre, wenn das Bett das Überschreiten eines bestimmten Schwellenwertes meldet.

Der Kühlschrank sondiert ständig, welche Produkte sich in welcher Menge (Füllstände, Gewicht) in ihm befinden und wie lange sie noch haltbar sind. Solche Informationen liefern Sensoren des Kühlschranks (Gewicht) oder der Verpackung (Füllstand) sowie elektronische Etiketten auf den Produkten (Art und Marke des Lebensmittels, Haltbarkeit) an die Zentralsteuerung des Kühlschranks. Dabei unterscheidet er zwischen Standard-Lebensmitteln, die stets frisch verfügbar sein müssen und daher per UMTS-Kommunikation beim nächsten Supermarkt automatisch nachgeordert werden müssen, wenn das BIBO-Kühlfachüberwachungssystem (Be In, Be Out) das Fehlen oder den Ablauf des Aussonderungsdatums eines Produktes feststellt, und Sonder-Lebensmitteln, die Egon Digital mal zusätzlich mitgebracht hat und bei denen nur so lange die Frische geprüft wird, bis der Kühlschrank automatisch erkennt, dass es für Egon ein Standard-Produkt geworden ist.

Die Alarmmeldung des Bettes jedoch veranlasst den Kühlschrank, kalorienärmere Varianten der Standard-Produkte zu ordern. Das System sorgt jedenfalls dafür, dass Egon Digital an diesem Morgen seine frischen Lebensmittel zum Frühstück hat. Bald nachdem er das Haus verlassen hat, um zur Arbeit zu fahren, wird ein Lieferwagen seines Supermarktes kommen und die Bestellungen des Kühlschranks bringen. Komplexe Authentisierungsverfahren der Eingangstür sorgen dafür, dass nur der Lieferant des Vertrauens den Kühlschrank bestücken kann, und andere Sensoren sorgen dafür, dass er in der Wohnung nicht vom Pfad der Tugend abweichen kann.

Egons Auto hat bei seiner Annäherung automatisch die Fahrertür geöffnet, den Lieblingssender eingestellt und gestartet, weil das Auto Egon an seiner Gesichtsgeometrie erkannt hat. Als begeisterter Autofahrer hat Egon darauf verzichtet, das automatische Steuerungssystem zu aktivieren. Mit diesem System hätte er ein eingespeichertes Ziel mit seinem Auto erreichen kön-

nen, ohne sich um das Fahren kümmern zu müssen, weil der Weg durch das Navigationssystem festgelegt wird und Rundum-Abstandsmessgeräte dafür sorgen, dass stets der richtige Abstand zu allen denkbaren Hindernissen gewahrt wird.

Nach seinem Arbeitstag will Egon etwas für seine Gesundheit (und gegen sein ansteigendes Gewicht) tun und joggt. Beim Joggen will er ein bestimmtes Durchschnittstempo einhalten, weil er sich weder unter- noch überfordern will. Die Sohlen seiner Joggingschuhe messen automatisch die Schrittfrequenz und die Schrittlänge und ermitteln somit die aktuelle Geschwindigkeit und die bereits gelaufene Strecke und melden diese Daten über Funk an ein in die Armbanduhr eingebautes Display.

Der abendliche Blick in die eingegangenen E-Mails zeigt ihm die Kehrseite der Technisierung: Mindestens zwei Lebensmittelkonzerne haben Ernährungsdefizite aufgedeckt, die sie mit ihren Produkten beheben möchten, seine Krankenkasse warnt vor einer Prämienerhöhung in Verbindung mit erhöhten gesundheitlichen Risiken von Übergewicht und seine Kfz-Versicherung tut das Gleiche wegen seiner Gewohnheit, das automatische Steuerungssystem seines Autos auszuschalten.

Das Szenario handelt vom Pervasive Ubiquitous Computing (UC), zwei Begriffe, die für die gleiche Informationstechnik stehen. Der „um sich greifende“ „allgegenwärtige“ Computereinsatz wird nach Meinung von Herstellern und Entwicklern als prägende Einsatzform der Informationstechnik den PC ablösen. Dabei werden folgende Trends vorausgesagt, die diese Entwicklung vorantreiben:

- Die Steigerung der Leistungsfähigkeit und Miniaturisierung von Prozessoren und Speicherbausteinen wird im gleichen Tempo wie bisher fortschreiten.
- Das Internet wächst mit Mobilkommunikationssystemen zusammen (z. B. UMTS).
- Der omni- multifunktionale Personal Computer wird durch kleine auf bestimmte Anwendungen hin spezialisierte Miniatursysteme teilweise verdrängt.
- Die Sensortechnik wird erhebliche Fortschritte hinsichtlich der Leistungsfähigkeit und der Miniaturisierung machen und dabei auf neuen Materialien aufbauen.

UC-Systeme wird man nicht mehr als solche erkennen, sie werden unsichtbar. Wie im Szenario dargestellt, können sie in Möbeln, Haushaltsgeräten, Schuhen und selbstverständlich auch in Autos eingebaut sein. Höherpreisige Fahrzeuge zeigen heute schon Ansätze für sensorgesteuerte, identifizierende oder lokalisierende Systeme. In Schreibgeräten, Kleidungsstücken, Accessoires oder Druckerzeugnissen können solche Systeme eingearbeitet sein. Kurzum: Es ist denkbar, dass jeder Gegenstand Träger informationstechnischer Funktionen sein wird.

Ein weiteres Merkmal ist, dass die UC-Systeme sich spontan vernetzen und somit selbstständig miteinander kommunizieren können.

Das Szenario mag auch die Fantasie des Lesers anregen, selbst weitere Beispiele für Anwendungen zu finden.

Wie das Beispielszenario zeigt, kann die Fantasie auch eine Vielfalt von Problemen aufzeigen, die sich für die Aufrechterhaltung der informationellen Selbstbestimmung ergeben. Die UC-Systeme generieren beständig eine Vielzahl personenbezogener Daten, so dass darüber nachgedacht werden muss, wie diese Systeme datenschutzfreundlich gestaltet werden können, damit sie nicht zum Motor omnipräsenter Überwachungsinfrastrukturen werden.

Darüber hinaus werden diese Techniken den Datenschutz vor grundsätzliche Probleme stellen. Bisher als grundlegende Prinzipien des Datenschutzes anerkannte Anforderungen wie Erforderlichkeit, Zweckbindung oder Transparenz lassen sich nicht mehr realisieren, ein umfassender Auskunftsanspruch über alle Daten ist illusorisch. Hier wird ein neues Instrumentarium zu entwickeln sein. Erste Ansätze finden sich in dem Gutachten „Modernisierung des Datenschutzrechts“[35].

UMTS und Lokalisierung

Der Berichtszeitraum war ein schlechtes Jahr für all die Trends, die wir in früheren Jahren an dieser Stelle dargestellt haben. Die Träume und Fantasien der Unternehmensgründer des Neuen Marktes sind weltweit verpufft, der Niedergang dieser Unternehmen hat viel Kreativität neutralisiert und damit Innovationspotenziale gestört. Wer jetzt noch dabei sein will, ist vorsichtig und blickt auf eher eingeführte Techniken. Neue Entwicklungstrends können so nicht entstehen. Was ist also aus den in den letzten Jahren beschriebenen Trends geworden?

Unter dem Eindruck der Versteigerung der UMTS-Lizenzen haben wir im Vorjahr über Handy-Dienste spekuliert, die sich moderne Lokalisierungsmöglichkeiten zunutze machen. Dies war ein Leistungsmerkmal, von dem sich die Hersteller die langgesuchte „Killerapplikation“ erhofften, mit der das Geld zurückverdient werden könnte, was für die Lizenzen ausgegeben wurde. Dieses Thema hat zwar bisher keine Dominanz gewinnen können.

Gleichwohl werden Lokalisierungsverfahren künftig gerade im Rahmen von UC-Systemen eine große Rolle spielen. Die datenschutzrechtliche Brisanz ist hoch: Gestatten die Systeme doch, nicht nur das Kommunikationsverhalten genau nachzuvollziehen, sondern auch zentimetergenau die Bewegungen der Kommunikationspartner nachzuvollziehen. Die Internationale Arbeitsgruppe Datenschutz in der Telekommunikation hat

[35] vgl. Roßnagel u. a., a.a.O., S. 68 ff.

diesem Thema deshalb besondere Aufmerksamkeit gewidmet[36].

Mensch und Technik

Unverändert ist der Glaube, dass der Einsatz von informationstechnischen Systemen Allheilmittel für wesentliche gesellschaftliche Problemstellungen ist und das menschliches Handeln und Denken zurückstehen muss, wenn informationstechnische Lösungen propagiert werden.

Das erste Beispiel zeigen die internationalen und nationalen Reaktionen auf die Terroranschläge vom 11. September.

Obwohl diese Attentate durch die längst existierenden und früher an dieser Stelle auch beschriebenen globalen Telekommunikationsüberwachungssysteme wie ECHOLON oder die Überwachung der Internetkommunikation mittels CARNIVORE weder erkannt noch erst recht verhindert werden konnten, wurde der Ruf nach weiteren technischen Überwachungssystemen laut. Die amerikanischen Sicherheitsbehörden sollen angeblich unter der Bezeichnung „Magic Lantern“ an einer Schnüffelsoftware arbeiten, mit der Tastaturanschläge an Rechnern aufgezeichnet und weiter versendet werden können, damit Daten zugänglich werden, die verschlüsselt übertragen werden, weil entweder die Eingabe des noch unverschlüsselten Textes oder der Schlüssel Passwörter aufgezeichnet werden kann. Die Implementierung solcher Programme müsste dann aus der Ferne möglich sein, z. B. als Trojanische Pferde, die gezielt auf die zu überwachenden Rechner übertragen werden. Inzwischen beginnen die Produzenten von Virenschutzsystemen darüber nachzudenken, ob ihre Systeme beim Erkennen solcher Software alarmieren sollen oder nicht.

In Deutschland wurde auch sofort der Ruf nach neuen informationstechnischen Verfahren laut, mit denen alle möglichen Überwachungsfunktionen gegenüber den Bürgern umgesetzt werden sollen. Die Tatsache, dass Personen, die an den Terroranschlägen vom 11. September beteiligt waren, in Deutschland unerkannt und unter Umständen mit mehreren Identitäten leben konnten, gab den Anlass, neue Systeme zur Authentifizierung von Personen zu fordern. Dabei sollen die Fortschritte biometrischer Systeme ausgenutzt werden, mit denen Finger- und Handabdrücke, Irismuster, Gesichtsgeometrien und -bewegungsabläufe, Stimmen und sogar Unterschriften erfasst und verglichen werden können. Biometrische Merkmale auf Personalausweisen und anderen Legitimationspapieren sollen erreichen, dass diese Unterlagen nicht mehr gefälscht werden können oder die falschen Personen sich nicht mit echten Papieren ausweisen können. Selbstverständlich sieht auch die einschlägige Industrie endlich die Chance, komplexe Chipkartentechnik massenweise verkaufen zu können – die deutsche Reaktion auf die An-

[36] vgl. 6.4; vgl. auch Beschluss vom 15./16. Februar 2001 „Gemeinsamer Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten“. In: Anlagenband, a.a.O., IV.1

schläge in Amerika bietet hier endlich eine Chance, auf die die Chipkartenunternehmen lange gewartet haben[37].

Mit den Fähigkeiten von Systemen zur Erkennung von Gesichtsgeometrien ist es mittlerweile möglich, Videoaufzeichnungen darauf zu analysieren, ob bestimmte Personen von den Aufzeichnungen erfasst worden sind. Sofern über alle Bürger Vergleichsdaten verfügbar sind, wären die technischen Voraussetzungen geschaffen, eine vollständige Auflistung aller Personen zu erhalten, die von der Videoüberwachung erfasst worden sind.

Glaubt man den Versicherungen der Hersteller, so sollen die Systeme inzwischen so weit ausgereift sein, dass die Fehlerrate vernachlässigt werden kann. Objektiv ist sicher festzuhalten, dass hier technologische Entwicklungstrends bestehen, die von der politischen Debatte um Sicherheitsfragen beflügelt werden. Ob sich daraus tatsächlich ein breiter Bedarf entwickeln wird, wird davon abhängen, wieweit politisch bei der Gewährleistung von Sicherheit auf breiten Technikeinsatz anstelle von menschlicher Intelligenz gesetzt wird.

Auch in einem anderen Bereich ausstehender politischer Reformprojekte sollen Fortschritte der Informationstechnik die Lösung bringen: In der Diskussion darum, wie in Zukunft Gefahren für Patienten abgewehrt werden könnten, die am Beispiel der schwerwiegenden Nebenwirkungen des Cholesterinhemmers „Lipobay“ in Verbindung mit der Einnahme anderer Medikamente deutlich wurden, brachte die Bundesgesundheitsministerin den elektronischen Medikamentenpass ins Gespräch, also eine Chipkarte, in die alle Medikamente eingetragen werden sollen, die ein Patient verwendet, damit Unverträglichkeiten erkannt werden können[38]. Auch hier wird nach technischen Lösungen gesucht, weil dem menschlichen Sachverstand – etwa wegen der Verschreibung unverträglicher Medikamentenkombinationen – nicht vertraut wird.

Gleichzeitig wurde die Debatte um weitere Chipkartenanwendungen im Gesundheitswesen erneut entfacht, um Beiträge zur Dämpfung der Kostensteigerungen in diesem Bereich zu erhalten[39]. Offensichtlich verspricht die quantitative Verbesserung der Leistungsmerkmale von Chipkarten größere Erfolge als diverse Projektansätze seit Mitte des letzten Jahrzehnts.

2.2 Datenverarbeitung in der Berliner Verwaltung

Trotz der finanziellen Engpässe, unter denen der öffentlichen Verwaltung Berlins große Opfer zugemutet werden müssen, gehen die Bemühungen um eine zeitgemäße Automation des Verwaltungshandelns in Berlin ungebrochen weiter. Modernisierung der Verwaltung heißt unter solchen Bedingungen eben nicht nur Abbau und Privatisierung öffentlicher Leistungen,

[37] z. B.: „G&D setzt auf neue Chipkarten“. In: FAZ vom 1. Dezember 2001, S. 18
[38] vgl. Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu „Datenschutzrechtliche Anforderungen an den Arzneimittelpass (Medikamentenchipkarte)**“**. In: Anlagenband, a.a.O, T.3
[39] JB 1995, 3.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

sondern auch Rationalisierung von Verwaltungsprozessen mit moderner Informationstechnik und Entbürokratisierung des Verhältnisses zwischen Bürgern, Unternehmen und Verwaltung unter Einsatz moderner Kommunikationsformen. Die Forcierung des letztgenannten Modernisierungsziels war Ziel einer Arbeitsgruppe des Koordinationsausschusses für Informationstechnik in Berlin (IT-KAB), die sich mit der Konzeption einer „interaktiven Verwaltung“ beschäftigte.

E-Government in Berlin

Die moderne Vorsilbe „E-“ steht für die Durchführung traditioneller Geschäftsprozesse unter der Nutzung moderner Kommunikationsmedien, speziell der Dienste des Internet. Für viele Privatleute und für fast alle Beschäftigten in Wirtschaft und Verwaltung ist die Nutzung von elektronischer Post (E-Mail) selbstverständlich geworden. Viele haben sich auch schon im E-Business versucht, indem sie Bestellungen über das Internet abgesetzt, vielleicht die Ware gleich über das Internet empfangen haben, wenn sie in die Form von Bits und Bytes gebracht werden konnte. Zwar wächst der Trend zu solchen Formen des Kundenkontaktes langsamer, als es den Internet-Handelsunternehmen recht sein könnte, so dass viele Versuche, auf diesem Feld Geld zu verdienen, scheiterten. Trotz alledem gibt es kaum Zweifel daran, dass E-Business letztlich eine wesentliche Form zukünftigen Umgangs mit Kunden sein wird.

Diesem Trend kann sich auch die öffentliche Verwaltung nicht entziehen. Viele Prozesse des Regierens und Verwaltens lassen sich über das Internet abwickeln. Die moderne Bezeichnung dafür lautet E-Government und umfasst ein ganzes Spektrum von Dienstleistungen, die zum Teil bereits über das Internet angeboten werden und zum anderen Teil jetzt nach und nach entwickelt werden. Längst sind die Verwaltungen von Bund, Ländern und Kommunen bemüht, sich nach dem Vorbild von Wirtschaftsunternehmen durch Behördenportale im Internet zu präsentieren und Verwaltungsinformationen bereitzustellen, die es Bürgern und Unternehmen vereinfachen, sich im Dickicht der Verwaltung zurechtzufinden. Öffnungszeiten, Zuständigkeiten, Hinweise auf Rechte und Pflichten und viele Antworten auf Fragen können so angeboten werden, ohne dass der Bürger Scheu vor dem Amtsschimmel haben muss. Kontaktmöglichkeiten per E-Mail, die Bestellung von Informationsmaterialien und die Bereitstellung von Behördenformularen zum Download und Ausdruck im heimischen Wohn- oder Arbeitszimmer sind die nächsten Schritte zum E-Government.

Als Nächstes kommen interaktive elektronische Bürgerdienste, also die vollständige Abwicklung öffentlicher Dienstleistungen und hoheitlicher Aufgaben über das Internet, soweit dies mit dem Austausch von Daten erledigt werden kann. Die meisten öffentlich-rechtlichen Geschäftsprozesse, die Bürger und Verwaltung miteinander abwickeln, sind rein informationeller Art und können daher über das Medium Internet

Die Berliner Verwaltung wird die Möglichkeiten des E-Government nutzen, um

- die Beziehungen des Bürgers zur Verwaltung,
- die Beziehungen von Unternehmen zur Verwaltung,
- die Beziehungen der Verwaltung(en) untereinander

effektiver zu gestalten.

Bürgern und Wirtschaft sollen Dienstleistungen der Verwaltung möglichst umfassend auf elektronischem Wege zugänglich gemacht werden. Die herkömmliche Erbringung von Dienstleistungen soll durch den Einsatz der Informationstechnik unterstützt werden. In diesem Zusammenhang müssen Arbeitsprozesse neu gestaltet, Kommunikation und Interaktion zwischen Mitarbeitern und Behörden verbessert und optimiert werden. Die Möglichkeiten des E-Government sind damit ein integraler Bestandteil der Verwaltungsreform.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

stattfinden. Die Arbeitsgruppe zur Interaktiven Verwaltung benennt das Ziel, dass über kurz oder lang sämtliche Dienstleistungen der Verwaltung den Bürgerinnen und Bürgern zugänglich gemacht werden sollen. Ein weiterer Aspekt des E-Government ist die Beteiligung der Bürger an demokratischen Entscheidungsprozessen, also die Beteiligung an der öffentlichen Meinungsbildung im Vorfeld politischer Entscheidungen oder die Durchführung von Wahlen (E-Democracy).

Der Masterplan E-Government, der von der Arbeitsgruppe „Interaktive Verwaltung“ im Dezember 2001 vorgelegt wurde, sieht berlin.de als das einheitliche Internetportal der Berliner Verwaltung an, über das die Dienstleistungen der öffentlichen Verwaltungen erreicht werden können. So sollen die Bürgerämter lebenslagen- bzw. zielgruppenorientierte Dienstleistungen anbieten. Wer z. B. ein Auto anmelden muss, umziehen will, seine verlorenen Papiere ersetzen oder einen Sterbefall abwickeln muss, soll diese sonst komplexen Amtsgänge durch den Internet-Dialog mit dem Bürgeramt oder durch die Vermittlung eines Call-Centers einfach ersetzen können.

Konkrete Projekte zum E-Government in der Berliner Verwaltung befassen sich u. a. mit dem Vorbestellungs- und Ausleihwesen im Verbund Öffentlicher Bibliotheken, der Beantragung von Mahnbescheiden, Wohngeld und Wunschkennzeichen für das Kfz, der Anmeldung bei Volkshochschulen, der Erteilung von Auskünften aus dem Melderegister, dem Grundbuch und anderen öffentlichen Registern und den Ausschreibungen von Bauleistungen und anderen Gütern.

Die Einführung des E-Government bedarf einer Vielzahl gesetzlicher Anpassungen. Wenn die persönliche Antragstellung, vielleicht sogar die persönliche Vorsprache in einem Amt, durch einen unpersönlichen Kommunikationsprozess ersetzt werden sollen, so muss der Kommunikationsprozess auch die sichere Authentifizierung des Antragstellers gewährleisten und den anerkannten Nachweis seiner Willensbekundung liefern. Die eigenhändige Unterschrift und die Vorlage des Personalausweises müssen durch eine digitale Signatur ersetzt werden und diese Signatur muss für die erforderliche Rechtssicherheit von der Behörde akzeptiert werden. Aufbauend auf dem neuen deutschen Signaturgesetz[40] wurde daher ein Berliner Erprobungsgesetz zum Einsatz elektronischer Signaturen verabschiedet. Dieses benennt eine Vielzahl von Erprobungsbereichen und enthält eine Verordnungsermächtigung, die nähere Festlegungen ermöglicht. Dabei geht es insbesondere um die Signaturstufen, die jeweils erreicht werden müssen. Da nur die qualifizierte elektronische Signatur in den bereits existierenden Formanpassungsgesetzen des Bundes[41] die gleichen rechtlichen Anforderungen wie die handschriftliche Unterschrift erfüllt, muss immer dann, wenn die Schriftform verlangt wird, diese Stufe erreicht werden.

Die politische und administrative Steuerung, Priorisierung und Ressourcenzumessung sowie die Schaffung der rechtlichen, organisatorischen und technischen Rahmenbedingungen erfolgt auf der Grundlage einer gemeinsamen E-Government – Strategie.

Der IT-Koordinierungsausschuss Berlin (IT-KAB) hat unter Leitung der Senatsverwaltung für Inneres eine „Arbeitsgruppe interaktive Verwaltung“ eingerichtet und Zielkonzeption und Strategie des E-Government im Land Berlin im Masterplan „eGovernment“ erarbeitet.

Im Masterplan werden auch die notwendigen rechtlichen Anpassungen und die Voraussetzungen zur rechtssicheren Kommunikation mittels elektronischer Signatur erörtert.

[40] Gesetz über Rahmenbedingungen für elektronische Signaturen vom 16. Mai 2001, BGBl. I S. 876

[41] Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehrs vom 13. Juli 2001, BGBl. S. 1542-1549

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Die qualifizierte elektronische Signatur setzt den Einsatz einer Chipkarte voraus, die den geheimen Schlüssel enthält und mit ihm die notwendigen Verschlüsselungen durchführt. Diese Chipkarte bedarf ebenso wie die Systeme, mit denen ein Trust-Center das aus geheimem und öffentlichem Schlüssel bestehende Schlüsselpaar generiert, der amtlichen Zertifizierung. Eine noch höhere Stufe, die qualifizierte elektronische Signatur mit Anbieterakkreditierung, verlangt sogar, dass sich auch das Trust-Center selbst der amtlichen Zertifizierung unterwirft.

Personen, die die Vorzüge des E-Government genießen wollen, werden sich also eine solche Chipkarte für die Durchführung des Signaturvorgangs beschaffen müssen.

Mit der elektronischen Signatur werden auch die Maßnahmen getroffen, die es erlauben, über das Netz gesandte personenbezogene Daten ihrem Ursprung zuzuordnen, also die Authentizität der Daten nach § 5 Abs. 2 Nr. 4 BlnDSG zu gewährleisten. Selbstverständlich besteht beim E-Government auch die Forderung, dass die vom Bürger an die Verwaltung und auch zurück von der Verwaltung zum Bürger übertragenen personenbezogenen Daten auf dem Netz vor der unbefugten Kenntnisnahme und Veränderung geschützt werden, also auch die Vertraulichkeit und Integrität nach § 5 Abs. 2 Nr. 1 und 2 BlnDSG durch sichere Datenverschlüsselung gewährleistet werden.

Mit dem Entwurf eines Dritten Gesetzes zur Änderung verwaltungsverfahrensrechtlicher Vorschriften will die Bundesregierung die rechtsverbindliche elektronische Kommunikation zwischen Bürgern und Verwaltung ermöglichen. Es soll das gesamte Verwaltungsverfahrensrecht des Bundes für die Entwicklungen der Informations- und Kommunikationstechnik im modernen Rechtsverkehr geöffnet und Bürgern wie Verwaltung grundsätzlich in allen Fachgebieten und jeder Verfahrensart die Verwendung der elektronischen Kommunikationsformen gleichberechtigt neben der Schriftform und der mündlichen Form rechtswirksam ermöglicht werden. Da nach dem Gesetz über das Verfahren in der Berliner Verwaltung (§ 1) das Verwaltungsverfahrensgesetz für die öffentlich-rechtliche Verwaltungstätigkeit der öffentlichen Stellen des Landes Berlin gilt, sofern nichts anderes bestimmt ist (§§ 2 bis 4), hat dieser Entwurf auch unmittelbare Auswirkungen auf die Berliner Verwaltung.

In unserer Stellungnahme haben wir gefordert, dass die elektronische Kommunikation – insbesondere bei Verwaltungsakten – zwischen Bürgern und Verwaltung von der ausdrücklichen Zustimmung der Betroffenen abhängig gemacht werden sollte. Nach dem Entwurf ersetzt die Signatur bei Verwendung eines Pseudonyms nicht die Schriftform, was im Hinblick auf das Gebot der Datenvermeidung nicht in dieser allgemeinen Form hinnehmbar ist. In Fällen, in denen die Identifizierung des Bürgers gegenüber der Verwaltung nicht zwingend erforderlich ist, sollten auch Pseudonyme genutzt werden können. Problematisch ist auch die Festlegung,

Der Senat hat sich gegenüber dem Bundesinnenministerium ebenfalls für die Aufnahme eines Zustimmungserfordernisses in den Gesetzestext ausgesprochen, hält allerdings nicht in allen Fällen eine ausdrückliche Erklärung der Zustimmung für erforderlich.

Nach dem Entwurf der Bundesregierung ersetzt die Signierung mit einem Pseudonym die Schriftform nur dann, wenn die Identifizierung des Absenders durch die Verwendung des Pseudonyms nicht gefährdet ist. Diese Regelung hält der Senat für richtig. Im Bereich des Verwaltungsverfahrensrechts soll die Schriftform

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

wann ein Dokument als „zugegangen“ gilt. Angesichts der Unwägbarkeiten des Übermittlungswegs bei E-Mail erscheint ein Tag als Fiktion für den Zugangszeitraum zu kurz.

dort, wo sie gefordert wird, gerade auch die Gewähr dafür bieten, dass beispielsweise ein Antrag von einem bestimmten Antragsteller stammt.

Der Entwurf wurde bereits dahingehend geändert, dass gemäß § 41 Abs. 2 VwVfG-E ein elektronisch übermittelter Verwaltungsakt grundsätzlich am dritten Tage nach der Absendung als bekannt gegeben gilt. Nach § 15 Satz 2 VwVfG-E gilt in den dort genannten Fällen ein elektronisch übermitteltes Dokument am dritten Tage nach der Absendung als zugegangen.

Eine weitere Voraussetzung für ein erfolgreiches E-Government in Berlin ist die Modernisierung der informationstechnischen Verfahren in der Berliner Verwaltung, damit sie auf die neue Kommunikationsform mit den Bürgern über das Internet vorbereitet ist, und die Schulung der Mitarbeiter, damit sie einerseits mit den komplexer werdenden informationstechnischen Systemen umgehen können und andererseits die neue Form des Bürgerkontaktes und deren Anforderungen in der täglichen Arbeit internalisieren können[42].

Der Senat betrachtet die Modernisierung der informationstechnischen Verfahren und die Schulung der Mitarbeiter als eine kontinuierliche Aufgabe, die auch den IT-Einsatz außerhalb von eGovernment betrifft.

Beratung bei der Einführung neuer IT-Verfahren in der Berliner Verwaltung

Das neue Berliner Datenschutzgesetz sieht nicht mehr vor, dass der Berliner Beauftragte für Datenschutz und Informationsfreiheit weiterhin ein Dateien- und Geräteregister führt. Damit wurde eine Regelung abgeschafft, die die Verwaltung zwang, komplexe Meldepflichten mit hohem Aktualisierungsbedarf wahrzunehmen. Eine praktische Bedeutung hat das bei uns geführte Register kaum erlangt. Weder haben die Bürger ihr Recht intensiv wahrgenommen, in diese Unterlagen Einsicht zu nehmen, um sich über die Umstände der Verarbeitung ihrer Daten in den öffentlichen Stellen Berlins zu informieren, noch konnte es für uns eine verlässliche Quelle bei der Planung und Durchführung von Kontrollmaßnahmen sein, weil die Unterlagen bereits kurze Zeit nach dem Eintreffen als veraltet anzusehen waren. Es ist daher im Interesse der Verwaltung und der Effizienz unserer Behörde zu begrüßen, dass dieser Bürokratismus beendet werden konnte. Es ist auch im Sinne der modernen Dezentralisierung der Datenschutzkontrolle, wenn die erforderlichen Übersichten bei den behördlichen Datenschutzbeauftragten geführt und der Öffentlichkeit zur Einsicht angeboten werden.

Eine andere Vorschrift, die sich als wesentlich wirksamer bei der Durchsetzung des Datenschutzes erwiesen hat, aber dennoch gern ignoriert wird, blieb unverändert: § 24 Abs. 3 Satz 3 BlnDSG verpflichtet die öffentlichen Stellen des Landes, uns über die Einführung neuer Automationsverfahren und wesentliche Änderungen automatisierter Datenverarbeitungen zu informieren. Zweck dieser Vorschrift ist, uns rechtzeitig Gelegenheit zur Stellungnahme zu geben, um mögliche Verstöße gegen das Datenschutzrecht vorab zu erken-

In § 24 Abs. 3 Satz 3 BlnDSG wurde im Normtext die Informationspflicht auf die wesentliche Änderung automatisierter Datenverarbeitungen erweitert, blieb also nicht unverändert. Die öffentlichen Stellen des Landes Berlin sind zur uneingeschränkten Beachtung des Normbefehls verpflichtet.

[42] Zur Gesamtproblematik vgl. die Broschüre der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Vom Bürgerbüro zum Internet: Empfehlungen zum Datenschutz für eine serviceorientierten Verwaltung. Hannover LfD Niedersachsen, 2000

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

nen und zu verhindern. Diese Beratungstätigkeit ist zumeist unnötig aufwendig, da die datenschutzrechtlich relevanten Fragestellungen nur selten kompakt behandelt werden, sondern verstreut in den häufig mehrere Leitz-Ordner umfassenden technischen Unterlagen verborgen sind. Wegen der Pflicht zur Erstellung von Sicherheitskonzepten auf der Grundlage plausibler Risikoanalysen durch die datenverarbeitenden Stellen und zur Durchführung von Vorabkontrollen bei sensiblen Verfahren durch die behördlichen Datenschutzbeauftragten gehen wir in Zukunft von einer wesentlichen Rationalisierung dieser Beratungstätigkeit aus. Dies muss der Befriedigung des erheblich gesteigerten Kontrollbedarfs in der privaten Wirtschaft zugute kommen.

Unter anderem haben wir folgende informationstechnische Vorhaben intensiv begleitet:

Im Bereich der Inneren Sicherheit haben wir uns mit dem Projekt der *Verfassungsschutzabteilung* der Senatsverwaltung für Inneres beschäftigt, die Tätigkeit in Zukunft mit einem integrierten IT-Verfahren für die verschiedenen Aufgabenbereiche zu unterstützen. Dieses seit langem unter dem Begriff „Amtsdatei“ geplante Projekt soll jetzt endlich angegangen werden. Jedoch blieb lange unklar, ob eine amtsinterne Planung realisiert werden oder ein woanders bewährtes System eingeführt werden soll. Wir werden dieses Projekt mit Interesse weiterverfolgen.

Es ist geplant, die Entwicklung der „Amtsdatei“ bis Ende 2002 abzuschließen und mit der Realisierung im Jahr 2003 zu beginnen.

Der *Polizeipräsident in Berlin* unterrichtete uns Anfang August über die im September vorgesehene Erneuerung wichtiger Systemkomponenten des polizeilichen Einsatzleitsystems (Projekt PELZ II). Weil grundsätzliche datenschutzrechtliche Bedenken nach kursorischer Betrachtung der Unterlagen nicht geltend zu machen waren, haben wir keine Einwände gegen die Inbetriebnahme erhoben, obwohl eine Befassung im Detail aus zeitlichen Gründen nicht mehr möglich und wegen des fortgeschrittenen Planungsstandes nicht mehr sinnvoll war. Zur Modernisierung des polizeilichen Informationssystems (Projekt POLIKS) liegen uns keine neueren Erkenntnisse vor.

Im Bereich der *Ordnungsverwaltung* steht die Modernisierung des automatisierten Melderegisters im Rahmen des Projektes EWW-neu im Mittelpunkt des Interesses. Es ist eng verzahnt mit dem Projekt ProBüd und den Bemühungen um eine interaktive Verwaltung. Auch das Bußgeldverfahren bedarf der Modernisierung. Wir sind über einen neuen Anlauf unter der Bezeichnung BOWI 21 informiert worden, der zu Beginn 2003 realisiert werden soll. Ein erster Versuch unter der Bezeichnung BOWI II war erfolglos abgebrochen worden.

Der Nachholbedarf der *Justiz* bei der Einführung moderner Technologien ist in der breiten Öffentlichkeit diskutiert worden. Tatsächlich gibt es jedoch seit Jahren eine Reihe von Einzelverfahren und -projekten in den unterschiedlichen Bereichen des Justizwesens. Zu

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

erinnern ist an unsere kritische Auseinandersetzung mit dem IT-Verfahren BASIS 2000 bei den Justizvollzugsanstalten[43].

Im Bereich der *Finanzverwaltung* haben wir uns noch einmal anlassbezogen mit den Zugriffsregelungen im alten DCL (Dezentrale Computer Leistung) der Oberfinanzdirektion Berlin beschäftigt[44]. Der Erfolg des bundesweiten Projektes FISCUS, welches die alten Besteuerungsverfahren in den Bundesländern ablösen sollte, ist wegen der öffentlich diskutierten Kostenentwicklung und der damit begründeten Rückzugsankündigung eines großen Bundeslandes in Frage gestellt.

Die Finanzministerkonferenz hat am 06.12.2001 beschlossen, das Projekt FISCUS auch nach dem Ausscheiden des Landes Bayern fortzusetzen, da es keine sinnvolle Alternative zu einer möglichst umfassenden Zusammenarbeit des Bundes und der Länder im Bereich der steuerlichen Automation gibt.

Im Gesundheitswesen sind verstärkte Automatisierungstendenzen im Bereich der bezirklichen *Gesundheitsämter* festzustellen. Zur elektronischen Unterstützung der Veterinär- und Lebensmittelämter steht das IT-Verfahren HAMLET 2000 vor der Einführung. Es betrifft die Aufgaben der Lebensmittelaufsicht, die Überwachung der Einhaltung des Handelsklassenrechts und der Preisangabenverordnung sowie die gesamte Veterinäraufsicht. Trotz der beabsichtigten baldigen Einführung bestehen in dem Projekt noch erhebliche Defizite im Hinblick auf die Erstellung und Umsetzung von Sicherheitskonzepten.

Das IT-Verfahren „HAMLET“ dient der Speicherung von Daten aus der Lebensmittel- und Veterinärüberwachung in den Veterinär- und Lebensmittelaufsichtsämtern (nicht in den Gesundheitsämtern).
Der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist wegen der noch zu verbessernden Schutzvorkehrungen an die Nutzer herangetreten. Die Anwendergemeinschaft aus den Veterinär- und Lebensmittelaufsichtsämtern hat sich bemüht, die Verfahrensempfehlungen zum Sicherungssystem umzusetzen. Wegen der unterschiedlichen Bezirksstrukturen ist jedoch kein einheitliches Sicherungskonzept möglich, sodass der BlnBDI im Februar 2002 auf ein „weitergehendes verfahrensspezifisches Sicherungskonzept“ verzichtet hat.
Die Bezirke haben somit in jeweils eigener Verantwortlichkeit die Pflicht, für ein ausreichendes Sicherheitskonzept unter Einbeziehung des/der bezirklichen Datenschutzbeauftragten und Umsetzung der erforderlichen Maßnahmen zu sorgen.

In den Anfängen steht noch die Planung eines IT-Verfahrens SpiDI für die Aufgabenerfüllung der *Sozialpsychiatrischen Dienste*. Dieses Aufgabengebiet arbeitet mit den besonders schutzbedürftigen Daten von psychisch kranken Menschen, so dass auch hier auf die strikte Beachtung der neuen Vorschriften zu den technisch-organisatorischen Maßnahmen des Datenschutzes zu achten ist. Dies gilt umso mehr, als die Verfahren meist im Rahmen der bezirklichen Rathausnetze betrieben werden, deren durchschnittliches Sicherheitsniveau bei den Sozialpsychiatrischen Diensten nicht ausreicht.

Der Senat geht von der in der bezirklichen Verantwortung liegenden Beachtung der maßgebenden Datenschutznormen bei der weiteren Planung und Realisierung aus.

Die *Sozialverwaltung* steht immer noch im Banne der Einführung eines Ersatzverfahrens für das veraltete und ergonomischen wie fachlichen Ansprüchen nicht mehr genügende DOS-Verfahren BASIS I auf der Grundlage von PROSOZ. Das ursprüngliche Vorhaben, mit BASIS 3000 ein Verfahren zu entwickeln, welches durch den Export in andere Kommunen zumindest teilweise refinanziert werden sollte, scheiterte, nachdem sich ein großes Softwarehaus als wichtiger Projektpartner zurückgezogen hatte. Das zweite Softwarehaus im Projektkonsortium wollte das Projekt allein weiterführen. Aufgrund der Verzögerungen, die sich

Die Darstellung des Berliner Beauftragten für Datenschutz und Informationsfreiheit entspricht teilweise nicht dem aktuellen Sachstand, da die im Bericht als offen erscheinenden Entscheidungen über einen möglichen Fortgang der Entwicklung von BASIS^{3000} durch das zweite Softwarehaus im Projektkonsortium sowie die Frage einer Zwischenlösung in Gestalt des Einsatzes der Windows-Version des PROSOZ-Verfahrens inzwischen getroffen sind:

Das Land Berlin sah sich gezwungen, die abgeschlossenen Verträge zu BASIS^{3000} aufzulösen. Das vom

[43] JB 2000, 2.2
[44] vgl. 4.3.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

dabei ergaben, sahen sich die Bezirke als Hauptanwender gezwungen, eine eigene vorübergehende Lösung anzustreben. Sie haben unter Führung eines Pilot-Bezirksamts eine Windows-Version des PROSOZ-Verfahrens zum Einsatz gebracht. Dieses Vorgehen wurde vom Rat der Bürgermeister gebilligt, jedoch von der für das Projekt Basis 3000 zuständigen Senatsverwaltung kritisiert. Dort will man an der Schaffung eines modernisierten und neu zu erstellenden Verfahrens festhalten und sieht die Windows-Variante des PROSOZ-Verfahrens nur als Notlösung an.

BlnBDI erwähnte Softwarehaus, das das Projekt allein weiterführen wollte, hatte sich als nicht in der Lage erwiesen, die im Rahmen eines beiderseitigen Vertragsmoratoriums dem Land Berlin zu erbringenden Nachweise über eine erfolgversprechende und vertragskonforme Projektdurchführung vorzulegen. Die Realisierung von BASIS^{3000} durch die beauftragten Firmen war somit endgültig gescheitert. Trotzdem ist die Ablösung der derzeit eingesetzten PROSOZ-Verfahren durch ein fachlich weiterentwickeltes und technologisch modernes IT-Verfahren im Berliner Sozialwesen zwingend geboten. Dies soll nunmehr nach Möglichkeit auf der Grundlage marktgängiger Standardprodukte erfolgen. Die hierzu erforderlichen Markterkundungen zur Vorbereitung eines Vergabeverfahrens laufen derzeit.

Seitdem sich die ersten Verzögerungen bei der Bereitstellung von BASIS^{3000} abzeichneten, wurde von den meisten Bezirksämtern nachdrücklich die Umstellung des MS-DOS basierten PROSOZ/S Verfahrens auf die moderner wirkende Windows-Variante als akzeptable Zwischenlösung gefordert. Der Rat der Bürgermeister hatte am 22.09.2000 auf der Grundlage eines von der BASIS-Geschäftsstelle vorgelegten Konzepts die Umstellung von PROSOZ/S für DOS auf die Windows-Version beschlossen. Die zuständige Senatsverwaltung stellte ihre anfänglichen Bedenken gegen den Versionswechsel auf die Windows-Variante, die mit Ausnahme der grafischen Bildschirmoberflächen in technologischer Hinsicht keinen und in fachlich-funktionaler Hinsicht nur wenig Fortschritt mit sich bringt, zurück. Sie setzte sich im Hauptausschuss dafür ein, die Finanzierung der Umstellungskosten des Versionswechsels sicherzustellen, um bis zu einer nicht vor dem Jahr 2005 erwarteten Verfügbarkeit eines Zielsystems die volle Arbeitsfähigkeit der Sozialämter durch eine zeitlich befristete Übergangslösung weiterhin zu gewährleisten. Die vom Rat der Bürgermeister mit der Projektdurchführung des Versionswechsels beauftragte BASIS-Geschäftsstelle plant, den Versionswechsel bis Mitte 2003 realisiert zu haben.

In der *Jugendhilfe* soll die derzeit im Einsatz befindliche Variante PROSOZ-J in Zukunft durch ein moderneres Verfahren ersetzt werden. Die Vorbereitungen für dieses Projekt mit dem Namen ISBJ (Integrierte Software Berliner Jugendhilfe) sind angelaufen.

Die derzeit in den Jugendämtern sehr unterschiedlich eingesetzte Variante PROSOZ/J für DOS soll in 2002 durch die abgestimmte und einheitliche Einführung von PROSOZ/J für Windows ersetzt werden. Darüber hinaus laufen die Vorbereitungen für das Projekt „Integrierte Software Berliner Jugendhilfe (ISBJ)„ in welches wesentliche IT-Fachverfahren der Jugendhilfe (auch PROSOZ/J) durch Weiterentwicklung bzw. Ersatz integriert werden.

Unter dem Kürzel InWo sollen in Zukunft sämtliche Verfahren aus dem Bereich des *Wohnungswesens* integriert werden. Dieses Verfahren setzt auf dem DiWo-Verfahren (Dialoggeführtes Wohnungswesen) auf und soll im nächsten Schritt alle Anwendungen im Wohnungswesen (u.a. die Verfahren Fehlbelegungsabgabe und Wohnberechtigungsschein) integrieren. Geplant ist auch eine Online-Nutzung, mit der Bürger InWo interaktiv als E-Government-Verfahren nutzen können.

Nach Zustimmung des Hauptausschusses des Abgeordnetenhauses und anschließender Auftragsvergabe in 2001 wurde Anfang 2002 mit der Entwicklung von InWo, in dem aufbauend auf das DiWo-Verfahren (Dialogisiertes Wohngeldverfahren) sämtliche Verfahren aus dem Bereich des Wohnungswesens integriert werden, begonnen. Die flächendeckende Einführung in den Bezirken ist Ende des 1. Quartals 2004 vorgesehen.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Auch die Bürgerämter sollen einen schnellen und aktuellen Zugriff für ihre Aufgaben erhalten.

Als Online-Komponente steht DiWo-Online bereits zur Verfügung, mit dieser kann der Bürger eine Wohngeldberechnung durchführen, um so schon im Vorfeld einen möglichen Wohngeldanspruch abzuprüfen. Die Realisierung weiterer Online-Komponenten im Bereich des Wohnungswesens ist geplant.

Im Bereich von *Wissenschaft und Forschung* wurden uns diverse Verfahren zur Unterstützung von Hochschulverwaltungen vorgestellt. Aktuell stehen wir in der Beratung der Technischen Universität Berlin, die nach der Technischen Fachhochschule[45] das zweite Versuchsobjekt für die Einführung einer Chipkarte als Studenten- und Mitarbeiterausweis darstellt. Unter anderem soll dieser Ausweis neben den üblichen Ausweisfunktionen zur Authentifizierung seiner Inhaber und zur Rationalisierung von Verwaltungsverfahren in der Hochschule auch als Signaturkarte für eine qualifizierte Signatur fungieren, mit der Rückmeldungen und Prüfungsanmeldungen als E-Government-Anwendungen den Studenten vom heimischen Computer aus ermöglicht werden sollen.

Im Bereich der *Kulturellen Angelegenheiten* ist im Sommer des Jahres das letzte Bezirksamt an das VÖBB-Verfahren *(Verbund Öffentlicher Bibliotheken Berlins)* angebunden worden. Nunmehr sind alle Bezirksämter und die großen Bibliotheken an das neue Verfahren angeschlossen.

Das in der Erprobungsphase befindliche Verfahren VHS-IT dient der Einführung eines multifunktionalen, einheitlichen, vernetzten und datenbankbasierten EDV-Fachverfahrens für alle Berliner *Volkshochschulen* und die für die Volkhochschulen zuständige Senatsverwaltung. Dabei sollen folgende Ziele erreicht werden: Überbezirkliche Bildungsberatung, Information und Buchung, Ausgleich bestehender Servicedefizite, Optimierung der Kursorganisation, der Erstellung und Auswertung der Statistiken, der Abrechnung und der Dozenten- und Teilnehmerverwaltung, Bereitstellung von Controlling-Informationen und Steuerungsdaten und die Schaffung der Voraussetzung für ein Online-Stadtinformations- und Buchungssystem im Internet. Unsere Beratung zu diesem Projekt ist noch nicht abgeschlossen, da sowohl in rechtlicher als auch in technisch-organisatorischer Hinsicht noch nicht alle Fragen abschließend geklärt werden konnten.

Das Projekt Elektronisches Ticketing der *BVG* wurde im vergangenen Jahr als Schwerpunktthema behandelt[46]. Die Darstellungen im Jahresbericht 2000 waren als konstruktive Vorschläge für eine datenschutzfreundliche Lösung des Konflikts zwischen dem Bedarf der BVG, möglichst viel über ihre Kunden zu erfahren, und der Verhinderung des gläsernen ÖPNV-Nutzers gedacht. Wie sich die BVG in diesem Konflikt zwischen dem Bedarf der Nutzer nach Einzelfahrtnachweisen und seinen Bedürfnissen nach Anonymität letztlich positioniert hätte, bleibt dahingestellt. In der

[45] JB 1998, 4.5.1
[46] JB 2000, 3.2

Zwischenzeit ist das Projekt in gemeinsame Vorhaben des Verbundes der Verkehrsunternehmen in Berlin und Brandenburg sowie mit dem Verband der deutschen Verkehrsunternehmen eingeflossen, so dass die datenschutzrechtliche Beratung in Zukunft in Koordination mit den anderen Landesbeauftragten für den Datenschutz und den anderen Aufsichtsbehörden stattfinden wird.

3. Schwerpunkte im Berichtsjahr

3.1 Sicherheit in Europa

Schengener Informationssystem

Die Ereignisse des 11. September haben nicht nur in Deutschland, sondern auch in Europa eine Diskussion darüber ausgelöst, wie europaweit eine Verbesserung der Zusammenarbeit der Sicherheitsbehörden erreicht werden kann. Im Folgenden soll deshalb ein Überblick über den Stand sowie die offenen datenschutzrechtlichen Probleme gegeben werden.

Die Regierungen der Staaten der Benelux-Wirtschaftsunion, die Bundesrepublik Deutschland und die Französische Republik unterzeichneten am 14. Juni 1985 in dem kleinen Ort Schengen ein Übereinkommen zur Schaffung eines gemeinsamen Raumes für den freien Waren- und Personenverkehr. Vorgesehen war, die Kontrollen an den gemeinsamen Grenzen der Unterzeichnerstaaten Schritt für Schritt abzubauen. Um trotz Abschaffung der gemeinsamen Binnengrenzen in dem entstandenen Gemeinschaftsraum ein einheitliches Sicherheitsniveau zu gewährleisten, unterzeichneten dieselben Vertragsparteien am 19. Juni 1990 das Übereinkommen zur Durchführung des Übereinkommens von Schengen, das am 26. März 1995 in Kraft trat. Zu den konkreten Ausgleichsmaßnahmen, die im Schengener Durchführungsübereinkommen (SDÜ) beschlossen wurden, zählen u. a.

- die Angleichung der jeweiligen Visumpolitik,
- eine gemeinsame Politik zur Bestimmung des für die Prüfung eines Asylantrages zuständigen Staates,
- die Verbesserung der polizeilichen und justiziellen Zusammenarbeit,
- eine intensivere Bekämpfung des illegalen Betäubungsmittelhandels,
- die Angleichung der Kontrollstandards an den Außengrenzen des Schengener Raumes sowie
- die Einrichtung eines Schengener Informationssystems (SIS).

Zu den ursprünglichen Vertragsparteien sind weitere hinzugekommen. Derzeit sind 15 europäische Staaten am SIS beteiligt. Das SIS setzt sich aus einem nationalen Teil (N.SIS) in der jeweiligen Vertragspartei und einer gemeinsamen technischen Unterstützungseinheit (C.SIS) zusammen. Ziel der in Straßburg eingerichteten technischen Unterstützungseinheit ist die inhaltli-

che Angleichung aller N.SIS. Hierzu ist im C.SIS ein Bestand enthalten, der durch die Online-Übermittlung von Daten sicherstellt, dass die nationalen Bestände identisch bleiben. Die Datenübermittlung erfolgt nach den von den Vertragsparteien für die technische Unterstützungseinheit gemeinsam festgelegten Protokollen und Verfahren. Durch einen Abruf im automatisierten oder nicht-automatisierten Verfahren haben die von den Vertragsparteien bezeichneten Behörden (mit Polizeiaufgaben betraute Dienststellen, Botschaften und Konsulate usw.) unmittelbaren Zugriff auf den Datenbestand des SIS. Dieser umfasst Daten über Personen, Sachen und Fahrzeuge (Art. 94 SDÜ).

Über einzelne Personen dürfen deren Personenstand, Aliasnamen, besondere physische Merkmale, die etwaige Angabe, dass sie bewaffnet oder gewalttätig sind, und das Verhalten im Fall einer Entdeckung im SIS gespeichert werden. Als Ausschreibungsgründe gelten

- Festnahme zum Zweck der Auslieferung (Art. 95 SDÜ),
- Fahndung nach Vermissten, Fahndung nach Minderjährigen oder Personen, die aufgrund einer Entscheidung einer zuständigen Behörde in Gewahrsam zu nehmen sind (Art. 97 SDÜ),
- Festnahme wegen Erscheinens vor Gericht, auch als Zeuge, im Rahmen eines Strafverfahrens oder wegen Verbüßens einer Freiheitsstrafe (Art. 98 SDÜ),
- verdeckte Registrierung und gezielte Kontrolle zur Strafverfolgung, zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Abwehr von erheblichen Gefährdungen für die Sicherheit des Staates (Art. 99 SDÜ),
- Einreiseverweigerung aufgrund einer Entscheidung einer Verwaltungsbehörde oder eines Gerichtes – nur bei Personen, die nicht Staatsangehörige der Mitgliedstaaten der Europäischen Gemeinschaft sind – (Art. 96 SDÜ).

Angaben über Sachen können – einschließlich des Namens ihrer Eigentümer – im SIS gespeichert werden, wenn sie sich auf gestohlene, unterschlagene oder sonst abhanden gekommene Fahrzeuge, Schusswaffen, Schriftstücke und Banknoten beziehen, die zur Sicherstellung oder Beweissicherung im Strafverfahren gesucht werden (Art. 100 SDÜ). Unabhängig davon dürfen auch Daten über gesuchte Fahrzeuge zur verdeckten Registrierung oder gezielten Kontrolle (Art. 99 SDÜ) eingegeben werden. Diese Kategorie von Daten erlaubt die Speicherung von Angaben über den Fahrer und die Insassen der überwachten Fahrzeuge.

Folgende Grundsätze des Datenschutzes sind im Durchführungsübereinkommen aufgeführt:

- Grundsatz der Zweckgebundenheit hinsichtlich der Speicherung der Daten und ihrer Verwendung (Art. 94 bis 100, 102 SDÜ),

- Verbot der Verarbeitung sensibler Daten und abschließende Aufzählung der zulässigen Daten (Art. 94 SDÜ),
- Festlegung der Datenempfänger (Art. 101 SDÜ),
- Verbot des Kopierens der Ausschreibung einer anderen Vertragspartei in einen nationalen Bestand und Beschränkung der Vervielfältigung auf technische Zwecke (Art. 102 SDÜ),
- Verpflichtung zur Protokollierung jeder zehnten Datenübermittlung zur Kontrolle der Zulässigkeit (Art. 103 SDÜ),
- Festlegung einer Aufbewahrungsdauer für die Daten (Art. 112 und 113 SDÜ),
- Verpflichtung zur Aufbewahrung der gelöschten Daten während eines Jahres in der technischen Unterstützungseinheit zur nachträglichen Kontrolle ihrer Richtigkeit und der Rechtmäßigkeit ihrer Speicherung (Art. 113 Abs. 2 SDÜ).

Unabhängig davon haben Betroffene das Recht auf:

- Auskunft über die zu ihrer Person im SIS gespeicherten Daten (Art. 109 SDÜ),
- Berichtigung von unrichtigen oder Löschung von unrechtmäßig gespeicherten Daten (Art. 110 SDÜ),
- Erhebung einer Klage auf Berichtigung, Löschung, Auskunftserteilung oder Schadensersatz (Art. 111 SDÜ),
- Überprüfung der Daten (Art. 114 Abs. 2 SDÜ).

Mit der Einrichtung des SIS ging die Schaffung einer Gemeinsamen Kontrollinstanz für den Schutz personenbezogener Daten (GK) einher. Die GK, der zwei Vertreter jeder nationalen Kontrollinstanz der Vertragsparteien angehören, überprüft vordringlich die ordnungsgemäße Anwendung der SDÜ-Bestimmungen durch die technische Unterstützungseinheit des SIS (Art. 115 SDÜ). Zusätzlich hat sie die Aufgabe der Beratung und der Angleichung der nationalen Praktiken oder Rechtslehren. Deutschland ist in der GK durch den Bundesbeauftragten für den Datenschutz und den Hessischen Datenschutzbeauftragten vertreten. Jede Vertragspartei hat eine nationale Instanz mit der unabhängigen datenschutzrechtlichen Kontrolle – unter Beachtung des nationalen Rechts – des nationalen Datenbestandes (N.SIS) zu beauftragen.

In den vergangenen Jahren haben wir mehrfach über datenschutzrechtliche Probleme bei der Ausschreibung von Betroffenen im SIS berichtet[47]. Vor dem Hintergrund, dass das Bundesministerium des Innern die Länder – angesichts der festgestellten hohen Zahl unzulässiger Ausschreibungen – gebeten hatte, eine SDÜ-konforme Ausschreibungspraxis sicherzustellen, ging es dabei insbesondere um die Voraussetzungen, unter denen eine Ausschreibung im SIS zulässig ist. Bei den Ausschreibungen zur Einreiseverweigerung nach

[47] JB 1999, 4.2.3; JB 2000, 4.2.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Art. 93 Abs. 3 SDÜ konnte mit der zuständigen Senatsverwaltung für Inneres Übereinstimmung erzielt werden, dass eine Ausschreibung im SIS nur bei der Ausweisung, Zurückweisung oder Abschiebung eines Betroffenen zulässig ist. Eine Ausschreibung zur Aufenthaltsfeststellung des Betroffenen ist – gestützt auf Art. 93 Abs. 3 SDÜ – dagegen, auch wenn ansonsten die Voraussetzungen für eine Abschiebung vorliegen, nicht erlaubt.

Ein weiterer datenschutzrechtlicher Aspekt konnte bisher dagegen nicht zur Zufriedenheit gelöst werden: Das BKA verlängert die Ausschreibungen nach Ablauf einer dreijährigen Speicherungsdauer automatisch um drei Jahre, sofern sich die zuständige Ausländerbehörde auf einen entsprechenden Hinweis des BKA nicht ausdrücklich gegen die Verlängerung der Speicherung ausspricht. Dabei verlangt Art. 112 SDÜ, dass spätestens nach drei Jahren die Erforderlichkeit einer weiteren Speicherung der Ausschreibungsdaten zu überprüfen und festzustellen ist. Die Senatsverwaltung für Inneres hat diesen Missstand zum Anlass genommen und das Bundesministerium des Innern um eine Stellungnahme zur Rechtmäßigkeit der gegenwärtigen Verwaltungspraxis gebeten. Dieses hat sich dazu bisher nicht abschließend geäußert. Es hat jedoch angekündigt, dass die sicherheitsrelevanten Teile des SDÜ – angesichts der Veränderungen der aktuellen Sicherheitslage durch die Ereignisse in den USA – einer kritischen Überprüfung zu unterziehen sind.

Die Ausführungen des Berliner Beauftragten für Datenschutz und Informationsfreiheit zur Problematik der Verlängerung von Speicherungen der Ausschreibungen im Schengener Informationssystem treffen zu. Was die ausstehende abschließende Stellungnahme des Bundesministeriums des Innern zur Rechtmäßigkeit der gängigen Verwaltungspraxis betrifft, so wird die Senatsverwaltung für Inneres das Bundesministerium des Innern hierauf hinweisen.

Europol

Neben der Schaffung eines freien Waren- und Personenverkehrs durch das Schengener Übereinkommen sind im Vertrag über die Europäische Union (EUV) als wichtigste Ziele die Gewährung eines Höchstmaßes von Sicherheit und Recht für die Bürgerinnen und Bürger festgeschrieben worden (Art. 29 EUV). Aus diesem Grund wurde 1992 im Maastrichter Vertrag über die Europäische Union die Einrichtung von Europol beschlossen, die nach der Ratifizierung der Europol-Konvention (EPK) 1998 zum 1. Juli 1999 den Dienst aufgenommen hat.

Europol ist die polizeiliche Strafverfolgungsbehörde der Europäischen Union und befasst sich sowohl mit der Sammlung von Informationen über Straftaten als auch mit ihrer Analyse. Damit sollen die Leistungsfähigkeit der zuständigen Behörden der Mitgliedstaaten und ihre Zusammenarbeit im Hinblick auf die Verhütung und die Bekämpfung des Terrorismus, des illegalen Drogenhandels und sonstiger schwerwiegender Formen der internationalen Kriminalität verbessert werden, sofern zwei oder mehr Mitgliedstaaten betroffen sind und ein gemeinsames Vorgehen erforderlich ist (Art. 2 EPK). Der Anhang zu Art. 2 enthält eine umfassende Liste sonstiger schwerwiegender Formen der internationalen Kriminalität, mit denen sich Europol ergänzend zu den bereits in Art. 2 vorgesehenen Zielen befassen könnte. Außerdem können die Befugnisse von Europol durch die Beschlusse des Europäi-

schen Rates erweitert werden. Durch einen solchen Rechtsakt ist die Zuständigkeit von Europol auch auf die Geldwäsche im Allgemeinen ausgedehnt worden. Außerdem ist geplant, Europol mit echten operativen Zuständigkeiten auszustatten.

Europol erhält seine Daten entweder von den nationalen Kontaktstellen, die dann auch für die Daten selbst verantwortlich sind, oder erhebt Daten selbst. Jedes Land hat daher auch eine nationale Kontrollinstanz (Art. 23 EPK), die die Zulässigkeit der Verarbeitung der nationalen Stelle prüfen soll. Jeder betroffene Bürger kann diese nationale Kontrollinstanz ersuchen, die Zulässigkeit der Eingabe und der Übermittlung an Europol sowie des Abrufes durch den Mitgliedstaat zu prüfen. Dabei gilt dann das nationale Recht.

Jeweils zwei Vertreter dieser nationalen Kontrollinstanz jedes Mitgliedslandes bilden die gemeinsame Kontrollinstanz (Art. 24 EPK), die ebenfalls vom Betroffenen angerufen werden kann. Diese Kontrollinstanz prüft, ob durch die Datenverarbeitung bei Europol Rechte von Betroffenen nach Maßgabe der Europol-Konvention verletzt wurden. Stellt die gemeinsame Kontrollinstanz Verstöße fest, so richtet sie Bemerkungen an den Direktor. Mit dem In-Kraft-Treten des Amsterdamer Vertrages nutzen die drei Kontrollstellen für Schengen, Europol und das Zollinformationssystem ein gemeinsames Sekretariat.

Daten, die nach nationalem Recht gelöscht werden müssen, können weiter gespeichert werden, wenn Europol ein weitergehendes Interesse an diesen Daten geltend macht und über Erkenntnisse verfügt, die der Herkunftsstaat der Daten nicht besitzt (Art. 21 Abs. 4 EPK). Es werden hier also nationale Datenschutzstandards außer Kraft gesetzt, ohne dass der von der Speicherung Betroffene zwingend informiert werden muss oder ein Rechtsmittel dagegen hat. Gespeichert werden Daten über Personen (Art. 8 Abs. 1, Art. 10 Abs. 1 EPK), die

- einer der in der EPK aufgezählten Straftat verdächtig oder wegen ihr verurteilt sind, und Personen, bei denen schwerwiegende Tatsachen dafür sprechen, dass sie eine solche Tat begehen,
- Zeugen solcher Taten oder mögliche Zeugen der Strafverfolgung,
- Opfer oder potenzielle Opfer solcher Taten,
- Kontakt- und Begleitpersonen sind, und
- Personen, die Informationen über die betreffenden Straftaten liefern können.

Bei einer derartig weit gefassten Speicherungsbefugnis auch im Vorfeld von Straftaten können Daten in einem Maß erhoben und verarbeitet werden, wie es das bundesdeutsche Recht nicht zulässt. Über die jeweiligen Personen dürfen folgende Merkmale (Art. 8 Abs. 3 und 4 EPK) gespeichert werden:

- Name, Geburtsname, Vorname, Alliasnamen,

- Geburtsdatum und –ort,
- Staatsangehörigkeit,
- Geschlecht,
- andere zur Identitätsfeststellung geeignete Merkmale, insbesondere objektive und unveränderliche Merkmale,
- Straftaten und Tatvorwürfe,
- Tatzeiten und -orte,
- Tatmittel, die verwendet wurden oder verwendet werden könnten,
- aktenführende Dienststelle und deren Aktenzeichen,
- Verdacht der Zugehörigkeit zu einer kriminellen Organisation und
- Verurteilungen wegen Straftaten, die in die Zuständigkeit von Europol fallen.

Auch hier können die unbestimmten Begriffe wie „andere zur Identitätsfeststellung geeignete Merkmale“ oder Vermutungen wie „verwendet werden könnten“ sehr weit ausgelegt werden, ohne dass eine rechtliche Überprüfung möglich ist.

Europol kann von folgenden Einrichtungen Daten entgegennehmen oder anfordern (Art. 10 Abs. 4 EPK):

- den Europäischen Gemeinschaften und allen ihren öffentlich-rechtlichen Institutionen,
- den sonstigen öffentlich-rechtlichen Einrichtungen der Europäischen Union,
- Einrichtungen, die von zwei oder mehr Staaten der Europäischen Union geschaffen wurden,
- Drittstaaten,
- internationalen Organisationen und den ihnen zugeordneten öffentlich-rechtlichen Einrichtungen,
- sonstigen öffentlich-rechtlichen Einrichtungen, die aufgrund einer Übereinkunft zwischen zwei oder mehr Staaten bestehen und
- Interpol.

Hier sind insbesondere hinsichtlich der Drittstaaten mit zweifelhaftem Datenschutzniveau oder bei den internationalen Einrichtungen Präzisierungen dringend erforderlich.

Europol nimmt aber von solchen Institutionen und Staaten nicht nur Daten entgegen, sondern übermittelt in Einzelfällen zur Verhütung und Bekämpfung von Straftaten auch Daten an sie (Art. 18 EPK). Dies soll allerdings nur erfolgen, wenn dort ein angemessener Datenschutzstandard gewährleistet ist. Offen bleibt allerdings, wann ein Standard angemessen ist und wer ihn prüft.

Die Mitarbeiter von Europol sind von der Strafverfolgung freigestellt (Art. 41 EPK). Ein entsprechendes Protokoll wurde auch von der Bundesrepublik

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Deutschland ratifiziert. Die Mitarbeiter genießen Immunität von jeglicher Gerichtsbarkeit (Art. 8 des Protokolls zu Art. 41 EPK). Das umfasst die Haftung bei unzulässiger oder unrichtiger Datenverarbeitung. Die Mitarbeiter oder die Behörde sind zwar an die Europol-Vorschriften gebunden; Konsequenzen für ihr Tun oder Lassen haben sie jedoch nicht zu befürchten. Hier ist eine klarstellende Regelung erforderlich, damit Regelverstöße besonders in diesem Bereich nicht nur disziplinarisch geahndet werden können, sondern auch justiziabel sind.

Eurojust

Noch ist Europol eine Polizeibehörde, die keiner Aufsicht durch Justiz oder Parlament unterliegt. Über unbestimmte Rechtsbegriffe wie „schwerwiegende Formen internationaler Kriminalität“ oder „kriminelle Organisationsformen“ (Art. 2 EPK) und einen langen Katalog mit Kriminalitätsfeldern sowie eine zusätzliche Öffnungsklausel kann eine Zuständigkeit im Bedarfsfall fast immer begründet werden. Jede Form der Weisungsgebundenheit wird ausgeschlossen. Ein von den Mitgliedstaaten zusammengesetzter Verwaltungsrat „wirkt mit“, „sorgt“, „prüft“ und „billigt“ (Art. 28 EPK), hat aber keinen Einfluss auf die konkrete Arbeit von Europol. Sowohl dem europäischen als auch den nationalen Parlamenten bleibt nur, Berichte unter Wahrung der Verschwiegenheits- und Geheimhaltungspflichten (Art. 34 EPK) entgegenzunehmen. Auch gegenüber den Regierungen existieren keine Verantwortlichkeiten. Sofern der Betroffene selbst von seinen Datenschutzrechten Gebrauch machen will, wird er auf das auseinanderweichende nationale Recht verwiesen. Bei der Wahrung des Rechts auf Auskunft, Berichtigung und Löschung hat Europol ein gerichtlich nicht nachprüfbares Widerspruchsrecht (Art. 19, 20 EPK). Die im deutschen Recht geltende Justizförmlichkeit eines Ermittlungsverfahrens unter der Leitung der Staatsanwaltschaft existiert bei den sensiblen internationalen Verfahren bei Europol nicht.

Bereits 1999 hatte der Europäische Rat in Tampere auf Betreiben der Bundesregierung daher die Einrichtung einer gemeinsamen Stelle „Eurojust“ zur Bekämpfung schwerer Kriminalität beschlossen. Am 6. Dezember 2001 wurde der erforderliche rechtliche Rahmen für die Errichtung dieser Stelle geschaffen. Um die Zeit bis zum In-Kraft-Treten des Regelwerkes zu überbrücken, hat der Rat im Vorgriff auf Eurojust im Dezember 2000 die Einrichtung einer vorläufigen Stelle (genannt: „Pro-Eurojust“) beschlossen. Sie hat ihre Arbeit im März 2001 aufgenommen.

Entsprechend den Beschlussvorgaben des Europäischen Rates vom Oktober 1999 soll Eurojust vorrangig der Unterstützung und Verbesserung der Rechtshilfe dienen und dabei u.a. folgende Punkte umfassen:

- Service-Angebote für die Strafverfolgungspraxis (Vorhalten eines Sprachdienstes sowie Bereitstellung von Rechtsdokumenten und weiterer wichtiger Informationen über nationale Verfahrensordnungen),

Der Senat begrüßt die am 28. Februar 2002 vom Europäischen Rat endgültig beschlossene Errichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität mit - vorläufigem - Sitz in Den Haag. Die Initiative zur Errichtung von Eurojust ging beim Europäischen Rat in Tampere (Finnland) 1999 maßgeblich von deutscher Seite aus. Sie wurde von den Justizministerinnen und -ministern der Länder unterstützt und über die Bundesministerin der Justiz, an die sich die Justizministerkonferenz mit mehreren Beschlüssen gewandt hat, auch inhaltlich mitgestaltet. Die Beschlüsse der Justizministerkonferenz wurden durch die AG Europa des Strafrechtsausschusses unter der Leitung der Justizverwaltung Berlin vorbereitet, die hierzu zahlreiche Sachverständige aus Wissenschaft, Verwaltung, Strafrechtspraxis und Anwaltschaft gehört hat. Zwischen dem Berliner Beauftragten für Datenschutz und Informationsfreiheit und der Justizverwaltung hat zu diesem Thema ebenfalls ein Austausch stattgefunden.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

- Vermittlung sachdienlicher Direktkontakte,
- Clearing-Funktion für auftretende Fragen in supranational geführten Ermittlungsverfahren (Auslegung von Rechtshilfeübereinkommen und Zuständigkeiten).

Die sachliche Zuständigkeit von Eurojust soll sich insbesondere auf den Bereich der organisierten Kriminalität und auf kriminelle Verhaltensweisen im Bereich der schweren Kriminalität erstrecken, wenn mindestens zwei Mitgliedstaaten hiervon betroffen sind. Die konkreten Aufgaben sind:

- Ermittlungsersuchen an zuständige Behörden der Mitgliedstaaten,
- Unterrichtung der zuständigen Behörden über weitgreifende Ermittlungsmaßnahmen,
- Ersuchen um Koordinierung an Mitgliedstaaten,
- Koordinierung und logistische Unterstützung auf Ersuchen der Mitgliedstaaten,
- generelle und konkrete Erleichterung der Erledigung von Rechtshilfesachen,
- Ausbau der Dokumentations-Datenbank des Europäischen Justiziellen Netzes,
- Beistand für Europol (auf Ersuchen) insbesondere durch Erstattung von Gutachten aufgrund von Europol-Analysen,
- Vermittlung/Erleichterung von Registeranfragen an die Mitgliedstaaten.

Strittig ist zurzeit noch die Frage, ob Eurojust ermittlungsinitiierend oder eher nur auf Ersuchen der Mitgliedstaaten tätig werden soll. Fraglich ist ferner, ob Eurojust gestaltenden Einfluss auf die so genannten ermittlungsinitiierenden Analysen von Europol nehmen kann, die einer justiziellen Kontrolle – oder zumindest Begleitung – bedürfen.

Eurojust soll sich aus je einem Richter, Staatsanwalt oder Polizeibeamten mit gleichwertigen Befugnissen pro Mitgliedstaat nebst einem Vertreter zusammensetzen. Diese handeln als so genannte „nationale Mitglieder“ für den und im Auftrag des Entsendestaates.

Um seine Aufgaben wahrnehmen zu können, kann Eurojust sowohl durch seine einzelnen Mitglieder als auch als Kollegium handeln. Wenn es sich jedoch um Angelegenheiten von allgemeiner Bedeutung handelt oder es von einem Mitgliedstaat besonders gewünscht wird, ist ein Handeln des Kollegiums vorgesehen.

Eurojust besitzt eigene Rechtspersönlichkeit ; die nationalen Mitglieder von Eurojust unterliegen gleichwohl dem nationalen Recht ihres Herkunftslandes, weshalb sich der Zugriff auf die nationalen Straf- und Verfahrensregister nach nationalem Recht richtet.

Nach alledem findet damit keine wirkliche Verlagerung innerstaatlicher Befugnisse auf eine europäische Stelle statt.

Wie der Berliner Beauftragte für Datenschutz und Informationsfreiheit zu Recht herausstellt, kann durch Eurojust in seiner gegenwärtigen Ausgestaltung die teilweise notwendige justizielle Einbindung von Europol, insbesondere bei der Verarbeitung personenbezogener Daten im Rahmen von Analyseprojekten zum Zweck der Strafverfolgung, nicht gewährleistet werden. Nach Vorstellung der Justizministerkonferenz - die der Senat teilt - sollte Eurojust diese Aufgabe jedoch künftig zugewiesen werden.

Zur Klärung der Frage, inwieweit Bedarf einer justiziellen Kontrolle gegenüber Europol - auch angesichts der zu erwartenden Ausweitung seiner Kompetenzen - besteht und welche Institution diese Kontrolle wahrnehmen könnte, ist ebenfalls unter der Leitung der Berliner Justizverwaltung eine gemeinsame Projektgruppe aus Vertretern der Justiz- und Innenverwaltungen der Länder und des Bundes eingesetzt worden. Die Projektgruppe wird voraussichtlich im Herbst einen Bericht vorlegen, der dem Berliner Beauftragten für Datenschutz und Informationsfreiheit, ggf. nach Kenntnisnahme der Innen- und Justizministerkonferenz, zur Verfügung gestellt werden wird.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Zu begrüßen ist jedoch, dass die von den Datenschutzbeauftragten seit langem geforderte justizielle Einbindung der von Europol zusammengetragenen Daten mit der Errichtung von Eurojust vorangetrieben werden soll. Nur eine solche Einbindung gewährleistet, dass die erhobenen Daten nicht politischen, polizeitaktischen oder anderen Präferenzen bei Europol unterliegen, sondern einer justizförmigen Behandlung unterworfen sind. Der Anspruch der Justiz, ihre Funktion als Leiterin des Ermittlungsverfahrens auch auf europäischer Ebene gegenüber der Polizei wahrzunehmen, wird durch Eurojust damit erstmalig institutionell umgesetzt und verschafft ihm insoweit einen starken symbolischen Charakter. Nach der Einrichtung von Europol ist diese ständige justizielle Einrichtung erforderlich, um als derzeit einziges politisch erreichbares Instrument der Strafjustiz in Europa der Gewaltenteilung Ausdruck zu verleihen.

Ebenfalls positiv ist, dass mit der Errichtung von Eurojust die nationalen Staatsanwaltschaften eine direkte Möglichkeit erhalten, auf das Informationssystem von Europol zuzugreifen, um strafrechtsrelevante Daten zu erlangen. Die bisherige Zwischenschaltung des BKA bei der Datenanforderung verliert damit ihre Brisanz, denn es entfällt die Möglichkeit für das BKA, die Weiterleitung von Informationen von eigenen Interessenlagen (z. B. polizeitaktischen Erwägungen) abhängig zu machen. Insoweit stärkt Eurojust die justizförmige Kontrolle der europaweiten Ermittlungstätigkeit von Europol.

Bedauerlich ist, dass wegen der Kürze der Zeit notwendige Vertragsverhandlungen zwischen den betreffenden EU-Staaten nicht möglich waren. Für die Legitimation einer justiziellen Institution, die möglicherweise sogar „Keimzelle“ für eine europäische Staatsanwaltschaft sein könnte, war ein derartiger, fast ausschließlich durch die Exekutive abgestützter Entscheidungsprozess nicht ausreichend.

Sollte Eurojust zu einer europäischen Großbehörde heranwachsen, die sensibelste Daten auch von Opfern und Zeugen sammeln soll – und damit in hohem Maß in Bürgerrechte eingreifen würde –, wäre die Schaffung einer entsprechenden demokratischen Legitimation, etwa durch eine Konvention unter Beteiligung des Europäischen Parlamentes, erforderlich.

Die in Art. 10 des Beschlussentwurfes getroffene Regelung, wonach Eurojust in dort näher bezeichnetem Umfang eigenständig Dateien anlegen kann, wirft die Frage der datenschutzrechtlichen Verantwortlichkeit auf. Aus den Vorschriften der Art. 11 bis 15 lässt sich folgern, dass Eurojust die so gespeicherten Daten in eigener Zuständigkeit verwaltet. Fraglich ist, wie die nationalen Auskunftsrechte der Betroffenen auszugestalten sind. Sofern die datenschutzrechtliche Verantwortlichkeit abschließend bei Eurojust gesehen wird (z. B. hinsichtlich der Daten, die von Europol eingestellt werden), bedarf es eines Auskunfts- und Informationsanspruches zugunsten der betroffenen Privatpersonen. Im Interesse eines effektiven Rechtsschutzes

gegen die unzulässige Speicherung persönlicher Daten ist eine solche Norm unerlässlich.

Ähnlich der Diskussion um die Weitergabe von Daten bei Europol ist zu fordern, dass der Gang der Daten auch bei Eurojust nachvollziehbar dokumentiert wird. Es muss erkennbar sein, welche Daten wann an wen weitergegeben bzw. wann welche Daten durch wen angefordert wurden, um eine effektive Kontrolle des Datenganges aus datenschutzrechtlicher Sicht zu ermöglichen. Insbesondere im Hinblick auf die Möglichkeit von Europol, Daten an Drittstaaten weiterzugeben – und damit ein besonderes Gefahrenpotenzial des Datenmissbrauches zu begründen –, erscheint es unumgänglich, den Übertragungsgang von Daten bereits bei Eurojust zu dokumentieren. Nur so wird eine effektive Überprüfung datenschutzrechtlich relevanter Vorgänge möglich. An dieser Stelle müsste auch die Frage der diesbezüglichen Speicherfristen diskutiert werden.

Im Hinblick auf die sensiblen personenbezogenen Daten, die von Eurojust erhoben, verarbeitet und genutzt werden, sind – unter besonderer Berücksichtigung der eigenen Rechtspersönlichkeit von Eurojust – umfassende Datenschutzvorschriften erforderlich. Die Datenschutzbeauftragten des Bundes und der Länder haben daher folgende Problempunkte herausgehoben[48]:

- Zulässigkeit des Informationsaustausches mit Partnern,
- Voraussetzung für die Verarbeitung personenbezogener Daten,
- Ermittlungsindex und Dateien,
- Auskunftsrechte Betroffener,
- Änderung, Berichtigung und Löschung von Daten,
- Speicherungsfristen,
- Datensicherheit,
- Gemeinsame Kontrollinstanz für Eurojust,
- Rechtsschutz für Betroffene,
- Rechtssetzungsbedarf.

Nach dem 11. September 2001 fordern Rechtsexperten darüber hinaus wieder verstärkt eine europäische Staatsanwaltschaft sowie zentrale Strafregister im Kampf gegen das internationale Verbrechen und den Terrorismus. Sie halten angesichts der Anschläge in den USA eine schnelle und unkomplizierte Zusammenarbeit von Polizei und Justiz in Europa für notwendig. Dass Eurojust die „Keimzelle“ einer solchen europäischen Staatsanwaltschaft sein könnte, ist durch die jüngsten Ereignisse in den USA wieder realistischer geworden.

So will man die nationalen Visa-Dateien vernetzen und „Eurodac“ der Polizei öffnen – eine Fingerabdruckda-

[48] Entschließungen der 62. Konferenz zu „EUROJUST-Vorläufer einer künftigen europäischen Staatsanwaltschaft?“. In: Anlagenband, a.a.O., I.3

tei, die bislang nur in Asylverfahren eingesetzt wird. Polizei und Staatsanwaltschaften sollen vollen Zugriff auf das „Schengener Informationssystem“ (SIS) bekommen, in dem polizeirelevante Daten über EU-Bürger enthalten sind. Auch eine intensive strafrechtliche Zusammenarbeit mit den USA auf dem Gebiet der Terrorismusbekämpfung wird angestrebt. Derzeit scheitert eine direkte Kooperation mit dem FBI an einer fehlenden Übereinkunft für den Datenschutz.

3.2 Gentests - Gierige Blicke ins Innerste des Privaten

Die genetische Forschung schafft schrittweise Möglichkeiten, durch Tests den genetischen Einblick in den Kernbereich der Privatsphäre, etwa in Gesundheitsdispositionen, Anlagen der Persönlichkeitsstruktur oder den voraussichtlichen Lebensverlauf zu erhalten. Solche Untersuchungen schaffen eine ganz neue Qualität des Wissens und des Offenlegens persönlichster Daten. Sowohl für die Betroffenen selbst als auch für dritte Personen einschließlich deren Familienangehörigen kann es von lebensentscheidender Bedeutung sein, ob und inwieweit sie selbst und wer außer ihnen von solchen Ergebnissen Kenntnis erhalten. Aus der grundgesetzlichen Verpflichtung zur Wahrung der Menschenwürde und des allgemeinen Persönlichkeitsrechts entsteht die Frage, ob und aus welchen Anlässen überhaupt genetische Untersuchungen am Menschen vorgenommen werden dürfen. Mit der Würde des Menschen und dem allgemeinen Persönlichkeitsrecht sind Verhältnisse nicht vereinbar, in denen die Betroffenen nicht mehr ihr Recht auf Nichtwissen um ihre genetischen Anlagen und Dispositionen wahrnehmen können, weil faktische wirtschaftliche oder gesellschaftliche Zwänge sie zu einem anderen Handeln veranlassen.

Da mit der Entschlüsselung des menschlichen Genoms entscheidende wissenschaftliche Durchbrüche gelangen und Technologien entwickelt wurden, mit denen in kürzester Zeit in einem erheblichen Umfang genetische Proben untersucht werden können, hatte im Oktober 2000 die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beschlossen, eine Arbeitsgruppe zu bilden, die sich mit den datenschutzrechtlichen Konsequenzen beschäftigen sollte[49].

Im Dezember 2000 stellte fast zeitgleich mit der Konstituierung der Arbeitsgruppe die *Enquetekommission des Deutschen Bundestages „Recht und Ethik der modernen Medizin“* den Datenschutzbeauftragten eine Reihe von Fragen. Die Koordinierung der Beantwortung dieser Fragen sowie der Arbeit der Arbeitsgruppe übernahm der Hamburgische Datenschutzbeauftragte. In die Beantwortung flossen auch die in Berlin bei der Beratung von verschiedenen auf dem Gebiet der genetischen Analyse tätigen Forschungseinrichtungen mit ein. Bundesweit wurde zusammengetragen, in welchem Umfang bereits Gendatenbanken bestehen oder im Entstehen begriffen sind, ob es Bestrebungen gibt, auf

[49] JB 2000, 4.5.1

Patientenchipkarten Gendiagnosen zu speichern, welche institutionellen Kontrollmöglichkeiten beim Umgang mit genetischen Daten bestehen, ob sichergestellt werden kann, dass anderweitig gewonnenes biologisches Material (z. B. Blutkonserven) nicht missbräuchlich verwendet wird, welchen Status Daten verstorbener Probenspender haben, inwieweit sich genetische Daten von anderen Gesundheitsdaten unterscheiden und welche Besonderheiten bei genetischen Reihenuntersuchungen bestehen würden.

Weitere Fragen waren:

Sollte ein einheitliches Gesetz zum Umgang mit genetischen Daten erlassen werden, ist eine Zertifizierung von genetischen Laboren sinnvoll und durchsetzbar? Welche Anforderungen sind an die Einwilligung von Probenspendern oder bei anderen genetischen Untersuchungen zu stellen? Und nicht zuletzt: Inwieweit lassen sich genetische Daten tatsächlich anonymisieren und welche Rolle könnte die Pseudonymisierung spielen?

Mit den Antworten wurde eine wesentliche Vorarbeit für die weitere Tätigkeit der Arbeitsgruppe geleistet. Schwerpunkt war dann, Anforderungen an ein Gesetz zur Sicherung der Selbstbestimmung bei genetischen Untersuchungen zu formulieren. Bis zur 62. Datenschutzkonferenz des Bundes und der Länder Ende Oktober 2001 gelang es, Vorschläge so zu unterbreiten, dass sie als Grundlage für einen Gesetzentwurf dienen können. Relativ schnell wurde zu folgenden Punkten Einigung erzielt:

Ein Gentestgesetz sollte Regelungen treffen über

- genetische Untersuchungen zu medizinischen Zwecken, im Zusammenhang mit Arbeits- und Versicherungsverhältnissen, zur Abstammungsklärung und Identifizierung außerhalb der Strafverfolgung und zu Forschungszwecken,
- die Aufnahme eines Benachteiligungsverbotes aufgrund von Erkenntnissen aus den Erbanlagen oder der Weigerung, eine genetische Untersuchung durchführen zu lassen,
- Begriffsbestimmungen,
- den Grundsatz der freiwilligen schriftlichen Einwilligung der betroffenen Person in genetische Untersuchungen, so sie nicht durch ein Gesetz oder die Strafprozessordnung geregelt sind,
- die Zulassung bzw. Zertifizierung von Stellen, die genetische Untersuchungen durchführen,
- die Beschränkung genetischer Tests auf Ärztinnen und Ärzte oder zertifizierte Labore und die damit verbundene Einschränkung der Berufsfreiheit,
- die Zweckbindung der für eine genetische Untersuchung entnommenen Probe an die Einwilligung und besondere Anforderungen an die Speicherung genetischer Daten,
- ein explizites Einsichts- und Auskunftsrecht der Betroffenen mit Verfahrensvorschriften.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Genetische Untersuchungen zu medizinischen Zwecken, so wurde vorgeschlagen, dürfen prädiktiv nur durchgeführt werden, wenn sie nach ärztlicher Indikation der Vorsorge, Behandlung oder der Familienplanung der betroffenen Person dienen. Pränatale Untersuchungen sind auf das Erkennen solcher Krankheiten zu richten, die vorgeburtlich behandelt werden können. Ob darüber hinaus auch schwere Behinderungen und Anlagen für schwere, nicht behandelbare Krankheiten Ziele pränataler DANN-Untersuchungen sein dürfen, muss der gesellschaftlichen Diskussion, der fachmedizinischen Bewertung und der Verantwortung des Gesetzgebers überlassen bleiben. Auch die genetischen Untersuchungen bei Minderjährigen und nicht einsichtsfähigen Erwachsenen müssen besonderen Restriktionen unterliegen. Genetische Reihenuntersuchungen sollten unter dem Vorbehalt der Zulassung der zuständigen Landesbehörde stehen. All diese Untersuchungen sollen außerdem unter einem Arztvorbehalt stehen. An Aufklärung und Beratung der betroffenen Person sind klare Vorgaben zu knüpfen. Ebenso an die Einwilligung. Die Unterrichtung über das Untersuchungsergebnis darf nur durch den veranlassenden Arzt erfolgen und muss mit einer Beratung über mögliche Folgen und Entscheidungsalternativen verbunden sein. Gegen den Willen des Betroffenen darf der Arzt Verwandte oder Partner nur dann von dem Untersuchungsergebnis unterrichten, soweit dies zur Wahrung erheblich überwiegender Interessen dieser Personen erforderlich ist.

Für genetische Untersuchungen im Zusammenhang mit Arbeits- und Versicherungsverhältnissen sollte es durch ein grundsätzliches Verbot verhindert werden, Gentests oder Testergebnisse zu fordern oder entgegenzunehmen. Wenn ein Arbeitsplatz trotz vorrangig durchzuführender Arbeitsschutzmaßnahmen mit einer erhöhten Erkrankungs- oder Unfallgefahr einhergeht, für die eine bestimmte Genstruktur von erheblicher Bedeutung ist, so soll der Bewerber darauf hingewiesen werden. Hinsichtlich geeigneter genetischer Untersuchungen sollte dann eine Beratung durch den Betriebsarzt erfolgen oder auf für die Untersuchung zugelassene Ärzte verwiesen werden.

Das generelle Verbot der Nutzung von Ergebnissen prädiktiver genetischer Untersuchungen für Versicherungsverhältnisse könnte dahingehend eingeschränkt werden, dass bei einer sehr hohen Leistungssumme die Versicherung berechtigt ist zu fragen, ob und wann eine prädiktive genetische Untersuchung durchgeführt wurde. Damit wird dem Versicherer bei arglistigem Schweigen die Möglichkeit der Kündigung gegeben.

Die Arbeitsgruppe hat vorgeschlagen, für genetische Untersuchungen zur Abstammungsklärung und zur Identifizierung außerhalb der Strafverfolgung festzulegen, dass die untersuchende Stelle die Proben bei der betroffenen Person selbst zu entnehmen und dies zu dokumentieren hat. Außerdem ist eine schriftliche Einwilligung der betroffenen Person oder eine gerichtliche oder behördliche Anordnung erforderlich. Damit

soll insbesondere die sich ausweitende Praxis unterbunden werden, Abstammungsuntersuchungen lediglich auf Grundlage eingesandter Proben vorzunehmen.

Die intensivsten Diskussionen wurden in der Arbeitsgruppe zu den Anforderungen an genetische Untersuchungen zu Forschungszwecken geführt. Dies liegt daran, dass dieser Punkt zum einen gegenwärtig noch nicht im Mittelpunkt der öffentlich geführten Diskussion steht und zum anderen auch international keine Vorbilder an gesetzlichen Vorschriften oder Regelungsentwürfen zu finden sind. Hier wird Neuland betreten. Aufgrund der nach der Beratung verschiedener Forschungsunternehmen in Berlin vorliegenden Erfahrungen übernahm unsere Behörde die Federführung für diesen Abschnitt. Ausgangspunkt bildete eine Stellungnahme zu Forschungsproblemen, die der Berliner Beauftragte für Datenschutz und Informationsfreiheit gegenüber der Enquetekommission des Bundestages „Recht und Ethik der modernen Medizin“ im April 2001 abgab.

Zur Lösung der anstehenden Probleme wurden zwei Fallkonstellationen unterschieden. Für konkrete und zeitlich befristete Forschungsvorhaben, bei denen eine Bindung der Nutzung der Proben und genetischen Daten auf dieses einzelne Vorhaben beschränkt ist und deren Vernichtung nach Abschluss des Forschungsvorhabens einschließlich der Frist zu Sicherung der Selbstkontrolle der Wissenschaft erfolgt, wurden erleichternde Bedingungen vorgeschlagen. So sollten Proben und genetische Daten für diese konkreten und befristeten Zwecke verarbeitet werden dürfen, wenn sie der betroffenen Person nicht mehr zugeordnet werden können oder die betroffene Person eingewilligt hat. Ausnahmsweise kann auf die Einwilligung verzichtet werden, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Interessen der betroffenen Person überwiegt und der Forschungszweck nicht auf andere Weise erreicht werden kann. Bei einer personenbeziehbaren Verarbeitung sind die Merkmale gesondert zu speichern, mit denen der Personenbezug hergestellt werden kann.

Im Unterschied zu konkreten und zeitlich befristeten Forschungsvorhaben sind jedoch die Anforderungen an Gendatenbanken, d. h. Sammlungen von Proben und genetischen Daten zu noch unbestimmten, allgemeinen Forschungszwecken anders zu sehen. Eine Aufnahme von Proben und Daten in eine solche Sammlung darf nur zulässig sein,

- wenn der Betroffene über Zweck und Nutzungsmöglichkeiten der Sammlung aufgeklärt wurde,
- wenn die Zuordnung der Probe und der genetischen Daten zur betroffenen Person vor Aufnahme in die Sammlung aufgehoben wurde und eine Pseudonymisierung durch eine Treuhänderregelung erfolgte,
- wenn der Träger der Sammlung eine kontinuierliche Datenschutzkontrolle auch beim Wechsel des Trägers sicherstellt.

Sowohl für konkrete und zeitlich befristete Forschungsvorhaben als auch für Gendatenbanken gilt, dass zuvor die Zustimmung durch die zuständige Ethikkommission einzuholen ist und bei Gendatenbanken eine Anzeige bei der für die Datenschutzkontrolle zuständigen Behörde erfolgt. Zur Sicherung der Rechte der Betroffenen einschließlich des Rechts auf Widerruf der Einwilligung und Vernichtung der Probe sowie der genetischen Daten wurden besondere Anforderungen formuliert. Um bei Gendatenbanken zu sichern, dass Informationen, die erst Jahre nach der Probenspende bei der Forschung anfallen und für die betroffene Person von Bedeutung sein können, diese auch erreichen, wurde vorgeschlagen, den Träger des Forschungsvorhabens durch die Nutzung des Treuhänderverfahrens zur Information der betroffenen Person zu verpflichten. Hat die betroffene Person nicht von ihrem Recht auf Nichtwissen Gebrauch gemacht, wird damit verhindert, dass die Forschungsergebnisse allein Dritten und nicht der betroffenen Person zugute kommen. Die Vorschläge schließen auch Sanktionen bei Verstößen ein. Da eine Nutzung genetischer Daten hinter dem Rücken der Betroffenen nicht ausgeschlossen werden kann, wurde es als erforderlich angesehen, dass zum Strafantrag auch die für die Datenschutzkontrolle zuständige Behörde berechtigt werden soll.

Wohlwissend, dass sich solche gesetzlichen Regelegungen auf Gegenstände beziehen, die erst in Zukunft breit zum Tragen kommen, wurde vorgeschlagen, das Gesetz zunächst auf zehn Jahre zu befristen und acht Jahre nach In-Kraft-Treten durch die für die Datenschutzkontrolle zuständigen Behörden einen Bericht über deren Wirksamkeit und neue Gefährdungen für das Persönlichkeitsrecht sowie mögliche Rechtsvereinfachungen vorzulegen. Diesem Bericht sollte auch eine Stellungnahme des Ethikrates und der Deutschen Forschungsgemeinschaft beigefügt werden.

Bereits im Sommer haben wir den damaligen Arbeitsstand mit mehreren Berliner Forschungsunternehmen, die Gendatenbanken aufbauen, diskutiert. Der Grundtenor der Stellungnahmen war nicht etwa wie zunächst befürchtet eine Kritik an Forschungsbeschränkungen oder Überregulierung durch den Staat, sondern der Wunsch dieser Unternehmen, ihre Tätigkeit in Rechtssicherheit und auf einer gesetzlichen Basis durchführen zu können. Hier zeigte sich, dass gerade in diesem Bereich eine schnell zu erreichende Rechtssicherheit durch ein Gentestgesetz als ein wirtschaftlicher Standortvorteil wahrgenommen wird.

3.3 Daten gegen Cash: Rabatt- und Bonussysteme

In den 50er und 60er Jahren war es in vielen deutschen Kaufhäusern und „Tante-Emma-Läden“ üblich, Stammkunden mit Rabattmarken zu belohnen und zu binden. Auch nach 1970 gab es noch einige wenige Kaufhäuser und Supermärkte, die das Sammeln von Rabattmarken anboten. Allerdings stellten Rabattmarken ab 1970 eher eine Rarität dar. Da Rabattmarken

nicht an bestimmte Personen gebunden waren, war „Omas Rabattmarkensystem“ datenschutzfreundlich.

In den letzten Jahren etablierte sich ein neues Rabattsystem: die Kundenkarte. Da Kundenkarten anders als Rabattmarken an eine bestimmte Person gebunden sind, muss der Emittent von Kundenkarten in einem gewissen Umfang personenbezogene Daten seiner Kunden speichern. Kundenkarten haben inzwischen in Deutschland große Verbreitung gefunden, sie sind nicht auf einzelne Branchen beschränkt. Besonders stark verbreitet sind Kundenkarten allerdings im Einzelhandel; viele Kaufhausketten, aber auch kleinere Bioläden bieten ihren Stammkunden über Kundenkarten Rabatte an. Fluggesellschaften und Bahnbetriebe versuchen, mit Vielflieger- bzw. Vielfahrerprogrammen ihre Stammkunden zu belohnen. Besonders hervorzuheben ist das von der LoyalTY Partner GmbH entwickelte Rabattsystem von Payback. Hier haben sich verschiedene Unternehmen unterschiedlichster Branchen (z. B. Realkauf, Kaufhof, DEA, Eurocar, Apollo Optik, FTI Touristik, Palmers, Sportarena, UfA-Theater etc.) zusammengeschlossen und bieten ihren Kunden nunmehr einen gemeinsamen Rabatt an. Dies hat für die Kunden den Vorteil, dass sie auch bei Unternehmen, bei denen sie keine Stammkunden sind, auf „Rabattjagd“ gehen können.

Die Vorteile, die Kunden mit Kundenkarten gewährt werden, beschränken sich nicht auf Preisnachlässe, häufig werden auch sonstige Anreize (Incentives) angeboten. Insofern kann man in vielen Fällen nicht mehr von einem Rabattsystem, sondern muss man von einem Bonussystem sprechen. So bieten einige Unternehmen ihren Kunden ab einem bestimmten ausgegebenen Geldbetrag Geschenke an, ein Kaufhaus ermöglichte es Kundenkarteninhabern (neben der Rabattierungsmöglichkeit), die Ware selbst einzuscannen und so Schlangen an der Einkaufskasse zu vermeiden. Außerdem werden den Kunden bessere Parkmöglichkeiten, die Benutzung des VIP-Raums und sonstige Sonderrechte angeboten. Bei der Lufthansa haben Vielflieger die Möglichkeit, bestimmte Ränge, wie etwa den des „Senators“ zu erhalten. Senatoren erhalten viele Sonderrechte, so sind sie etwa die ersten, die bei Spät- oder Umbuchungen noch freie Plätze erhalten.

Mit der Kundenkarte, die Rabatte und sonstige Incentives gewährt, verfolgen die jeweiligen Unternehmen mehrere Ziele. Eines der wichtigsten Ziele ist die Kundenbindung: Kunden sollen mit Hilfe der Kundenkarte zu Stammkunden werden. Auch ist beabsichtigt, dass Stammkunden einen besseren Service erhalten als jemand, der sich nur zufällig in ein bestimmtes Unternehmen „verlaufen hat“. Der Wegfall des Rabattgesetzes hat bei vielen Verbrauchern zu der Erwartung geführt, dass man durch gutes Verhandeln mit dem Verkäufer Vorteile erlangen kann. Die Kundenkarte gibt den Unternehmen die Möglichkeit, Kunden, die Preisnachlässe fordern, durch Verweis auf die Incentives der Kundenkarte zufrieden zu stellen. Nach Aussage von Verbraucherschützern sind die Preisvorteile, die Kun-

denkarten gewähren (in der Regel 3 %), für die Unternehmen nur von geringem Nachteil. Die „Preisvorteile“ werden teilweise schon bei der Preisbildung berücksichtigt, teilweise gleichen sich die Preisvorteile der Stammkunden dadurch aus, dass diese, durch die Kundenkarte verleitet, keine Preisvergleiche bei Konkurrenzunternehmen vornehmen und hierdurch im Schnitt genauso viel Geld ausgeben wie Verbraucher, die preiskritisch in verschiedenen Kaufhäusern einkaufen.

Das Rabatt- bzw. Bonussystem führt je nach Ausgestaltung dazu, dass die Unternehmen nicht nur durch die bei der Antragstellung auf eine Kundenkarte preisgegebenen Daten, sondern insbesondere durch die sonstigen im Rahmen des Rabattierungsverfahrens gespeicherten Daten umfangreiche Kundenprofile (bei Kunden von Verkehrsunternehmen kann man von Bewegungsprofilen sprechen) erhalten, die den Kundenkarteninhaber in vielen Fällen zu einem gläsernen Kunden machen. Soweit das Konsumverhalten der Kundenkarteninhaber bekannt ist, kann der Kunde entsprechend seinen Bedürfnissen von dem jeweiligen Unternehmen angesprochen werden, etwa um neue Produkte vorzustellen, die nach dem bisherigen Konsumverhalten für diesen besonders interessant sein könnten. Gerade bei Geschäften, bei denen im Falle eines Bargeldeinkaufs keinerlei Datenspuren der Kunden entstehen würden, ermöglichen es Rabattsysteme, das Kundenverhalten zu analysieren.

Obwohl immer mehr Kundenkarten emittiert werden und diese von den Verbrauchern auch in großem Umfang angenommen werden, gibt es doch viele Bürger, die gegen die Datensammelwut mit Hilfe von Rabatt- und Bonussystemen Bedenken äußern. Insbesondere gegen das Paybackverfahren der LoyalTY Partner GmbH sind bei verschiedenen Aufsichtsbehörden Beschwerden eingegangen. Besondere Aufmerksamkeit erregte, dass Payback für die Speicherung personenbezogener Daten zum Kaufverhalten von (inzwischen mehreren Millionen) Kunden und aufgrund des undurchsichtigen Umgangs mit den personenbezogenen Daten im Jahre 2000 den sogenannten Big Brother Award erhielt. In einem Urteil des Landgerichts München I[50] wurde festgestellt, dass das bis dahin praktizierte Verfahren von Payback wegen Verstoßes gegen das AGB-Gesetz rechtswidrig war. Bei der Datenspeicherung konnte sich Payback nicht auf die Einwilligung der Betroffenen berufen, da diese wegen Verstoßes gegen das AGB-Gesetz unwirksam war.

Nicht nur bei Payback, sondern auch bei anderen Kundenkarten wurden bei datenschutzrechtlichen Überprüfungen verschiedene Probleme festgestellt.

Bei dem Erwerb von Kundenkarten muss der Interessent ein Antragsformular (online oder offline) ausfüllen. Der hier entstehende Basisdatensatz des Kunden sollte nur personenbezogene Daten enthalten, die für die Teilnahme an dem Rabattsystem erforderlich sind (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Für vom Rabattsys-

[50] Urteil vom 1. Februar 2001, Az.: 12 O 13009/00

tem nicht benötigte Basisdaten, wie etwa E-Mail-Adresse, Telefon- und Mobilfunknummer etc., muss sich das Rabatt gewährende Unternehmen die Einwilligung des Betroffenen geben lassen.

Eine Datenverarbeitung, die sich ausschließlich an den für das Bonussystem erforderlichen Daten orientiert und diese Daten auch umgehend wieder löscht, wenn sie für das Bonussystem nicht mehr benötigt werden, bewegt sich im Rahmen der Zweckbestimmung des Vertragsverhältnisses und ist rechtmäßig. Die Frage, welche Daten wie lange aufgrund des „Rabattvertrages“ gespeichert werden dürfen, orientiert sich an den Modalitäten des Bonussystems. Da Rabatte sich an der Höhe des Umsatzes orientieren, können Umsatzdaten gespeichert werden. Da Umsatzleistungen der Kunden im Regelfall nur bis zu einem bestimmten Zeitraum eingelöst werden (bis zu diesem Zeitpunkt muss ein bestimmter Umsatz erzielt werden), sind Umsatzzahlen, die nicht mehr Berücksichtigung finden (allerdings auch die, die abschließend berücksichtigt wurden), zu löschen. Bei ausschließlich umsatzorientierten Rabattsystemen dürfen die jeweils gekaufte Ware bzw. die jeweils in Anspruch genommene Dienstleistung nicht gespeichert werden.

Da auch die ausschließlich umsatzorientierten Rabattkundenkartenemittenten von ihrem – gläsernen – Stammkunden wissen möchten, welche Produkte und Dienstleistungen er (wann) nachgefragt hat, versuchen die Unternehmen, die Rabatt wünschenden Kunden zu einer entsprechenden Einwilligungserklärung zu bewegen, die in dem Antragsformular enthalten ist.

Bei der rechtlichen Überprüfung der verwendeten Formulare bzw. der Einwilligungserklärungen wurden die verschiedensten Mängel festgestellt.

- Bei einem Formular war die Einwilligungserklärung, die zusammen mit dem Gesamtantrag abgegeben wurde, nicht besonders hervorgehoben und damit nach § 4 a Abs. 1 Satz 4 BDSG i. V. m. § 125 BGB unwirksam.
- Bei einem Online-Formular musste der Betroffene einen Button anklicken, wenn er die Speicherung der nicht für das Rabattsystem (sondern für Werbezwecke) erforderlichen Daten nicht wünscht. Dies reicht nicht aus, um eine wirksame Einwilligungserklärung zu bewirken. Ausreichen würde etwa ein Button mit der Angabe „Hier ankreuzen, wenn Sie einverstanden sind“.
- In einem Formular war den Kunden nicht die Möglichkeit eingeräumt worden, der Datenverarbeitung für Werbe- und Marketingzwecke zu widersprechen. Das Kaufhaus wollte nur demjenigen einen Rabatt einräumen, der sich auch bewerben lassen wollte. Das nach § 28 Abs. 4 Satz 1 BDSG bestehende Widerspruchsrecht des Betroffenen gegen Werbung oder Markt- und Meinungsforschung ist unabdingbar und darf dem Betroffenen nicht verwehrt werden.

- Das Werbeverbot muss bei dem Rabatt gewährenden Unternehmen auch zu Konsequenzen bezüglich des Umfangs der gespeicherten Daten führen. Daten über Kaufgegenstände und Dienstleistungen, die nur zu Werbezwecken benötigt werden, sind bei den Kunden, die ein Werbeverbot ausgesprochen haben, zu löschen. Da dies mit erheblichem Verwaltungsaufwand verbunden ist, behalten einige Unternehmen bei den Personen, die keine Einwilligung gegeben haben, den gleichen Datensatz vor. Dies ist rechtswidrig.
- Bei Online-Formularen haben wir darauf hingewiesen, dass es erforderlich ist, dass der Einwilligungsbutton erst dann angeklickt werden kann, wenn der Betroffene vorab die Information zum Datenschutz aufgerufen hat.
- Der Inhalt der Erklärung sowie die Erläuterung zum Datenschutz müssen so konkretisiert sein, dass von einer informierten Einwilligung ausgegangen werden kann. Der bloße Hinweis, dass Daten für Marketingzwecke verwendet werden, hat wenig Aussagewert, da Marketingverfahren auch nicht personenbezogen möglich sind. Häufig beabsichtigen die Unternehmen, mit den Kundendaten ein Data-Warehouse aufzubauen und Data-Mining-Verfahren anzuwenden. Über die dabei auftretenden Probleme sowie die Problematik einer Einwilligungserklärung für Data-Warehouse-Data-Mining-Verfahren hatten wir im Jahresbericht 2000[51] hingewiesen.

3.4 Telemedizin

Wer sich in ärztliche Behandlung begeben muss, wird je nach Art und Schwere der Erkrankung seinem Arzt alles über seine Beschwerden, vielleicht auch über Lebensweise, Gewohnheiten, frühere Krankheiten, Sorgen und manches mehr sagen müssen, wenn dieser ihm helfen soll. Hinzu kommen mit den Untersuchungsergebnissen des Arztes zusätzliche Daten, die dieser originär beim Patienten erhebt. Die Bereitschaft des Patienten, seine – möglicherweise auch unangenehmen, peinlichen oder ihn gegenüber Dritten diskriminierenden – Geheimnisse preiszugeben, setzt ein großes Vertrauen in den Arzt voraus, dass dieser die erlangten Kenntnisse als Geheimnis bewahrt und nicht missbräuchlich verwendet. Die Wahrung der ärztlichen Schweigepflicht ist seit der Antike als humane Verpflichtung der Arztes und als Voraussetzung für das Vertrauensverhältnis zwischen Arzt und Patient bekannt. Heute ist der Bruch der ärztlichen Schweigepflicht nach § 203 Strafgesetzbuch strafbewehrt und die Berufsordnungen der Ärztekammern regeln dieses besondere Berufsgeheimnis näher.

Die meisten modernen niedergelassenen Ärzte kommen nicht ohne Helfer aus, die zumindest zum Teil von den Geheimnissen der Patienten erfahren. Diese notwendige Öffnung der ärztlichen Schweigepflicht führt dazu, dass sie sich auf die „ärztlichen Erfüllungsgehilfen“, die unter Aufsicht des Arztes tätig sind, erweitert.

Die Bedeutung der Telemedizin ist in den letzten fünf Jahren sprunghaft angestiegen, dies sieht man u.a. an der nicht mehr überschaubaren Flut von Publikationen und einer großen Zahl von Kongressen zu dieser Thematik. Die Projekte reichen von der elektronischen Patientenakte über globale Systeme zum Erhalt einer sogenannten „second opinion“ bis zur telemedizinisch gesteuerten Hirnoperation.

Die Anwendungsgebiete sind mittlerweile so vielfältig, dass sie praktisch die gesamte Medizin erfassen und die dabei auftretenden Probleme in Bezug auf den Datenschutz kaum noch zu beschreiben sind.

Erschwert wird diese Situation dadurch, dass die seitens des Gesetzgebers und der Krankenkassen geforderte stark vermehrte Dokumentationspflicht den Einsatz EDV-gestützter telemedizinischer Systeme geradezu zwingend erfordert. Im Bereich der Charité finden zahlreiche telemedizinische Projekte statt, die teils wissenschaftlich orientiert, teils schon in der Routine eingesetzt werden. Der Datenschutz ist hier u. a. dadurch gewahrt, dass sich der Datenaustausch innerhalb der „fire wall“ der Charité abspielt, und somit der Zugriff auf diese Daten durch externe Pesonen kaum möglich ist. Auch werden die Daten, soweit möglich, in anonymisierter Weise oder kryptisch verschlüsselt übertragen.

[51] JB 2000, 4.6.3

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Die Spezialisierung der Ärzte führt zu weiteren Öffnungen, weil häufig weitere Ärzte in die Behandlung eines Patienten eingebunden werden müssen. Dies muss mit der Zustimmung der Patienten erfolgen.

Ein wichtiges Problem ist tatsächlich die Vernetzung mit niedergelassenen Arztpraxen und mit anderen Krankenhäusern. Die Übertragung personenbezogener Daten, einschließlich der Unterlagen aus bildgebender Diagnostik, ist für den Patienten äußerst hilfreich, beschleunigt den Behandlungsprozess und verbessert die Kommunikation zwischen den Ärzten. Die dabei auftretenden datenschutzrechtlichen Probleme werden derzeit dahingehend gelöst, dass der Patient über die Vorgänge informiert wird. Aus Sicht der Charité ist es notwendig, hier grundsätzlich rechtliche Regelungen zu treffen, damit das Risiko nicht beim einzelnen Arzt bzw. beim Krankenhausträger verbleibt. Die dahingehenden Aktivitäten der Deutschen Gesellschaft für Medizinrecht sind in diesem Zusammenhang hilfreich und sollten bei der Ausgestaltung gesetzlicher Regelungen einbezogen werden.

In den Krankenhäusern geht die Arbeitsteilung zwangsläufig noch weiter als in Praxen der niedergelassenen Ärzte. Hier erfahren wesentlich mehr Personen von den Geheimnissen der Patienten: Es gibt nicht nur den behandelnden Arzt, sondern mehrere, teils wegen der Schichtwechsel, teils wegen der notwendigen Einbindung anderer Spezialisten. Der Kreis der ärztlichen Erfüllungsgehilfen ist ebenfalls groß und vielfältig: Er reicht vom Pflegepersonal bis hin zu den Datenverarbeitungsspezialisten, die die informationstechnischen Systeme in den Krankenhäusern betreuen. Wo hier von den Regeln der ärztlichen Schweigepflicht die Grenzen gezogen werden, ist umstritten. Zwei Grundsätze sind aber zu beachten: Der Grundsatz der Erforderlichkeit, der besagt, dass von den Geheimnissen des Patienten nur diejenigen erfahren dürfen, für die das Wissen für die Behandlung des einzelnen Patienten erforderlich ist, und auch nur in dem Umfang, in dem es erforderlich ist, und der Grundsatz der Datensparsamkeit, der besagt, dass dort, wo es möglich ist, mit anonymen, pseudonymen, aggregierten oder verschlüsselten Daten zu arbeiten, dies auch getan werden soll.
Über die Probleme, die sich hier in der Praxis der Krankenhausinformationssysteme ergeben, haben wir im Vorjahr ausführlich berichtet[52].

Eine weitere Herausforderung für die Verfechter der ärztlichen Schweigepflicht und des Datenschutzes im Krankenhaus wird die *Telemedizin* mit sich bringen. Sie wird in verschiedensten Zielsetzungen und Anwendungsformen praktiziert, meist aber erst konzipiert oder erprobt.

Eine der bisher ausgereiftesten telemedizinischen Anwendungen ist das Projekt *QuaSi-Niere*, das von der Ärztekammer Berlin initialisiert wurde und jetzt von der QuaSi-Niere gGmbH in Berlin durchgeführt wird[53]. Zielsetzung dieses Projektes ist die Qualitätssicherung bei der Nierenersatztherapie und betrifft sowohl die Dialyse als auch die Nierentransplantation. Seit 1996

[52] JB 2000, 3.3
[53] JB 1995, 5.14; 1996, 4.5.1; 1997, 4.4.2; 1998, 4.5.1; 2000, 4.5.1

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

sind die Daten von 50.000 Dialysepatienten und 15.000 Patienten in der Transplantationsnachsorge zusammengeführt worden, um regionale Besonderheiten, Patiententwicklung und Morbidität, Alters- und Diagnosenverteilungen, stationäre Verweildauern und manche andere relevante Daten für die Qualitätssicherung zu erhalten.

Die Teilnahme an dem Projekt ist für die Patienten freiwillig. Nach ihrer Einwilligung wird ihnen eine Patienten-Chipkarte ausgestellt, mit der sie sich gegenüber jedem Arzt oder sonstigem Leistungserbringer als Teilnehmer an dem Projekt authentifizieren können. Die Leistungserbringer, die an dem Projekt teilnehmen, verfügen über eine Health Professional Card (HPC), mit der sie die Angaben über Patienten und behandelnde Institutionen für die Übertragung per Internet elektronisch signieren und verschlüsseln. Empfänger der Daten ist ein Notar als Datentreuhänder (Vertrauensstelle), der über eine HPC zur Entschlüsselung und Signaturprüfung verfügt. Der Datentreuhänder pseudonymisiert die Daten und leitet sie an die auswertende Stelle weiter.

In der Planung ist die Modernisierung des Meldewesens der *Tumorzentren*, stationär und ambulant tätiger Ärzte sowie bestimmter Gesundheitsämter an das *Gemeinsame Krebsregister* der ostdeutschen Bundesländer mit Sitz in Berlin (GKR). Die Vertrauensstelle des GKR nimmt auf der Grundlage des Krebsregistergesetzes und des Staatsvertrages über das Gemeinsame Krebsregister Meldungen über Krebsneuerkrankungen und Leichenschauscheine entgegen. Diese Meldungen sollen in Zukunft per E-Mail möglich sein. Grundsätzlich ist gegen diese Vorgehensweise nichts einzuwenden, wenn die Daten sicher verschlüsselt übertragen und vom Absender digital signiert werden. Ansonsten ist die Vorgehensweise bei diesem Meldewesen gesetzlich verankert.

Die Auffassungen des Berliner Beauftragten für Datenschutz und Informationsfreiheit zur Vorgehensweise der Datenübersendung per E-Mail werden geteilt. Folgende Festlegungen wurden für die Realisierung einer Datenübertragung zwischen Meldenden und dem GKR getroffen:

- Daten müssen sowohl verschlüsselt als auch digital signiert übertragen werden.
- Einführung einer PKI (Public Key Infrastructur) zwischen den Partnern.
- Es ist aus Sicherheitsgründen erforderlich, die geheimen Schlüssel auf Sicherheitschipkarten abzulegen. Diese Karte einschließlich des Schlüsselpaares ist durch eine akkreditierte Zertifizierungsstelle zu realisieren.

Zur Zeit wird das Angebot einer akkreditierten Zertifizierungsstelle im GKR geprüft und bewertet.
Diese Stelle realisiert als Herausgeber der Health Professional Card (Arztausweis) für das Bundesland Sachsen und als ein auf das Gesundheitswesen spezialisierter Dienstleister für elektronische Signaturen die Lieferung der rechtssicheren elektronischen Identität (PKI) und der Signaturkarte als rechtssicheren Ausweis.
Die Einführung der PKI ist in der ersten Stufe für den Datentransfer zwischen den Tumorzentren/Klinischen Krebsregistern und dem GKR im 3. Quartal 2002 geplant.

Dies gilt nicht für viele andere telemedizinische Projekte, die zu Zwecken epidemiologischer Forschung oder zur Optimierung der Informationsflüsse bei der Behandlung von Patienten begonnen worden sind:

Aus der Charité wurden wir um Beratung zu einer geplanten Pilotstudie *OncoCard.de* für eine Tumorverlaufsdokumentation gebeten. Nach der histologischen Sicherung der Tumorerkrankung erhält der Pati-

ent eine Chipkarte, die er bei jeder weiteren Behandlung seiner Erkrankung zur Dokumentation seiner Zustimmung vorlegt und die seiner Authentifizierung, der Pseudonymisierung und in Verbindung mit der HPC eines Arztes dem Aufbau einer sicheren Verbindung zum zentralen Datenbankserver bei der Deutschen Krebsgesellschaft in Frankfurt/Main dient. Die pseudonymisierten Daten sind passwortgeschützt über das Internet zu erreichen und enthalten zu sieben verschiedenen Sachverhalten nur drei verschiedene Werte, die durch eine grüne, gelbe oder rote Markierung dargestellt werden. Jeder Arzt, der an dem Verfahren teilnimmt und der den Patienten untersucht und behandelt, ergänzt die Verlaufsdokumentation um den jeweils neuen Status. Das Verfahren soll mit besten technischen Sicherheitsmaßnahmen ausgestattet werden, um die Sicherheit der Daten bei ihrer Übertragung, die Sicherung der angeschlossenen Systeme und die Anonymität der Patienten umfassend zu gewährleisten. Die Beratung in diesem Projekt ist noch nicht abgeschlossen.

Offensichtlich besteht ein erheblicher Bedarf an der *Vernetzung niedergelassener Arztpraxen mit Krankenhäusern*, denn wir sind dazu bereits einige Male in Berlin um Rat gefragt worden. Dabei geht es um den Informationsaustausch zwischen dem einweisenden niedergelassenen Arzt und dem Krankenhaus (Arztbriefe) sowie nach dem Krankenhausaufenthalt um den Zugriff des nachsorgenden Arztes auf die Daten des Krankenhauses. Wegen des unmittelbaren Zusammenhangs mit der Behandlung des Patienten sind grundsätzliche Bedenken bei solchen Projekten nicht angebracht. Jedoch ergeben sich aus den Sicherheitsanforderungen, die bei einer solchen Kommunikation zu stellen sind, häufig zunächst nicht in Betracht gezogene Aufwände, die zum Überdenken solcher Projekte führen: Die Datenübertragung muss in beiden Richtungen verschlüsselt und signiert erfolgen, die angeschlossenen Systeme müssen wegen der erforderlichen Netzöffnung gegen unbefugte Angriffe aus dem Netz geschützt werden und der Zugriff auf die Patientendaten muss durch technische Maßnahmen auf die jeweils betroffenen Patienten beschränkt werden.

Derzeit ist auf Bundesebene das Projekt zur Einführung eines *Elektronischen Patienten-Ausweises (EPA)* auf freiwilliger Basis im Gespräch. Eine Präsentation gegenüber dem Bundesbeauftragten für den Datenschutz und ein Workshop dazu wurden am Ende des Berichtsjahres durchgeführt. Der EPA wird als Teil der Gesundheitsreform angesehen und soll der Erschließung zentral gespeicherter Patientendaten für Haus- und Fachärzte, Krankenhäuser, Pflegedienste, Rehabilitationseinrichtungen, Apotheken, Kassenärztliche Vereinigungen, Krankenkassen und qualitätssichernde Institutionen dienen. Dabei soll der Patient steuern können, wer seine Daten in welchem Umfang erhält. Die Diskussion um dieses Projekt steht erst am Anfang.

Aus anderen Bundesländern ist eine Vielzahl weiterer telemedizinischer Projekte mit unterschiedlichen Ziel-

setzungen bekannt. Es geht meist um epidemiologische Fragestellungen, um die Datenkommunikation zwischen Leistungserbringern im Zusammenhang mit der Behandlung eines Patienten, um Qualitätssicherung, um die Führung von elektronischen Patientenakten, die dem Zugriff verschiedener Stellen unterliegen sollen, sowie um die Beiziehung zusätzlichen Sachverstandes bei der Behandlung von Patienten. In vielen Fällen leiden die Projekte an dem Umstand, dass nicht alle Beteiligten, meist Patienten oder Ärzte, das nötige Interesse aufbringen, um solche Pilotprojekte voranzubringen. Als Erfolgskriterien für solche Projekte dürften folgende Merkmale dienen, die z. B. für das oben beschriebene Projekt Quasi-Niere zutreffen:

Der Anwendungsbereich des telemedizinischen Projekts sollte eingeschränkt und genau spezifiziert sein, da anders der Sinn des Projekts und der Nutzen für den einzelnen Beteiligten nicht erkennbar sind. Das Projekt sollte sich an chronisch Erkrankte richten, denen klargemacht werden kann, welchen Nutzen sie davon haben. Telemedizinische Projekte, die sich auch an im Allgemeinen Gesunde richten, dürften nicht die notwendige breite Akzeptanz finden. Das Projekt sollte sich hinsichtlich der zu erreichenden Ziele selbst beschränken und nicht gleich alles auf einmal realisieren wollen, da es sonst wegen seiner Komplexität unbeherrschbar werden kann. Daraus folgt, dass das Konzept hinreichend einfach sein sollte und weitere Projektziele sukzessive angegangen werden, wenn die bisherigen Projektziele ihre Praxistauglichkeit erwiesen haben.

Wenn man dies beachtet, werden auch die datenschutzrechtlichen und technisch-organisatorischen Anforderungen umsetzbar und beherrschbar sein. Dafür gelten folgende Regeln:

- Die Teilnahme der Patienten muss freiwillig und im Einzelfall in Bezug auf Umfang und Intensität selbstbestimmt sein. Gesetzliche Verpflichtungen sind nur dann akzeptabel, wenn dies in einem überwiegenden Interesse der Allgemeinheit ist, wenn also akute Gefahren für die Gesundheit der Menschen vorliegen, sofern man sich auf freiwilliges Verhalten verlassen würde (z. B. Meldepflichten bei schweren ansteckenden Krankheiten).
- Solange es nicht um die konkrete Behandlung eines Patienten geht, sondern nur um Datengewinnung für epidemiologische, gesundheitsstatistische oder qualitätssichernde Maßnahmen, müssen die Daten anonymisiert werden. Sie sind zu pseudonymisieren, wenn es notwendig ist, im Laufe längerer Zeiträume Daten immer wieder bestimmten Patienten zuzuordnen. Dies kann durch Datentreuhänder geschehen oder mit kryptographischen Pseudonymisierungsverfahren.
- Bei der Übertragung von personenbezogenen Daten über öffentliche Datenübertragungswege sind die Daten mit starken kryptographischen Verfahren zu verschlüsseln, damit Unbefugte sie nicht lesen kön-

nen, und digital zu signieren, damit der Empfänger weiß, wer ihm die medizinischen Daten geschickt hat, und er damit ihre Relevanz einschätzen kann.

- Bei der Verwendung von Chipkarten sind die „Anforderungen zur informationstechnischen Sicherheit bei Chipkarten“ zu beachten.
- Die an öffentliche Netze angeschlossenen Systeme für die Durchführung telemedizinischer Verfahren sind gegen Angriffe auf dem öffentlichen Netz (z. B. Internet) zu schützen (Einsatz von Firewall-Systemen, Isolierung der Systeme gegenüber den lokalen Netzen in Krankenhäusern und Arztpraxen).

Wenn all dieses berücksichtigt wird, also konsequent Datenschutz durch Technik[54] sichergestellt wird, kann das eingangs beschworene Vertrauensverhältnis zwischen Arzt und Patient auch in die Informationsgesellschaft hinübergerettet werden.

3.5 Das Berliner Projekt Bürgerdienste (ProBüd)

Bereits Ende der 70er Jahre wurde im Westen Berlins damit begonnen, in fast allen Bezirken Bürgerberatungsstellen einzurichten. Nach der Wiedervereinigung der beiden Stadthälften wurden auch im Osten derartige Anlaufstellen für Rat suchende Bürger etabliert. Im Juni 1991 verabschiedete das Abgeordnetenhaus von Berlin einen Beschluss, mit dem die Schaffung einer einheitlichen, bürgernahen und effizienten Verwaltung für das wiedervereinigte Berlin gefordert wurde. Zur Umsetzung dieser Forderung wurde das Infrastrukturprojekt „Modellbezirksamt“ initiiert. Im Ergebnis eines Auswahlverfahrens wurde das Bezirksamt Weißensee dazu auserkoren, hinsichtlich seiner organisatorischen Strukturen, seiner technischen Ausstattung und einem daraus erwachsenden bürgerfreundlichen Dienstleistungsangebot als Vorreiter für ganz Berlin zu fungieren. Im Juli 1993 wurde als zentral gelegenes Kernstück des Modellbezirksamtes das Bürgerbüro in der Berliner Straße eröffnet[55]. Unter Nutzung der in Weißensee gewonnenen Erfahrungen konnte im Oktober 1994 ein weiteres Bürgerbüro im Rathaus des Bezirkes Köpenick seine Türen für Rat suchende Bürger öffnen. Bis Ende 1999 entstanden dann in 11 Bezirken 23 Bürgerämter/-büros unterschiedlicher Ausprägung.

Aus datenschutzrechtlicher Sicht wurde mit der Schaffung dieser Einrichtungen Neuland betreten. Wurden hier doch mannigfaltige Verwaltungsaufgaben, die zuvor ausschließlich durch die jeweils zuständigen Fachämter wahrgenommen wurden, nicht nur unter einem Dach vereint. Im Zuge einer durchaus gewünschten Allzuständigkeit der Mitarbeiterinnen und Mitarbeiter waren Interessenkollisionen hinsichtlich der in Beratungsgesprächen offenbarten personenbezogenen Daten aus den unterschiedlichsten Lebensbereichen kaum zu vermeiden[56]. Demzufolge war der Um-

[54] JB 1997, 2.2
[55] JB 1993, 2.1
[56] JB 1994, 3.4

gang mit derart vielfältigen personenbezogenen Daten in normenklaren, d. h. die jeweilige Rechtslage berücksichtigenden Geschäftsanweisungen zu regeln[57].

Mit der Verabschiedung des 3. Gesetzes zur Reform der Berliner Verwaltung (Verwaltungsreform-Grundsätze-Gesetz – VGG) im Mai 1999 wurde auch das Bezirksverwaltungsgesetz (BezVG) dahingehend geändert, dass nunmehr die Einrichtung von Bürgerämtern spätestens bis zum 1. Januar 2001 in allen Berliner Bezirken zur gesetzlichen Aufgabe wurde. In § 3 Abs. 5 VGG (Bürgerorientierung) wurden die Bürgerämter der Bezirke zudem zur Erbringung übergreifender bürgerorientierter Leistungen probehalber zur Wahrnehmung von Aufgaben des Landeseinwohneramtes (LEA) ermächtigt. Dies sollte unabhängig von ihrer örtlichen Zuständigkeit ermöglicht werden können. Gleichzeitig sollten im Rahmen dieser so genannten „Experimentierklausel“ Mitarbeiter des LEA in den Bürgerämtern auch einzelne – allerdings nicht näher bezeichnete – bezirkliche Aufgaben wahrnehmen können. Um die Entwicklung von Bürgerämtern mit integrierten Meldestellen und einer „verzahnten“ Aufgabenwahrnehmung auch finanziell zu unterstützen, wurden Vereinbarungen zwischen der Senatsverwaltung für Inneres und den jeweiligen Bezirksämtern abgeschlossen. Die dort vereinbarte Anschubfinanzierung wurde an die Einhaltung bestimmter Voraussetzungen geknüpft, in deren Mittelpunkt ein gemeinsamer Bezirksamtsbeschluss über die Wahrnehmung des vom – zwischenzeitlich installierten – Arbeitskreis Bürgerservice definierten Standard-Aufgabenkatalogs als ständig vorzuhaltendes Grundangebot des Bürgeramtes steht. Als weitere Kriterien werden neben der Gewährleistung von Mindestöffnungszeiten die Realisierung von Bürgerämtern mit Meldestellen an gemeinsamen Standorten und eine integrierte (verzahnte) Aufgabenwahrnehmung von bezirklichen und Meldestellenaufgaben auf der Basis der Experimentierklausel festgeschrieben.

Die Dauer der Erprobungsregelung wurde in § 3 Abs. 5 VGG bis zum Ablauf des Jahres 2001 begrenzt. Mit dem Gesetz zur Neuregelung der Zuständigkeit des Landeseinwohneramtes Berlin[58] wurde der Erprobungszeitraum hinsichtlich der Wahrnehmung von bis dahin anderen Zuständigkeiten obliegenden Aufgaben nicht ausgeschöpft. Mit diesem Artikelgesetz wurde in Artikel I die Anlage zum Allgemeinen Sicherheits- und Ordnungsgesetz (ASOG), die den Zuständigkeitskatalog Ordnungsaufgaben (ZustKatOrd) beinhaltet, dahingehend verändert, dass mit der eingefügten Nr. 22a den Bezirksämtern Ordnungsaufgaben des Melde-, Pass- und Personalausweiswesens sowie Aufgaben der Ausländerbehörde und mit Nr. 22b Ordnungsaufgaben aus dem Gebiet des Verkehrswesens zugewiesen wurden. Dabei beauftragen sich – je nach Ausgangslage – die Bezirksämter und das LEA gegenseitig mit der Aufgabenwahrnehmung in den Einzelfällen, in denen beim

[57] JB 1995, 3.6
[58] GVBl. 2000, S. 515

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

LEA bzw. bei den Bezirksämtern der Anlass für die Amtshandlung entsteht.

Mit diesen Gesetzesänderungen wurden die rechtlichen Rahmenbedingungen geschaffen, um die Bürgerämter auch langfristig in die Lage zu versetzen, die ihnen gestellten Aufgaben zum Erbringen übergreifender bürgerorientierter Leistungen zu erfüllen. Der aus Vertretern zahlreicher Bezirksämter, des LEA und der Projektgruppe BürgerDienste der Innenverwaltung gebildete Arbeitskreis Bürgerservice hat einen Standardaufgabenkatalog erarbeitet, der sich vom herkömmlichen Verrichtungsprinzip der öffentlichen Verwaltung löst, sich vorrangig an den Lebenslagen der Bürger orientiert und daher Aufgaben aus den unterschiedlichsten Verwaltungsbereichen integriert. Ziel dieser Vorgaben ist es letztlich, den Bürgern die Dienstleistungen der Verwaltung bei solchen alltäglichen Prozeduren, wie sie beispielsweise bei einem Umzug oder einer Pkw-Anmeldung zu absolvieren sind, aus einer Hand anzubieten, um die damit normalerweise verbundenen Behördengänge auf ein Minimum zu reduzieren.

Die genannte Zusammensetzung galt für den Arbeitskreis Bürger**service.** Am 22.11.2000 hat sich der Arbeitskreis Bürger**ämter** konstituiert. Dieser besteht aus Vertretern aller 12 Bezirke, wird durch einen Vertreter des LEA und für den Bereich Qualifizierung durch eine Vertreterin der Verwaltungsakademie Berlin begleitet, sowie von Mitarbeiter/inne/n der Projektgruppe Bürgerdienste moderiert und unterstützt.
Das Ziel, dem Bürger möglichst umfassend Dienstleistungen „aus einer Hand“ anzubieten, ist richtig benannt, die PKW-Anmeldung wird jedoch (zur Zeit) nicht im Bürgeramt durchgeführt, möglich ist hier die Änderung der Anschrift in den Fahrzeugpapieren nach erfolgter Ummeldung des Bürgers.

Für viele der in den Standardaufgabenkatalog aufgenommenen Dienstleistungen existieren bereits in den jeweiligen Fachämtern automatisierte Verfahren, die sich jedoch dadurch „auszeichnen“, dass sie bei der Fokussierung auf eine verfahrensübergreifende Nutzung durch die Bürgerämter die heterogene Berliner IT-Landschaft nachdrücklich widerspiegeln. Diese Verfahren basieren entwicklungsbedingt auf den unterschiedlichsten Plattformen hinsichtlich der eingesetzten Hard- und Software. Die integrierte Nutzung dieser Verfahren erfordert neben der Qualifizierung der Bürgeramtsmitarbeiter für eine fachübergreifende Sachbearbeitung demgemäß auch eine entsprechende technische und organisatorische Unterstützung zur Bewältigung der gestellten Aufgaben. Daher soll aufbauend auf der *Ve*reinheitlichung bzw. *Zu*sammenführung der verschiedenen *Da*tenstrukturen in der Berliner Verwaltung (Projekt VeZuDa) eine Anwendungsumgebung geschaffen werden, die einerseits die Effizienz in den Bürgerämtern erhöht und andererseits auch die datenschutzrechtlichen Belange berücksichtigt. Dieses Vorhaben firmiert unter dem Kürzel „TeBa“ (Technikunterstützter einheitlicher Bürgeramtsarbeitsplatz).

Dabei stellt sich über die rechtliche Zulässigkeit der verfahrensübergreifenden Datenverarbeitung durch die Bürgerämter hinaus insbesondere die Frage, wie mit geeigneten technischen und organisatorischen Maßnahmen sichergestellt werden kann, dass den Forderungen von § 5 BlnDSG zur Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten sowie zur Revisionsfähigkeit der Datenverarbeitung genügt werden kann. Wir haben der Projektgruppe empfohlen, den TeBa möglichst so zu gestalten, dass mit einer einmaligen Authentifikation nach dem Single-Sign-On-Prinzip und einer damit verknüpften Rechtematrix den genannten Forderungen entsprochen werden kann. Gerade durch die Einbindung verschiedener automati-

ProBüD realisiert in einem mehrstufigen Vorgehen die informationstechnische Unterstützung für die Bürgerdienste. Diese Maßnahmen stehen auch im Kontext der E-Government-Entwicklungen des Landes Berlin. Die erste Realisierungsstufe ist durch die Bereitstellung des (Start-) Infosystems abgeschlossen. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit war wie im Jahresbericht dargestellt eng an der Erarbeitung des Sicherheitskonzeptes beteiligt. Es liegt seit Ende des ersten Quartals 2002 eine freigegebene Version für den Echtbetrieb vor, die das Konzept aus der Probebetriebsphase fortschreibt. Die Hinweise und Anregungen des BlnBDI wurden durch ProBüD in allen Projektphasen aufgegriffen. Selbstverständlich werden auch in

sierter Fachverfahren ist das Risiko einer missbräuchlichen bzw. fehlerhaften Datenverarbeitung besonders hoch. Aus unserer Sicht kann diesen Risiken nur wirksam begegnet werden, wenn in diesem Teilprojekt eine sorgfältige Analyse durchgeführt wird und diese in ein umfassendes verfahrensspezifisches Sicherheitskonzept mündet. Zwar ist die Erstellung dieses Sicherheitskonzeptes mit einem hohen Aufwand verbunden, sie ist aber eine zwingende Voraussetzung für das Gelingen des Gesamtprojektes ProBüd.

Während uns dieses Sicherheitskonzept im Berichtszeitraum noch nicht zur Stellungnahme vorgelegt wurde, waren wir mit einem anderen Projektteil, dem Startsystem für den Querschnittsdienst „IT-gestütztes Informationssystem“, kurz Start-Infosystem, bereits befasst. Diese wesentliche Komponente des TeBa dient der Schaffung einer Informationsplattform zur Unterstützung der so genannten Front-Office-Arbeitsplätze in den Bürgerämtern sowie der Einbindung und Ergänzung der bereits bestehenden interaktiven Informationsangebote des Stadtinformationssystems der Senatskanzlei. Ausgehend von den Erfahrungen, die mit einem Pilotprojekt im Bezirksamt Köpenick gewonnen werden konnten, wurde die kurzfristige Schaffung eines Start-Infosystems initiiert, dass noch nicht den vollen Leistungsumfang des geplanten Zielsystems umfasst. In Zusammenarbeit zwischen dem Auftragnehmerkonsortium, Vertretern der Projektgruppe ProBüd als Auftraggeber, der Bezirke, des LEA, des Landesbetriebs für Informationstechnik (LIT), der Senatskanzlei und unserer Behörde konnte zum Jahresende 2001 ein – zunächst auf den Probebetrieb zielendes – abgestimmtes Sicherheitskonzept erarbeitet werden. Das für den Echtbetrieb, der auch einen Internetzugang zu diesem Infosystem ermöglichen soll, zu erweiternde verfahrensspezifische Sicherheitskonzept lag allerdings im Berichtszeitraum noch nicht vor.

3.6 Sicherheit im Berliner Landesnetz

Die Berliner Verwaltung betreibt seit einigen Jahren das Berliner Landesnetz für die Daten- und Sprachkommunikation innerhalb der Verwaltung. Wir haben uns wiederholt mit Datenschutz- und Sicherheitsfragen im Zusammenhang mit der Datenkommunikation auf diesem Netz beschäftigt. Dies geschah nicht, weil diesen Fragen ansonsten nicht die notwendige Aufmerksamkeit geschenkt wurde, sondern weil die Umsetzung des Sicherheitskonzepts für das Landesnetz (in der Organisations- und Sicherheitsrichtlinie des Landes als Zentrale Infrastruktur bezeichnet) gravierende Auswirkungen auf die Sicherheitskonzepte der angeschlossenen Behörden hat. Die IT-Sicherheitsrichtlinie des Landes[59] zielt folgerichtig auch schwerpunktmäßig auf die Sicherheit der Zentralen Infrastruktur, für die der Landesbetrieb für Informationstechnik als Zentraler Infrastrukturbetreiber verantwortlich ist.

Grob betrachtet betrifft die Sicherheit des Berliner Landesnetzes drei Problembereiche: die Sicherstellung

den folgenden Realisierungsstufen des Gesamtvorhabens („integriertes Infosystem“ für alle Vertriebswege und „TeBa“) die Problemstellung IT-Sicherheit eingehend zu behandeln und die erforderlichen Sicherheitskonzepte zu erstellen sein. Derzeit sind die Folgeaktivitäten allerdings noch im Planungsstadium, so dass ein Sicherheitskonzept für den „TeBa“ selbst noch nicht vorliegen kann. Das auch vom BlnBDI empfohlene Single-Sign-On-Prinzip ist für das (Start-) Infosystem durch die beabsichtigte frühzeitige Integration auf die VeZuDa-Plattform (die u.a. die SSO-Funktionalität anbieten soll) vorgesehen.

Generell ist beabsichtigt, die im Jahresbericht für das (Start-) Infosystem dargestellte Kooperation auch für die weiteren Arbeiten fortzusetzen.

[59] JB 1999, 2.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

der Vertraulichkeit und Integrität der Daten bei ihrer Übertragung über das Landesnetz, den Schutz des Berliner Landesnetzes und der angeschlossenen Systeme vor Übergriffen aus dem weltweiten Internet, an das das Landesnetz notwendigerweise angeschlossen ist, und den Schutz der dezentralen Verfahren und Infrastrukturen vor unbefugtem Handeln innerhalb des Landesnetzes.

Verschlüsselung im Landesnetz

Die Sicherstellung der Vertraulichkeit und Integrität der personenbezogenen Daten im Landesnetz erfolgt durch den Einsatz sicherer Verschlüsselungsverfahren, der Schutz des Landesnetzes gegenüber dem Internet erfolgt mit Hilfe des „Grenznetzes“, hier speziell mit den zentralen Firewallsystemen zwischen Landesnetz und Internet. Hier erfolgen auch erste Virenprüfungen für die eingehenden Mails und Dateien. Auch innerhalb des Landesnetzes sorgen die dezentralen Firewalls der dezentralen Infrastrukturbetreiber (Behörden-, Rathausnetze) für die Sicherheit der angeschlossenen lokalen Netze[60].

Der Senat misst dem Schutz der Vertraulichkeit bei der Datenübertragung im Berliner Landesnetz große Bedeutung zu.

Zur Notwendigkeit der Verschlüsselung im Landesnetz bestand von Anfang an Konsens zwischen den verantwortlichen Betreibern und dem Berliner Beauftragten für Datenschutz und Informationsfreiheit[61]. Wie wir jedoch in früheren Jahresberichten mitzuteilen hatten, geriet die Umsetzung dieser Maßnahmen zur „unendlichen Geschichte“[62]. 1999 konnten wir jedoch „weißen Rauch“ vermelden: Nach langwierigen Erprobungen empfahl der Landesbetrieb für Informationstechnik das Produkt SafeGuard VPN für den Einsatz im Lande Berlin. Dieses Verfahren wurde dann tatsächlich im Zusammenhang mit dem Großverfahren IPV (Integrierte Personalverwaltung) eingesetzt. Als flächendeckend für alle Nutzer des Berliner Landesnetzes anwendbar, erwies sich diese Lösung aber als zu teuer und in der Anwendung zu aufwendig, so dass die Vollzugsmeldungen aus den Jahresberichten 1999 und 2000[63] voreilig waren und die „unendliche Geschichte“ um weitere Kapitel verlängert wurde, obwohl die personenbezogenen Daten im Berliner Landesnetz – wenn auch zum größten Teil ungeschützt – weiterflossen.

Das nach umfangreichen Erprobungen ausgewählte Produkt SafeGuard VPN realisiert eine anforderungsgerechte Verschlüsselung der Daten und wurde daher vom LIT und vom IT-KAB im Laufe des Jahres 1999 zur Anwendung empfohlen. Dementsprechend wird SafeGuard VPN u. a. im Verfahren Integrierte Personalverwaltung (IPV) eingesetzt.

Der ursprünglich verfolgte Ansatz, SafeGuard VPN flächendeckend auch im Bereich der dezentralen IT-Infrastruktur einzusetzen, ließ sich aber wegen der bestehenden Haushaltssituation nicht finanzieren.

Ein hartnäckiger Diskussionsgegenstand war die Frage, auf welchen Übertragungsstrecken eine Verschlüsselung überhaupt erforderlich sei, ob z. B. auch innerhalb lokaler Netze eine Verschlüsselung verlangt würde. Diese Frage kann pauschal nur so beantwortet werden, dass immer dann, wenn die Übertragungswege nicht hinlänglich gesichert werden können, die Sicherheit an den Daten selbst anzusetzen ist. Dies bedeutet dann Verschlüsselung. Wenn jedoch die Datenübertragungswege innerhalb eines Gebäudes vor dem Risiko bewahrt werden können, dass Unbefugte versuchen

[60] JB 1998, 2.2
[61] JB 1996, 3.4 und 4.8.1
[62] so die Überschrift im JB 1999, 4.8.1
[63] JB 2000, 2.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

können, den Datenverkehr unbemerkt abzuhören bzw. mitzuschneiden, dann ist auf diesen Strecken eine Verschlüsselung entbehrlich. Eine solche Antwort vermeidet den Umgang mit dem schillernden Begriff des lokalen Netzes, denn im Sprachgebrauch sind auch die Rathausnetze eines Bezirksamtes lokale Netze, obgleich sie sich möglicherweise über die Fläche des Bezirks ausdehnen. Die Antwort berücksichtigt auch die Vorgehensweise der aktuellen Methoden zur Erstellung von Sicherheitskonzepten und die Vorgaben von § 5 des neuen Berliner Datenschutzgesetzes: Was für die Sicherheit getan werden muss, richtet sich nach den konkreten Risiken, die im Einzelfall ermittelt worden sind. Eine standardisierte Sicherheitsbetrachtung ist nur für die ungeschützten Übertragungswege auf „freier Strecke“ möglich. Die Wege können nicht geschützt werden, also müssen schutzbedürftige Daten verschlüsselt werden.

2001 wurde das Thema Verschlüsselung im Landesnetz nach den Widerständen gegen die ursprüngliche Lösung Safeguard VPN, die zwar eine Ende-zu-Ende-Verschlüsselung ermöglichte, aber als zu teuer und zu schwer beherrschbar für eine flächendeckende Einführung galt, vom Zentralen IT-Management in der Senatsverwaltung für Inneres und vom IT-Koordinations- und Beratungsausschuss der Berliner Verwaltung (IT-KAB)[64] mit neuer Nachhaltigkeit angegangen.

Mit Beschluss des IT-KAB vom 29. November 2001 wird jetzt die Verschlüsselung auf Leitungsebene vorgeschrieben. Dieser Beschluss ist hoffentlich der Anfang vom Ende der „unendlichen Geschichte“. Die Umsetzung des Beschlusses soll jetzt innerhalb der zentralen IT-Infrastruktur durch den Einsatz einer hardwarebasierten Leitungsverschlüsselung gewährleistet werden, ein Lösungsweg, der bereits 1996 erwogen (Black Boxes), dann aber aus Kostengründen verworfen wurde. Inzwischen spricht die Entwicklung des Preis-Leistungs-Verhältnisses für solche Hardware für ihren Einsatz.

Die Daten sollen am Eintrittspunkt in das Berliner Landesnetz durch Krypto-Gateways verschlüsselt, dann in verschlüsselter Form transportiert, um am Austrittspunkt zur dezentralen Infrastruktur vom dortigen Krypto-Gateway wieder entschlüsselt zu werden. Bereits verschlüsselte Daten (z. B. IPV-Daten, die einer Ende-zu-Ende-Verschlüsselung mittels Safeguard VPN unterliegen) werden transparent, also unverändert, durchgeleitet.

Für die dezentralen Infrastrukturen wird es den dort Verantwortlichen überlassen, aufgrund eigener Risikoanalysen und Sicherheitskonzepte selbst zu entscheiden, wie die Sicherheit auf den Übertragungswegen gewährleistet werden soll. Falls die dezentrale Infrastruktur über mehrere Standorte verteilt ist und ungeschützte Übertragungswege in Anspruch nimmt, müssen Verschlüsselungsmechanismen vorgesehen werden. Entsprechend der Verantwortungsverteilung wird

Am 29. November 2001 wurde vom IT-KAB ein neues Konzept zum Schutz der Vertraulichkeit beschlossen. Mit den im Jahresbericht dargestellten Prinzipien können unter Berücksichtigung der bestehenden Haushaltssituation abgestimmte und an die jeweiligen Anforderungen angepasste Maßnahmen schrittweise realisiert werden. Insbesondere wurde auch die vom Berliner Beauftragten für Datenschutz und Informationsfreiheit dargestellte Problematik zum Schutz der Vertraulichkeit innerhalb eines Gebäudes berücksichtigt.

[64] JB 1997, 2.3

es jedoch den dezentral Verantwortlichen überlassen, über das Verfahren zu entscheiden.

Der Beschluss des IT-KAB sieht vor, dass ab Beginn des zweiten Quartals 2002 die Leitungsverschlüsselung schrittweise nutzbar sein wird. Wir sind nach der Vorgeschichte gespannt über die Umsetzung des Zeitplans, auch über die verfließende Zeit zwischen den einzelnen Schritten.

Die im Bereich der vom Landesbetrieb für Informationstechnik (LIT) betriebenen zentralen Infrastruktur vorgesehene so genannte „Leitungsverschlüsselung“ steht schrittweise ab dem II. Quartal 2002 zur Verfügung.

Weitere Themen

Die Netzsicherheit war im Berichtsjahr auch Schwerpunkt der Arbeitsgruppe IT-Sicherheit des IT-KAB. Diese Arbeitsgruppe beschäftigt sich mit allen Fragen der informationstechnischen Sicherheit in der Berliner Verwaltung. Sie erstellt den jährlichen IT-Sicherheitsbericht der Berliner Verwaltung und ist maßgeblich an der Erarbeitung von Regelungen, die die Sicherheit der Informationstechnologie der Berliner Verwaltung betreffen, beteiligt.

Die Gruppe besteht aus Mitgliedern des IT-Management bzw. von IT-Stellen der Bezirks- und Senatsverwaltungen und der Verwaltung des Abgeordnetenhauses sowie in beratender Funktion aus Vertretern des LIT, des Rechnungshofs und des Berliner Beauftragten für Datenschutz und Informationsfreiheit.

Die Arbeitsgruppe behandelte in diesem Jahr eine Vielzahl von Themen, die die Sicherheit des Berliner Landesnetzes betrafen und über die bereits behandelte Verschlüsselungsproblematik hinausgingen:

Mit In-Kraft-Treten der IT-Sicherheitsrichtlinie im Januar 1999 ist die Erstellung von Sicherheitskonzepten für den Betrieb einer IT-Infrastruktur unabdingbar. Mit In-Kraft-Treten des neuen Berliner Datenschutzrechts im August 2001 wurde diese Verpflichtung auf alle Berliner Landesbehörden ausgedehnt. Der Bedarf für ein „Musterkonzept“ für die Verwaltungen, die das Berliner Landesnetz nutzen wollen, war absehbar.

Bei näherer Betrachtung stellte sich jedoch heraus, dass die IT-Landschaften in den Behörden zu individuell waren, als dass ein standardisiertes Konzept den Anforderungen hätte gerecht werden können. Es wurden daher lediglich *Bausteine* entwickelt, die *als Grundlage für die Erstellung von Sicherheitskonzepten* herangezogen werden können.

Auch wenn die Erstellung einen nicht unbedeutenden Anteil von personellen und finanziellen Ressourcen benötigt, ist ein Sicherheitskonzept kein statisches Dokument, das einmalig erstellt wird. Der Wandel, die Modernisierung und/oder Ausbau, im Grunde jede Veränderung in der IT-Struktur erfordert die Anpassung des Konzepts an die neuen Gegebenheiten.

Die Verschlüsselung allein ist zum Schutz von Netzen nicht ausreichend. Jedes Behördennetz sollte sich gegenüber dem Landesnetz mittels einer Firewall absichern. Unter einer Firewall wird eine Schwelle zwischen zwei Netzen mit unterschiedlichen Sicherheits-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

ansprüchen verstanden, die überwunden werden muss, um Systeme im jeweils anderen Netz zu erreichen. Inzwischen besteht Einigkeit über die Notwendigkeit, dass solche Firewalls auch zum Schutz der Behörden untereinander erforderlich sind. Sie ergänzen überdies die Sicherheitsmaßnahmen des Grenznetzes gegen Angriffe aus dem Internet. Auch bei der netztechnischen Anbindung von Außenstellen sollten Firewalls vorgesehen werden, um das Risiko von Angriffen von Seiten der ungesicherten Leitung (z. B. die Man-in-the-Middle-Attacke) zu minimieren. Zur Realisierung wurden durch das LIT verschiedene *Low-Cost-Firewalls*, zumeist auf LINUX basierend, untersucht, die die Anbindung kleiner Standorte zu niedrigen Kosten ermöglichen.

Der Wunsch, im Rahmen des Aufbaus einer interaktiven Verwaltung alltägliche Prozesse (z. B. die Ummeldung beim Landeseinwohneramt) in das Internet zu verlagern, macht es notwendig, dass Personen im Netz eindeutig identifizierbar sein müssen. Um das zu verwirklichen, wurde das Modell für eine so genannte PKI für die Berliner Verwaltung entwickelt.

PKI steht für eine *Public-Key-Infrastruktur*. "*Public Key*" bezeichnet die Kerntechnologie, die für die Fälschungssicherheit, die eindeutige Identifizierungsmöglichkeit, aber auch für die Vertraulichkeit und die Unversehrtheit der digitalen Identität grundlegend ist, nämlich die asymmetrische Verschlüsselung, die mit Schlüsselpaaren arbeitet, von denen ein Teil öffentlich bekannt sein muss und der andere geheim zu halten ist. Ein solches Verfahren kann sowohl der Authentifizierung von Personen untereinander oder gegenüber einer Behörde dienen, als auch dem Nachweis der Authentizität von miteinander kommunizierenden Rechnern und Programmen.

Der Aufbau einer PKI ist eine wesentliche Voraussetzung für die Nutzung von elektronischen Signaturen, mit denen Nachweisbarkeit, Integrität und Authentizität bei der elektronischen Übermittlung von Dokumenten sicher gestellt werden können. Die verschiedenen Aktivitäten im Zusammenhang mit einer PKI werden im Rahmen des IT-KAB koordiniert.

Seit November 2001 ist die Beachtung a*ktiver Komponenten* bei der Erstellung von Sicherheitskonzepten Pflicht. Aktive Komponenten sind im Wesentlichen Java-Programme, JAVA-Script-Programme (eine Programmiersprache, mit der auf Internetseiten für Bewegung und Benutzerfreundlichkeit gesorgt werden kann) und ActiveX (Technologie von Microsoft, die den Funktionsumfang des Browsers erweitert). Während beim Netscape Navigator/Communicator eine Plug-in-Schnittstelle dafür sorgt, dass externe Programme wie z. B. Shockwave eingebunden werden können, kann der Microsoft Internet Explorer mit Hilfe von ActiveX-Komponenten z. B. auch bewegte Bilder und Töne übertragen.

Die Gefahren aktiver Komponenten für die informationstechnische Sicherheit ergeben sich daraus, dass es sich um Programme handelt, die während der Nutzung von Internettechnologie mehr oder weniger unbemerkt geladen und zur Ausführung gebracht werden. Wenn diese Programme auch unerwünschte Funktionen oder Schadensfunktionen unbemerkt ausführen können, stellen sie für die Vertraulichkeit der Daten auf dem betroffenen Rechner und für die Integrität und Verfügbarkeit des betroffenen Systems ein ernsthaftes Risiko

Wegen der mit so genannten aktiven Komponenten verbundenen Risiken sehen die geltenden Regelungen zur IT-Sicherheit verschiedene, abgestufte Schutzmaßnahmen vor.

Diese Maßnahmen bewegen sich in einem Spannungsfeld zwischen funktionalen Anforderungen der Anwender einerseits und restriktiven Nutzungseinschränkungen zum Minimieren der Risiken anderseits. Unter diesem Gesichtspunkt wird die Wirksamkeit und prak-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

dar. Dabei ist ActiveX die gefährlichste Variante der aktiven Komponenten, da mit ihr unbemerkt Eingriffe in das Betriebssystem eines Rechners veranlasst werden können.

Schon seit Jahren weisen wir auf die Gefahren aktiver Komponenten hin und empfehlen, diese in den Browsern entsprechend abzuschalten. Da dies jedoch mit Einschränkungen bei der Nutzung des Internets oder des Intranets verbunden ist, ist ein solches Moratorium kaum durchsetzbar. Umso mehr ist es wichtig, dass diese Fragen in Risikoanalysen und Sicherheitskonzepten Berücksichtigung finden.

tische Umsetzbarkeit der Regelungen regelmäßig überprüft.

Ein weiteres Thema war die seit November 2001 erfolgte *Kopplung des Berliner und des Brandenburger Verwaltungsnetzes* über das so genannte Testa-Netz. Das bundesweite Testa-Netz ist für die gemeinde- und länderübergreifende Vernetzung konzipiert worden. Die Kopplung basiert auf einem gesonderten Sicherheitskonzept, dem wir beipflichten konnten.

Der *Einsatz von Filterprogrammen bei der Internetnutzung*, die dafür sorgen, dass bestimmte Seiten nicht (Negativliste) oder nur bestimmte Seiten (Positivliste) erreicht werden können, wird auch in der Berliner Verwaltung erwogen. Damit sollen die Mitarbeiter, die das Medium Internet zunehmend akzeptieren und damit vertraut werden, davon abgehalten werden, das Internet in unzulässiger Weise nichtdienstlich zu nutzen. Mittlerweile gibt es diverse technische Lösungen, die es erlauben, bestimmte WWW-Seiten zu sperren. Aufgrund der Größe und des hohen Pflegeaufwandes und der damit verbundenen Kosten sind aber bisher alle Ansätze gescheitert. Wir werden die Entwicklung auf diesem Gebiet weiterverfolgen.

Der Senat betrachtet den Einsatz von Filterprogrammen auch wegen der im Jahresbericht dargestellten vielfältigen technischen und organisatorischen Probleme derzeit nicht als wirksame Sicherheitsmaßnahme bei der Nutzung des Internet.

In diesem Jahr haben wir mit Bedenken festgestellt, dass diverse Verfahren regelrechte Löcher in die Sicherheit von dezentralen Firewalls schlagen, weil ihre Nutzung es erfordert, dass *Ports der dezentralen Firewalls geöffnet* werden und die Firewalls damit ihre Wirkung verlieren. Als Beispiel ist das Großverfahren NBR/Profiskal zu nennen, das durch die Benutzung von so genannten „r-Diensten“ das obige Phänomen bewirkte. Im nächsten Jahr werden wir u.a. verstärkt solche Verfahren, auch so genannte Altverfahren, daraufhin untersuchen, welche besonderen Risiken sie für die Sicherheit des Berliner Landesnetzes darstellen.

Dem Senat ist die Problematik, die mit dem teilweisen Öffnen von Ports in den dezentralen Firewalls verbundenen ist, bewusst. In den entsprechenden Arbeitsgremien (IT-KAB, AG IT-Sicherheit) werden Maßnahmen zum Schutz vor den entstehenden Risiken untersucht.

Im Hinblick auf das Verfahren „Neues Berliner Rechnungswesen" (NBR) ist die Darstellung nicht mehr zutreffend. Im NBR werden keine "r-Dienste" wie z. B. ***rlogin, remsh, rcopy*** usw. mehr genutzt. Statt dessen werden nur noch die sicheren "secure-Kommandos" (***slogin, scopy*** usw.) verwendet. Die Öffnungen von Ports in der dezentralen Firewall der Senatsverwaltung für Finanzen sind deshalb entbehrlich geworden. Die inzwischen landesweit abgeschlossene Serverkonsolidierung für das NBR beim LIT hat auch an anderen Standorten die Notwendigkeit beseitigt, bei Einsatz von NBR Ports für "r-Dienste" in dezentralen Firewalls zu öffnen.

4. Aus den Arbeitsgebieten

4.1 Sicherheit und Strafverfolgung

4.1.1 Rasterfahndung

Als Reaktion auf die Ereignisse des 11. September 2001 nutzten die Sicherheitsbehörden erstmals seit den Tagen der RAF vor über 20 Jahren in großem Umfang die Ermittlungsmethode der Rasterfahndung. Aufgrund der schnellen Ermittlungserfolge in den USA stand fest, dass einige Täter längere Zeit in Deutschland gelebt und offenbar von hier aus den monströsen Anschlag geplant hatten. Es war nicht auszuschließen, dass sich hier weitere „Schläfer“ oder andere potenzielle Attentäter aufhalten, die möglicherweise auch deutsche Einrichtungen angreifen könnten. Konkrete Hinweise hierfür gab es allerdings nicht. Da die Attentäter im Wesentlichen ähnliche Persönlichkeitsmerkmale aufwiesen, ging man davon aus, dass eine gezielte Suche nach Personen, die diese Merkmale aufweisen, auf ihre Spur führen würde.

Angeblich aufgrund einer Idee des damaligen Präsidenten des Bundeskriminalamtes, Horst Herold, war eine Rasterfahndung erstmals 1979 in Frankfurt, später auch in anderen Städten durchgeführt worden: Die Erkenntnis, dass es zur Logistik von Terroristen gehörte, verschiedene Wohnungen anzumieten, ohne diese jedoch tatsächlich zu bewohnen, führte zu der Vermutung, dass ein Vergleich der Daten der Meldeämter (typische Persönlichkeitsmerkmale), der Elektrizitätsunternehmen (geringer Stromverbrauch), der Wohnungsbauunternehmen (bare Mietzahlung) und ähnlicher Hinweise zu den Tätern führen würde. In der Tat konnte in Frankfurt ein Verdächtiger ausfindig gemacht werden. Spätere Wiederholungen in anderen Städten, u.a. in Berlin, blieben ohne Erfolg. Diese Maßnahmen erfolgten ohne hinreichende Rechtsgrundlage, was zur Beanstandung durch die damals gerade etablierten Datenschutzbeauftragten führte[65].

Wie üblich wurde diesem Mangel durch die Schaffung entsprechender Befugnisnormen sowohl in der Strafprozessordnung (StPO) als auch in den Polizeigesetzen der Länder begegnet.

Im Rahmen des Gesetzes zur Bekämpfung der Organisierten Kriminalität wurde 1992 die Rasterfahndung in die StPO eingefügt (§ 98 a). Danach kann sie angeordnet werden, wenn zureichende tatsächliche Anhaltpunkte dafür vorliegen, dass bestimmte Straftaten von erheblicher Bedeutung begangen worden und bestimmte auf den Täter vermutlich zutreffende Prüfungsmerkmale bekannt sind. Die Maßnahme darf nur angeordnet werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre. Die Maßnahme muss grundsätzlich von einem Richter angeordnet werden (§ 98 b).

[65] JB 1980, 2.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Das Berliner Allgemeine Gesetz zum Schutz der Öffentlichen Sicherheit und Ordnung (ASOG) führte ebenfalls 1992 „besondere Formen des Datenabgleichs“ in das Berliner Polizeirecht ein (§ 47). Voraussetzung ist hier, dass die Maßnahme zur Abwehr einer gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist. Auch diese Maßnahme muss der Richter anordnen.

Die Durchführung der Rasterfahndung vollzieht sich in mehreren Stufen:

Zunächst müssen die Personengruppen bestimmt werden, deren Daten aus Dateien öffentlicher oder nichtöffentlicher Stellen zum Zwecke des Abgleichs mit anderen Datenbeständen an die Polizei übermittelt werden sollen. Die Merkmale, nach denen die Personen bestimmt werden, sind im einzelnen Fall festzulegen. Die Aussonderung der Daten hat grundsätzlich die datenverarbeitende Stelle selbst vorzunehmen, es sei denn, wegen technischer Schwierigkeiten, die mit angemessenem Zeit- oder Kostenaufwand nicht beseitigt werden können, ist dies nicht möglich. Herausgegeben werden müssen Namen, Anschriften, Tag und Ort der Geburt.

Die Polizei kann nach § 47 Abs. 2 Satz 1 ASOG nicht nur die Übermittlung von Namen, Anschriften, Tag und Ort der Geburt, sondern auch von weiteren, im Einzelfall festzulegenden Merkmalen verlangen.

Die Polizei führt in einem zweiten Schritt die aus verschiedenen Quellen stammenden Daten zusammen und überprüft den so entstehenden Gesamtbestand auf typische Merkmalskombinationen. Als Ergebnis dieses eigentlichen Teils der Rasterfahndung entstehen Datensätze, die zur Grundlage weiterer Ermittlungen gemacht werden. Wesentlich ist, dass es sich bei diesen Personen noch immer nicht um Verdächtige handelt, sondern um Personen, auf die die festgelegten Merkmale mehr oder weniger zufällig zutreffen können. Die anschließende Ermittlungsarbeit ist selbst nicht mehr Bestandteil der Rasterfahndung, diese ist vielmehr mit dem Vergleich der einzelnen Datenbestände und der Aussonderung der Zieldaten abgeschlossen. Ist dieser Zeitpunkt erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten zu löschen.

Die ersten Ermittlungen

Nach den schnellen Erfolgen hinsichtlich der Attentäter selbst übermittelten die amerikanischen Sicherheitsbehörden bald nach dem 11. September Datensätze, die für die in Frage kommenden Tätergruppen typisch sind. Die in Berlin sofort aufgenommenen Ermittlungen konzentrierten sich auf die „Schläfer“, die einen normalen Alltag (z. B. als Student) führen und strafrechtlich bisher nicht auffällig geworden sind. Die Auffälligkeiten bestehen darin, dass die Personen an Stellen auftauchen, die nicht zu den sonstigen Lebensverhältnissen passen. Dabei gerieten zunächst Studenten in das Blickfeld, weil dies der einfachste Weg für Ausländer ist, einen legalen Aufenthaltsstatus zu erlangen.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Entgegen ursprünglichen Annahmen lehnte der Generalbundesanwalt eine auf die StPO gestützte Rasterfahndung ab. Stattdessen leitete der Polizeipräsident Ermittlungen aufgrund des ASOG ein. Nach der Festlegung gefährdeter Objekte und der Suchmerkmale wurde am 17. September 2001 damit begonnen, bei bestimmten Stellen, wie z. B. dem Hahn-Meitner-Institut, den Berliner Wasserbetrieben sowie Hochschulen und Fachhochschulen Daten zu erheben, um mit diesen eine Rasterfahndung durchzuführen. Eine richterliche Anordnung wurde zwar angekündigt, sie lag aber zu diesem Zeitpunkt noch nicht vor.

Der lange Weg zu einer richterlichen Anordnung

Erst am 19. September 2001 wurde die richterliche Anordnung der Rasterfahndung beantragt, der Antrag wurde jedoch zurückgewiesen, da die gegenwärtige Gefahr nicht hinreichend belegt worden war. Erst eine erneute Begründung führte am 20. September zu dem ersten Beschluss, in dem die verschiedensten Stellen wie Hochschulen und Fachhochschulen, Ver- und Entsorgungsunternehmen, Atomanlagen, Personennah- und fernverkehrsunternehmen, Kommunikationsdienstleister, Flughafengesellschaften, Sicherheitsdienste zur Herausgabe von Daten verpflichtet wurden. Als Rasterungsmerkmal wurden 11 Merkmale angegeben, u. a. männliches Geschlecht, islamische Religionszugehörigkeit ohne nach außen tretende fundamentalistische Grundhaltung, legaler Aufenthalt, keine Auffälligkeiten im allgemeinen kriminellen Bereich, finanzielle Unabhängigkeit oder Flugausbildung. Erst nach Erlass des Beschlusses stellte die Polizei fest, dass es bei Anlegung dieser Merkmale zu überhaupt keinen Trefferfällen kommen würde, weil keine der verpflichteten Stellen über alle diese Daten verfügt. Deshalb berichtigte der Amtsrichter am 21. September 2001 auf Antrag des Landeskriminalamtes den Beschluss dahingehend, dass die Merkmale der zu überprüfenden Personengruppe lediglich die Eigenschaften „vermutlich islamische Religionszugehörigkeit“ und „vermutlich legaler Aufenthaltsstatus in Deutschland“ (wegen eventuell gefälschter Papiere) umfassen. Nicht klar umschrieben wurde, aus welchen Datenbeständen die Daten überhaupt ausgesondert werden sollten und wie die betroffene Personengruppe definiert wird (z. B. Kunden- oder Mitarbeiterdaten).

Erst nach weiteren Beratungen, bei denen wir der Polizei Hinweise auf das korrekte Vorgehen gaben, wurde mit Beschluss vom 24. Oktober 2001 eine Anordnung getroffen, die den Anforderungen des § 47 ASOG im Wesentlichen entsprach, wenn sie auch nach wie vor gewisse Mängel aufwies. Ohne dass von diesem Teil der Anordnung Gebrauch gemacht worden wäre, hätte sie auch die Herausgabe von Daten durch Sozialbehörden gestattet, die zum Zeitpunkt der Anordnung nach dem Sozialgesetzbuch X rechtswidrig gewesen wäre und erst durch das Terrorismusbekämpfungsgesetz legalisiert wurde. Die Personen, die die Sicherheitsbe-

Die Darstellung ist im wesentlichen zutreffend.

Mit der ersten Rasterfahndung nach polizeirechtlichen Vorschriften in Berlin haben nicht nur Polizei und Gerichte, sondern auch der Berliner Beauftragte für Datenschutz und Informationsfreiheit Neuland betreten. Niemand konnte von daher für sich in Anspruch nehmen, auf Anhieb perfekte Lösungen zu haben.

Im übrigen hat das Landgericht Berlin die Anordnung des Amtsgerichts Tiergarten aufgehoben, weil es die Voraussetzungen für eine Maßnahme nach § 47 ASOG von vornherein nicht als gegeben angesehen hat.

Das Vorliegen dieser Voraussetzungen hat der BlnBDI jedoch zu keinem Zeitpunkt in Frage gestellt.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

hörden im Blickfeld hatten, wurden nach polizeilichen Erkenntnissen ohnehin von außen finanziert und kamen als Sozialhilfeempfänger nicht in Betracht.

Die Herausgabe der Daten

Das Hahn-Meitner-Institut lieferte vor der richterlichen Anordnung bereits auf deren Ankündigung hin Daten über Sicherheitsüberprüfungen von Mitarbeitern von Fremdfirmen, die am Reaktor tätig sind, und Besucherlisten der letzten Jahre einschließlich der Ablichtungen von Personalausweisen, die in der „Langen Nacht der Wissenschaften“ am 15. September 2001 angefertigt wurden. Eine Aussonderung von Daten nach den vorgegebenen Merkmalen wurde lediglich hinsichtlich der Sicherheitsüberprüfungen des eigenen Personals vorgenommen. Die Berliner Wasserbetriebe haben aufgrund einer telefonisch Anforderung Daten von 23 Beschäftigten herausgegeben.

Im Gegensatz zu diesen Unternehmen haben andere Stellen auf die erste Anforderung mit Zurückhaltung reagiert. Insbesondere Hochschulen verweigerten die Herausgabe, bis die richterliche Anordnung vorlag. Auch die meisten anderen befragten Stellen lieferten die Daten erst nach Vorliegen der richterlichen Anordnung vom 21. September.

Da keine der befragten Stellen über das Merkmal „Religionszugehörigkeit“ verfügte und deren Speicherung datenschutzrechtlich sogar rechtswidrig gewesen wäre, gestaltete sich die Auswahl der Datensätze schwierig. Als wesentliches Merkmal kristallisierte sich die Staatsangehörigkeit heraus, aus der – problematische – Schlüsse auf die Religionszugehörigkeit gezogen wurden.

Insgesamt sind an die Polizei etwa 58.000 Datensätze übermittelt worden, deren Überprüfung bis zum Jahresende andauerte und erst im Januar 2002 abgeschlossen wurde. Zum Verlauf und Ergebnis der Rasterfahndung werden wir dem Abgeordnetenhaus einen gesonderten Bericht nach § 29 Abs. 3 Satz 2 BlnDSG vorlegen.

Die Darstellung des Berliner Beauftragten für Datenschutz und Informationsfreiheit entspricht den Gegebenheiten. Die Festlegung der Merkmale erfolgte mit seiner Beteiligung.

4.1.2 Polizeialltag

Globalisierungsgegner

Mehrere Teilnehmer an den Demonstrationen der Globalisierungsgegner anlässlich des EU-Gipfels in Göteborg (Schweden) und des G 8-Treffens in Genua (Italien) haben die Vermutung geäußert, dass es im Vorfeld einen Datenaustausch zwischen den Sicherheitsbehörden gegeben haben muss. So hatten einige bereits bei der Einreise nach Schweden erhebliche Schwierigkeiten; andere, die per Bus angereist sind, wurden von der schwedischen Polizei begleitet und dabei mehrfach kontrolliert. Schwedische Beamte sollen einem Petenten erklärt haben, er würde auf einer so genannten „Sperrliste“ mit politischen Gewalttätern stehen. Ein Bürger, der sich in Genua aufgehalten und

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

in der Diaz-Schule festgehalten wurde, ist bei der Vorführung beim Haftrichter mit einem mehrere Jahre zurückliegenden Ermittlungsverfahren der Berliner Staatsanwaltschaft konfrontiert worden. Weiterhin hatte der Haftrichter ihm mitgeteilt, dass gegen ihn ein ihm bis daher gänzlich unbekanntes Ermittlungsverfahren geführt wurde.

Die Polizeibehörde in Västra Götaland hat etwa 200 Abweisungen nach schwedischem Ausländerrecht verfügt. Über 100 davon betrafen deutsche Staatsbürger. Der Polizeipräsident hat uns dazu mitgeteilt, dass er im Vorfeld des Gipfels keine personenbezogenen Daten nach Schweden übermittelt hat.

Vor dem G 8-Treffen in Genua hat der Polizeipräsident in Berlin verschiedenen Personen Meldeauflagen erteilt und Gefährderansprachen durchgeführt. Das Landeseinwohneramt Berlin hat den Geltungsbereich von Personalausweisen beschränkt. Diesen Personen wurde damit die Ausreise untersagt. Später hat der Staatsschutz auf Anforderung des Bundeskriminalamtes Listen mit den Namen, Anschriften und Geburtsdaten dieser Personen dorthin übermittelt. Die Übermittlung war nach § 13 Bundeskriminalamtsgesetz (BKAG) i.V.m. § 44 Allgemeines Sicherheits- und Ordnungsgesetz (ASOG) zulässig. Auch hier hat der Polizeipräsident in Berlin erklärt, dass er keine personenbezogenen Daten an italienische Behörden weitergegeben hat.

Die Senatsverwaltung für Justiz hatte uns zu den Ereignissen in Genua mitgeteilt, dass die Staatsanwaltschaft italienischen Stellen keine Auskünfte erteilt hatte. Auf der vom Landeskriminalamt dem Bundeskriminalamt zur Verfügung gestellten Liste war der Petent nicht enthalten; allerdings stand eine Person mit sehr ähnlichem Nachnamen auf der Liste, so dass eine Verwechslung bei dem Bundeskriminalamt oder aber bei den italienischen Behörden nicht ausgeschlossen werden kann.

Das Landeseinwohneramt Berlin hat im Zusammenhang mit dem G 8-Treffen in Genua gegen Personen, die mehrfach durch politisch motivierte Straftaten in Erscheinung getreten und dem Kreis der militanten Globalisierungsgegner zuzurechnen sind, wegen Gefährdung erheblicher Belange der Bundesrepublik Deutschland für die Dauer des Gipfeltreffens pass- bzw. ausweisbeschränkende Maßnahmen angeordnet. Die Ausführungen des Berliner Beauftragten für Datenschutz und Informationsfreiheit sind insoweit zutreffend.

Bekämpfung des Rechts- und Linksextremismus

Der Arbeitskreis II (Innere Sicherheit) der Innenministerkonferenz hat den Beschluss gefasst, in Anlehnung an die Datei „Gewalttäter Sport“ eine bundesweite Datei „Gewalttäter Rechts“ zu dem Zweck einzurichten, rechtsorientierte, politisch motivierte Straftaten, insbesondere Gewalttaten, zu verhindern. Zusätzlich wird ein personengebundener Hinweis „REMO“ (rechtsmotiviert) eingeführt. Darüber hinaus sieht der Arbeitskreis II auf der Grundlage der jeweiligen Polizeigesetze weitere geeignete Ansätze der Länder zur Verfolgung der rechten Szene durch eine DV-technische Erfassung von „rechten“ Störern im Rahmen der Gefahrenabwehr.

Die Innenministerkonferenz hat darüber hinaus einen Maßnahmenkatalog zur Bekämpfung der rechtsextremistischen, fremdenfeindlichen und antisemitischen Kriminalität (Intensivierung der Öffentlichkeitsarbeit, anlassunabhängige Recherche im Internet, Intensivierung von Fahndungs- und Kontrollmaßnahmen, Inten-

Durch die Einführung bundesweiter Dateien und von Katalogwerten zur Erfassung linksorientierter, rechtsorientierter sowie politisch motivierter Ausländerkriminalität soll eine bundesweit geführte Informationssammlung geschaffen werden, um einen verlässlichen Überblick über ein bedeutsames Krimi-

sivierung der Zusammenarbeit mit Schulen, Trägern der Jugendsozialarbeit usw., Gefährderansprachen und Hilfen für Ausstiegsangebote) sowie eine Präventionskampagne gegen Rechtsextremismus beschlossen. Gleichzeitig wurde die Einführung bundesweiter Dateien und von Katalogwerten zur Erfassung linksorientierter, politisch motivierter Straftäter und Straftäter politisch motivierter Ausländerkriminalität in INPOL sowie Störerdateien der Länder beschlossen.

Bei allem Verständnis für Maßnahmen, um die zunehmende politisch motivierte Kriminalität effektiver bekämpfen zu können, bestehen erhebliche Zweifel an der Erforderlichkeit und der Verhältnismäßigkeit des beschlossenen Maßnahmenkataloges. Diese neuen personengebundenen Hinweise gehen in der Intensität des Eingriffes in die Rechte der Betroffenen deutlich über die Aufnahme von Datensätzen in Dateien – z. B. in die Datei „Gewalttäter Sport“ – hinaus, weil der Hinweis automatisch bei jedem polizeilichen Kontakt mit dem Betroffenen wie bei einer Verkehrskontrolle angezeigt wird.

Nach dem BKAG ist die Speicherung von personengebundenen Hinweisen nur zulässig, wenn das zur Eigensicherung von Beamten oder zum Schutz des Betroffenen erforderlich ist (§ 7 Abs. 3). Die Senatsverwaltung für Inneres hält demgegenüber § 8 Abs. 2 BKAG – wonach personenbezogene Daten von Beschuldigten und Tatverdächtigen gespeichert, verarbeitet und genutzt werden dürfen, wenn das erforderlich ist, weil wegen der Art der Ausführung der Tat, der Persönlichkeit des Betroffenen oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass Strafverfahren gegen den Beschuldigten oder Tatverdächtigen zu führen sind – für eine breite und tragfähige Rechtsgrundlage. Subjektive Einschätzungen – also beispielsweise die Wertung, gewalttätig zu sein – bringt der Gesetzgeber durch den Begriff „personengebundene Hinweise“ zum Ausdruck. In § 8 Abs. 2 BKAG ist jedoch von personenbezogenen Daten die Rede. Wenn § 8 Abs. 2 BKAG auch die Speicherung subjektiver Einschätzungen umfassen würde, entfiele der eigenständige Anwendungsbereich des§ 7 Abs. 3 BKAG hinsichtlich der Beschuldigten und Verdächtigen. Die strengeren Anforderungen würden somit umgangen.

Die von der Innenministerkonferenz beschlossenen Maßnahmen zielen einerseits darauf ab, den Vollzugsbeamten in Bund und Ländern bei den polizeilichen Kontrollen vor Ort entscheidende personenbezogene Informationen zukommen zu lassen, auf deren Grundlage geeignete präventive oder repressive Maßnahmen ergriffen werden können. Dazu sollten die personengebundenen Hinweise in den INPOL-Dateien „Personenfahndung“, „Erkennungsdienst“ und „Kriminalpolizeilicher Aktennachweis“ (KAN) gespeichert werden. Andererseits werden den Vollzugsbeamten die Inhalte der auf Länderebene im Rahmen der Gefahrenabwehr eingerichteten Störer-Dateien zur Verfügung gestellt.

Es ist nicht zu erkennen, welche zusätzlichen Erkenntnisse aus den geplanten Verbunddateien gewonnen nalitätsphänomen wie das der politisch motivierten Straf- und insbesondere Gewalttaten zu gewinnen und um diese effektiver bekämpfen zu können.

Die Speicherung der personengebundenen Hinweise „LIMO“, „REMO“, „AUMO“ in den bereits bestehenden INPOL -Verbunddateien ist entgegen der Auffassung des Berliner Beauftragten für Datenschutz und Informationsfreiheit auf der Grundlage des § 8 Abs. 2 BKAG rechtlich zulässig. Diese Rechtsauffassung wird auch vom Arbeitskreis Innere Sicherheit II (s. Umlaufbeschluss vom 13.11.2000, Abschnitt II Nr. 3) bezüglich des personengebundenen Hinweises „REMO“ vertreten. Der Beschluss ist uneingeschränkt auf die von der Innenministerkonferenz am 24.11.2000 ebenfalls beschlossenen personengebundenen Hinweise „LIMO“ und „AUMO“ anwendbar.

Ausweislich der Gesetzesbegründung zu § 8 Abs. 2 BKAG ist die Speicherung von personenbezogenen Daten sowohl zu Zwecken der Verhütung von Straftaten als auch zur künftigen Strafverfolgung zulässig. Mit den genannten personengebundenen Hinweisen wird genau dieser vom Gesetzgeber beabsichtigte zweifache Zweck verfolgt. Richtig ist, dass diese Hinweise subjektive Einschätzungen in Bezug auf die Betroffenen wiedergeben. Allerdings bewirkt nicht die politische Anschauung allein kausal eine Eintragung, sondern es müssen zusätzlich die Voraussetzungen des § 8 Abs. 2 BKAG erfüllt sein. Nur dann, wenn der personengebundene Hinweis im konkreten Fall zur Verhütung von Straftaten oder zur künftigen Strafverfolgung erforderlich ist, kann er eingestellt werden. Es liegt damit eine klare Abgrenzung zu den Fällen des § 7 Abs. 3 BKAG vor.

Die polizeilichen Erfahrungen bei der Bekämpfung des Rechtsextremismus lassen eine verbesserte präventive und repressive Aufgabenerfüllung durch die personengebundenen Hinweise insofern erwarten, als sie geboten sind für die Durchführung polizeilicher Maßnahmen z.B. im Vorfeld von Skinheadkonzerten, Versammlungen etc. oder im Rahmen der Fahndung nach politisch motivierten Straftaten. Die Umstände, die zu der Annahme führen, dass solche Maßnahmen gegen die betreffende Person zu richten sein werden, sind Gegenstand der obligatorischen Einzelfallprüfung.

Die neuen Verbunddateien bzw. Anlass-Zweck-Kombinationen und die personengebundenen Hinweise in den bestehenden INPOL – Dateien wurden erforderlich, weil das gegenwärtige Dateiensystem von INPOL (aktuell) mit seinem Bestandsführungs- und Zugriffsregelungen es nicht mehr auf einfache Weise ermöglicht, jedem Polizeibeamten die für seine Aufgabenerfüllung richtigen Informationen zielgenau zur Verfügung zu stellen. Nur das Programm „Personenfahndung“ steht allen Polizeibeamten für Auskünfte bei „Fahndungsabfragen“ zur Verfügung; die drei neuen Dateien nutzen diese Möglichkeit, durch die Vergabe der Anlass-Zweck-Kombination derartige Personen, bei denen verdichtete Erkenntnisse zur Gewalttätigkeit bzw. Gewaltbereitschaft im Zusammenhang mit poli-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

werden können. Im Übergangsbetrieb ist ohnehin nur die Speicherung der Personalien der Betroffenen sowie die Anlass-Zweck-Kombination zulässig. In den Errichtungsanordnungen sind die Kriterien, nach denen die Daten eingestellt werden sollen, wenig präzise. Das Bundesministerium des Innern legt darüber hinaus den Begriff der „Straftaten von erheblicher Bedeutung“ sehr extensiv aus; das hat zur Folge, dass eine aus extremistischen, politischen Beweggründen begangene Tat dann regelmäßig eine Straftat von erheblicher Bedeutung (§ 2 Abs. 1 BKAG) ist. Diese Auslegung wird in dem Entwurf der Errichtungsanordnung für die INPOL-Verbunddatei KAN deutlich: Danach soll der Verdacht des Handelns zur Verfolgung extremistischer Ziele oder die Begehung fremdenfeindlicher Straftaten generell das Merkmal der überregional bedeutsamen Straftaten erfüllen. Dadurch wird eine viel zu weit gehende Hereinnahme potenziell extremistisch motivierter Straftaten unter faktischer Umgehung der Speicherungsschwellen des BKAG (§ 2 Abs. 1 BKAG) erreicht. Auch die Löschungs- und Prüffristen sind zu lang. Eine Pflicht zur Dokumentation der Begründung für die Vergabe eines personengebundenen Hinweises fehlt.

Die Senatsverwaltung für Inneres hat in das Abstimmungsverfahren – ohne die Zustimmung der Länder können Verbunddateien bei dem Bundeskriminalamt nicht dauerhaft eingerichtet werden – ihre Bedenken eingebracht, soweit Platzverweise oder Personalienfeststellungen als Speicherungsanlass bei den „sonstigen Personen“ – also Personen, die nicht Beschuldigte oder Verdächtige sind – ausreichen sollen. In Berlin werden Personen, die nach Polizeirecht „Störer“ sind, ohne Straftäter zu sein, nicht in Dateien zentral erfasst. Der Polizeipräsident in Berlin kann diese Daten nicht anliefern.

tisch motivierter Kriminalität vorliegen, bei jeder INPOL - Fahndungsabfrage sichtbar zu machen. Diese Kenntnis kann nicht zuletzt aus Gründen der Eigensicherung für die jeweiligen Polizeibeamten von Bedeutung sein. Ferner ermöglicht diese Information, dass im Einzelfall geeignete repressive bzw. präventive Maßnahmen ergriffen werden können. Die Dateien im beschriebenen Übergangsbetrieb sind im Gegensatz zu den Störer-Dateien auf Landesebene für den Nutzer länderübergreifend verfügbar. Das ist gerade in Ballungsräumen in der Nähe von Landesgrenzen für die polizeiliche Aufgabenerfüllung unverzichtbar. Allein die Realisierung von Störer-Dateien auf Landesebene macht nicht generell die länderübergreifende Sammlung verzichtbar, weil es gerade darum geht, das besondere Kriminalitätsphänomen der politisch motivierten Kriminalität länderübergreifend im Rahmen einer Verbunddatei abzubilden, um einen verlässlichen Überblick über diese Kriminalitätsform zu gewinnen. Durch den Austausch bzw. die Verfügbarkeit von Informationen bei der praktischen polizeilichen Arbeit ergeben sich regelmäßig zusätzliche Erkenntnisse; dies gilt sowohl für die Nutzung der Verbunddateien als auch für die auf Landesebene vorgesehenen Störer-Dateien, auf deren inhaltliche Ausgestaltung bundesseitig keinerlei Einflussmöglichkeit besteht.
Unabhängig davon haben bisher auch nicht alle Länder in eigener Zuständigkeit auf der Grundlage ihrer landesrechtlichen Regelungen eigene Störer-Dateien realisiert. Das gilt auch für das Land Berlin.

Im Gegensatz zu der vom Berliner Beauftragten für Datenschutz und Informationsfreiheit vertretenen Auffassung kommt extremistisch motivierten Straf- bzw. Gewalttaten im Hinblick auf ihre Wirkung auf die Gesellschaft und auch wegen ihrer nicht zu unterschätzenden internationalen Außenwirkung regelmäßig eine „erhebliche Bedeutung“ und in einer Vielzahl von Fällen auch „länderübergreifende Bedeutung“ i.S. des § 2 Abs. 1 BKAG zu. In der Gesetzesbegründung (BT-Drs. 13/1550, zu § 2, Seite 21) wird in diesem Zusammenhang u.a. auch auf die Beeinträchtigung des Rechtsfriedens und der Rechtssicherheit durch die konkrete Tat abgestellt.

Diese Kriterien dürften bei politisch motivierten extremistischen Straftaten regelmäßig wegen der bereits genannten Wirkung für die innere Sicherheit und ihrer internationalen Außenwirkung erfüllt sein, so dass die Speicherung der Daten nach hiesiger Auffassung auf § 2 Abs. 1 BKAG gestützt werden kann. Da die Einstellung der Daten in die drei Dateien bzw. Anlass-Zweck-Kombinationen von den Staatsschutzdienststellen in Bund und Ländern vorgenommen wird, ist die Würdigung des konkreten Einzelfalles und eine einheitliche Erfassungspraxis gewährleistet.

In dem bereits an anderer Stelle erwähnten Umlaufbeschluss des AK II vom 13.11.2000 ist im Zusammenhang mit der Einführung des personengebundenen Hinweises „REMO“ in Abschnitt II, Nr. 2 die grundsätzliche KAN-Relevanz für Straftaten aus rechtsori-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

entierten politisch motivierten Beweggründen beschlossen worden. Dieser Beschluss ist im Hinblick auf die nachfolgenden Beschlüsse der IMK vom 24.11.2000 erweiternd dahingehend zu interpretieren, dass von einer grundsätzlichen KAN-Relevanz aller aus politisch motivierten Beweggründen begangenen Straftaten auszugehen ist.

Die Auffassung des BlnBDI, dass die Löschungs- und Prüffristen zu lang sind, wird diesseits vor dem Hintergrund der polizeifachlichen Erforderlichkeit nicht geteilt. Es ist jedoch darauf hinzuweisen, dass der jeweilige polizeiliche Sachbearbeiter im konkreten Einzelfall nicht daran gehindert ist, eine von der Regel abweichende kürzere Aussonderungsprüffrist festzusetzen. Zudem wird sich die retrograde Erfassung in der Anlass-Zweck-Kombination nach einhelliger Auffassung der Kommission Staatsschutz der AG Kripo auf aktuelle Erkenntnisse beschränken.

Die Ausführungen des BlnBDI zu der Haltung des Landes Berlins im Zustimmungsverfahren nach § 34 Abs. 2 BKAG sind zutreffend. Richtig ist auch, dass das Land Berlin keine Datei führt, in der Störer, die keine Straftäter sind, zentral erfasst werden, so dass es diesbezügliche Daten nicht anliefern kann.

Telefonüberwachung

Die Zahl der Telefonüberwachungen ist in den vergangenen Jahren ständig gestiegen. So lag die Zahl der richterlichen oder staatsanwaltschaftlichen Anordnungen im Jahr 1995 noch bei 217; sie stieg bis zum Jahr 2000 auf 739[66]. Dabei wird über die Zahl der überwachten Gespräche sowie der betroffenen Personen keine Statistik geführt. Diese Maßnahmen haben im Haushaltsjahr 2000 rund 443.000,00 DM Fernmeldegebühren, etwa 42.000,00 DM mit steigender Tendenz – für Reparaturen sowie etwa 58.000,00 DM für Verbrauchsmittel zur Beweissicherung gekostet. Eine Statistik, in wie vielen Fällen die Ergebnisse einer Telefonüberwachung zu einer Verurteilung geführt haben, wird nicht geführt. Nach Wegfall der Analogtechnik im Jahr 1999 verfügt die Berliner Polizei über 75 digitale Aufzeichnungseinheiten zuzüglich zwei Aufzeichnungseinheiten der älteren Generation als Dauerleihgabe aus Brandenburg sowie über 55 Auswerteeinheiten. Seit Jahren bestehen erhebliche Engpässe bei der Umsetzung mit Wartelisten von bis zu 80 kapazitätsbedingt nicht umsetzbaren Beschlüssen im März/April 2001. Durch Fristablauf zahlreicher, nicht umsetzbarer Beschlüsse lag die Zahl im Mai 2001 bei 26 Telefonüberwachungen. Die vorhandene Technik ermöglicht sowohl die Überwachung des Telefonfestnetzes als auch von Telefonmobilfunknetzen, sofern die dafür erforderlichen Teilnehmerdaten bekannt sind.

Vor diesem Hintergrund ist es geboten, dass für Telekommunikationsabhörmaßnahmen – wie bei der akustischen Wohnraumüberwachung[67] – eine Berichts-

Hinweis zur Fußnote 66:

SenInn hat auf die Kleine Anfrage Nr. 1828, LPD 145/2001 vom 19. Juni 2001 zum Thema Telefonüberwachung geantwortet und darin Fernmeldegebühren in Höhe von 483 000 DM ausgewiesen.

[66] Antwort des Senates auf die Kleine Anfrage Nr. 1823, LPD 145/2001 vom 30. Juli 2001
[67] JB 2000, 4.1.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

pflicht im Gesetz festgeschrieben wird. Dabei sollte nicht nur einbezogen werden, wie die Maßnahmen wirken und wie viele Personen mit wie vielen Gesprächen betroffen waren, sondern auch welche Erfolge – Zahl der Verhaftungen, Anklageerhebungen und Verurteilungen – sie gebracht und gekostet haben sowie was mit den nicht mehr für die laufenden Ermittlungsverfahren benötigten Daten geschieht. Nur so können die Befugnisse, mit denen tief in die Persönlichkeitsrechte eingegriffen wird, im Hinblick auf die Wirkungen bewertet werden. Das macht das Instrument auch für die Bürger transparenter. Sie müssen nachvollziehen können, aus welchen Gründen die Eingriffe in ihre Freiheitsrechte in einem Rechtsstaat gerechtfertigt sind.

Schleierfahndung

Im vergangenen Jahr[68] haben wir über die nicht besonders beeindruckenden Ergebnisse der verdachts- und anlassunabhängigen Kontrollen berichtet. Danach kann die Polizei zur vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität im öffentlichen Verkehrsraum angetroffene Personen kurzzeitig anhalten, befragen und verlangen, dass mitgeführte Ausweispapiere zur Prüfung ausgehändigt werden, sowie mitgeführte Sachen in Augenschein nehmen. Die Maßnahme ist nur zulässig, wenn aufgrund von Lageerkenntnissen anzunehmen ist, dass Straftaten von erheblicher Bedeutung begangen werden sollen. Die Auswertung der im Berichtsjahr durchgeführten Maßnahmen bestätigt die ernüchternden Ergebnisse des Vorjahres. Ein durchschlagender Erfolg bei der Bekämpfung der grenzüberschreitenden Kriminalität war nicht zu erkennen.

Im Bereich einer Direktion wurden im Rahmen der lageabhängigen Kontrollen 272 Personen und 130 Fahrzeuge kontrolliert. Dabei sind immerhin 17 Strafanzeigen zu Delikten wie illegaler Aufenthalt, mutmaßliche Schleusertätigkeit, aber auch Urkundenfälschung, aufgefundener Pkw nach unerlaubtem Entfernen vom Unfallort und Verdacht der Trunkenheit im Straßenverkehr gefertigt worden. Es stehen also nur wenige der gefertigten Strafanzeigen im Zusammenhang mit dem eigentlichen Zweck der Regelung, Instrumente für die Bekämpfung der grenzüberschreitenden Kriminalität zu schaffen.

Im Bereich einer anderen Direktion belief sich die Zahl der kontrollierten Personen auf etwa 3.500 und die der kontrollierten Kfz auf etwa 1.900. Bei dieser hohen Zahl an kontrollierten Personen wurden lediglich acht Strafanzeigen, davon eine wegen Geldwäsche im Zusammenhang mit illegalem Zigarettenhandel, gefertigt. Darüber hinaus wurden diverse Ordnungswidrigkeitenverfahren verkehrsrechtlicher Art eingeleitet. An einem Tag wurden beispielsweise an vier Kontrollstellen 53 Personen und 40 Kfz ohne Ergebnis kontrolliert; an einem anderen Tag sind 70 Beamte an acht Kontrollstellen eingesetzt worden, ohne dass eine einzige An-

Der Gesetzgeber hat in § 18 Abs. 7 des Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG) keine verdachtsunabhängigen, sondern **lageabhängige** Kontrollen geregelt. Der Begriff „Schleierfahndung“ ist in diesem Zusammenhang irreführend und sollte künftig vermieden werden.

Die Darstellung des Berliner Beauftragten für Datenschutz und Informationsfreiheit kann wie folgt aktualisiert werden:
Aus Anlass der vermehrten Entwendung hochwertiger Kfz sowie deren Ausschlachtung und Verschiebung der Autoteile in das osteuropäische Ausland wurde eine weitere Kontrollmaßnahme Ende März /Anfang April 2002 durchgeführt. Seit Inkrafttreten der Vorschrift des § 18 Abs. 7 ASOG wurden somit insgesamt 8 Kontrollmaßnahmen durchgeführt. Bei der letzten Maßnahme wurden insgesamt 292 Personen und 274 Fahrzeuge kontrolliert. Es kam zu keinen Festnahmen. Ein Kfz wurde wegen ungeklärter Eigentumsverhältnisse sicher gestellt. Strafanzeigen wegen (kontroll-) anlassbezogener Delikte wurden nicht gefertigt. Es wurden jedoch 13 Strafanzeigen wegen Fahrens unter Alkohol/Drogeneinwirkung, Fahrens ohne Fahrerlaubnis, 3 Strafanzeigen wegen Verstoßes gegen das Ausländergesetz sowie 2 Strafanzeigen wegen Verstoßes gegen das Betäubungsmittelgesetz gefertigt. Ferner wurden insgesamt 50 Ordnungswidrigkeiten festgestellt.

Richtig ist, dass von einem „durchschlagenden Erfolg“ dieser polizeilichen Kontrollmaßnahmen bisher nicht

[68] JB 2000, 4.1.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

zeige oder eine Verkehrsordnungswidrigkeit aufgenommen wurde.

gesprochen werden kann. Allerdings kann ein solcher bei realistischer Betrachtung der hohen Delikts- und Eingriffsvoraussetzungen und der eingeschränkten Eingriffskompetenzen des § 18 Abs. 7 ASOG auch kaum erwartet werden und wurde polizeilicherseits auch nie in Aussicht gestellt. Die vermeintliche Erfolglosigkeit solcher Kontrollen lässt sich nicht allein daran bemessen, ob und in welcher Quantität „Treffer" im Sinne des Kontrollzwecks erzielt werden konnten. Diese Sichtweise berücksichtigt nicht die Vielzahl von der Polizei nicht zu steuernder bzw. nicht zu beeinflussender Faktoren (Täterprofessionalisierung, z.B. Streckenaufklärung, Kommunikationsmöglichkeiten, Zufall usw.). Die im Jahresbericht und oben genannten aktuellen Zahlen belegen andererseits, dass derartige Kontrollmaßnahmen durchaus geeignet sind, jegliche Straftaten außerhalb des engen lageabhängigen Kontrollanlasses festzustellen, die ansonsten nicht bzw. nur erschwert aufzuklären wären.

Es ist auf jeden Fall festzustellen, dass die lagebildabhängigen Kontrollen ein positives Echo bei der Bevölkerung hervorgerufen und eine subjektive Verstärkung des Sicherheitsgefühls zur Folge haben, so dass man diese Maßnahmen auf jeden Fall als Beitrag zur Stärkung der inneren Sicherheit werten kann.

Darüber hinaus wurde die Anweisung, wie die Anträge abzufassen sind, in keinem der Fälle beachtet: Einmal fehlte die Beschreibung des Umfanges der beabsichtigten Maßnahme, dann war in dem Antrag die erforderliche Darlegung der eingebundenen Dienstkräfte nicht enthalten, ein anderes Mal war der Bereich der Kontrollmaßnahme außerordentlich großzügig angegeben. Eine möglichst differenzierte Beschreibung des Bereiches der Kontrollmaßnahme ist nicht ersichtlich. Vielmehr entsteht der Eindruck einer großflächigen Kontrolle über mehrere Bezirke.

Die Kritik des BlnBDI an der Abfassung der Anträge nach § 18 Abs. 7 ASOG wird nicht geteilt. So wurden zur Erstellung der Anträge zwischenzeitlich angemessene und ausreichende Verfahrensrichtlinien erarbeitet, die es den Einsatzleitern der Polizei erlauben, jederzeit auf Lageveränderungen flexibel im Hinblick auf Personaleinsatz, Kontrollraum und Eingriffsvorgaben, z.B. hinsichtlich der zu kontrollierenden Fahrzeuge oder Personen, zu reagieren. Die vom BlnBDI genannten Kriterien werden bei der Antragsformulierung beachtet und sind in einem Musterantrag, der durch das LSA entworfen wurde, enthalten.

Die Senatsverwaltung für Inneres hat die Polizei erneut aufgefordert, die gesetzlichen und internen Vorgaben zu beachten. Eine Geschäftsordnung hält sie weiterhin für nicht erforderlich.

Polizeiberichte an alle

Die Polizei hat bei der Bekämpfung der Arzneimittelkriminalität Wohnungen von Tatverdächtigen durchsucht und dabei chemische Substanzen für die Herstellung der Partydroge „Liquid Extasy" beschlagnahmt. Ein Bericht darüber mit den personenbezogenen Daten der Beschuldigten mit zusätzlichen Informationen über die Droge und deren Herstellung wurde per Telefax an verschiedene Polizeidienststellen, die Staatsanwaltschaft, aber auch an sämtliche Bezirksämter (Gesundheitsämter und Veterinär- und Lebensmittelaufsichtsämter), die Senatsverwaltung für Gesundheit, das Landesamt für Arbeitsschutz, Gesundheit sowie technische Sicherheit sowie die Senatsverwaltung für Schule, Jugend und Sport versandt.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Die Information eines so großen Empfängerkreises wurde auf die Richtlinien für den Nachrichtenaustausch bei Umweltdelikten gestützt. Bei diesen Richtlinien handelt es sich allerdings nicht um eine besondere Rechtsvorschrift nach § 6 Abs. 1 Nr. 2 BlnDSG. Die Betroffenen dürften auch keine Einwilligung in diese Datenübermittlungen erteilt haben. Nach § 44 ASOG sind Datenübermittlungen zwar innerhalb des öffentlichen Bereiches zulässig. Eine Erforderlichkeit einer personenbezogenen Übermittlung ist aber nicht zu erkennen. Das bestätigt die Anfrage eines Gesundheitsamtes, das mit der Mitteilung nichts anzufangen wusste. Da das Landeskriminalamt die personenbezogene Übermittlung künftig nur noch auf die Polizei und Staatsanwaltschaft beschränken will, haben wir von einer Beanstandung abgesehen.

Die Darstellung des Berliner Beauftragten für Datenschutz und Informationsfreiheit bedarf insoweit der Klarstellung, als der Eindruck erweckt wird, bezüglich sämtlicher Empfänger sei die Erforderlichkeit einer Übermittlung personenbezogener Daten nicht zu erkennen. Der Senat hält im vorliegenden Fall jedenfalls die Übermittlung der persönlichen Daten der Beschuldigten an die Polizeidienststellen nach wie vor für erforderlich. Sowohl die Landeskriminalämter als auch das Bundeskriminalamt müssen zur Erfüllung ihrer Aufgaben bei der Gefahrenabwehr bzw. als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen über die Personen der Beschuldigten informiert sein.

Die Feststellung des BlnBDI, das Landeskriminalamt wolle künftig die personenbezogene Übermittlung auf die Polizei und die Staatsanwaltschaft beschränken, ist so nicht zutreffend. Wie dem BlnBDI mitgeteilt wurde, wird das Landeskriminalamt zukünftig in ähnlich gelagerten Fällen auf die Übermittlung personenbezogener Daten an andere Behörden als die Polizei und die Staatsanwaltschaft verzichten, sofern nicht die Prüfung im Einzelfall die Notwendigkeit einer personenbezogenen Übermittlung ergibt.

Gemeinsame Ermittlungsgruppe Graffity

Ein Bürger wurde durch Beamte des Bundesgrenzschutzes auf einem S-Bahnhof wegen des Verdachtes der Sachbeschädigung (Graffity-Sprayen) erkennungsdienstlich behandelt, obwohl zu diesem Zeitpunkt bereits aufgrund einer Zeugenaussage zweifelsfrei festgestanden haben soll, dass er nicht zu dem Personenkreis gehört, der bei der Sachbeschädigung beobachtet wurde.

Bei seiner Überprüfung bei dem Bundesgrenzschutz (BHS) hat der Bundesbeauftragte für den Datenschutz nicht nur festgestellt, dass der Sachverhalt zutreffend ist, sondern dass darüber hinaus die von der Gemeinsamen Ermittlungsgruppe Graffity erfassten Daten an die Berliner Polizei zur Datenspeicherung im ISVB weitergegeben wurden. An das Bundeskriminalamt sind die Daten der erkennungsdienstlichen Behandlung übermittelt worden.

Der Polizeipräsident in Berlin hat die Daten des Bürgers wieder gelöscht. Die Datenspeicherung hat er zunächst mit einer gemeinsamen Aufgabenwahrnehmung durch die Berliner Polizei und den BGS in der Gemeinsamen Ermittlungsgruppe Graffity gerechtfertigt. Dabei werden die gewonnenen Daten zu Vorgängen aus dem Zuständigkeitsbereich des BGS in das Berliner Polizeiliche Informationssystem eingestellt. Später hat er dann erklärt, dass der Bürger zu einem in der Zuständigkeit des BGS liegenden Vorgang erkennungsdienstlich behandelt wurde. Die Tatsache führte im Einzelfall zu einer Speicherung im ISVB und zur Aufnahme von Unterlagen in die kriminalpolizeiliche Personenakte.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Wir haben klargestellt, dass die Einrichtung einer Gemeinsamen Ermittlungsgruppe – bestehend aus Mitarbeitern verschiedener Polizeibehörden – nicht die Aufhebung der organisatorischen Trennung beider Polizeien mit den sich daraus ergebenden datenschutzrechtlichen Verantwortlichkeiten zur Folge haben darf. Gegen eine situationsbedingte ed-Behandlung durch die Berliner Polizei bei von dem BGS in eigener Zuständigkeit zu bearbeitenden Vorgängen haben wir keine grundsätzlichen datenschutzrechtlichen Einwände; das darf aber nicht zu Datenspeicherungen bei der Berliner Polizei führen. Dafür bietet das ASOG wegen der mangelnden eigenen Zuständigkeit des Polizeipräsidenten in Berlin keine Rechtsgrundlage.

Vorsorgliche Datenübermittlungen bei Beschimpfungen

Ein Bürger beschwerte sich darüber, dass die Polizei einer privat niedergelassenen Sozialarbeiterin und Berufsbetreuerin Auskunft über gegen ihn durchgeführte Ermittlungsverfahren erteilt habe.

Eine Auswertung der Protokollbänder ergab, dass mehrere Polizeibeamte auf den Datensatz des Bürgers zugegriffen haben. Diese mussten in dienstlichen Stellungnahmen den Grund für die Abfrage darlegen. Die Beamtin, die die Daten auch übermittelt hat, begründete den Abruf mit der Bearbeitung eines Vermissten-Vorganges. Der Vermisste stand unter Pflegschaft. Im Zuge der Ermittlungen wurde wiederholt mit der gesetzlichen Vertreterin, der Sozialarbeiterin und Berufsbetreuerin, wegen des möglichen Aufenthaltsortes telefoniert. Der Vermissten-Anzeige hat die Beamtin entnommen, dass der Vermisste die Betreuerin strikt ablehnt und statt dessen andere Personen – so auch den Petenten – vorgeschlagen hat. Bei diesen Personen handelte es sich um Zeugen und mögliche Wohnungsgeber des Vermissten. Die Beamtin hat die Daten abgefragt, um deren Wohnanschriften festzustellen. In einem der Telefonate mit der Sozialarbeiterin erklärte diese der Beamtin, dass sich der Bürger telefonisch als Vorsorgebetreuer des Vermissten vorgestellt und sie bedroht hätte. Eine Anzeige hat sie nicht erstattet. Auf Nachfragen der Beamtin wurde die Bedrohung in „Beschimpfungen übelster Art“ relativiert. Dennoch sah die Beamtin in dem Auftreten des Bürgers eine aktuelle Gefährdung der Betreuerin, die sie veranlasste, vorsorglich – als Vorsichtsmaßnahme zum eigenen Schutz – auf die früheren Ermittlungsverfahren hinzuweisen.

Die Polizei darf personenbezogene Daten an Private übermitteln, wenn das zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer Person erforderlich ist (§ 45 Abs. 1 Nr. 3 ASOG). Eine Datenübermittlung kommt danach immer dann in Betracht, wenn ein besonders umfangreicher Schaden immaterieller Rechtsgüter (beispielsweise Leben, Gesundheit oder Freiheit) oder materieller Werte (beispielsweise Eigentum, Besitz und Vermögen) zu besorgen ist. Das ist z. B. dann der Fall, wenn die Polizei erfährt, dass ein Gewalttäter wieder in Freiheit kommt, der in einer

In dem konkreten Fall war die Sachbearbeiterin der Vermisstenstelle aufgrund des geschilderten Verhaltens des Petenten von einer aktuellen Gefährdung gewichtiger Rechtsgüter der Betreuerin überzeugt, was sie veranlasste, sie vorsorglich darauf hinzuweisen, dass gegen den Petenten bereits Ermittlungen wegen Hausfriedensbruchs anhängig waren. Vor dem Hintergrund dieses Wissens hat sie das zunächst als „Bedrohung“ und erst später als „Beschimpfungen übelster Art“ bezeichnete Verhalten des Petenten als Gefährdung für die Betreuerin interpretiert. Die Übermittlung dieser Information geschah ausschließlich als Vorsichtsmaßnahme zum persönlichen Schutz der Betreuerin im Hinblick auf deren Amtsstellung und die besondere Gefährdungssituation, der sie in ihrem Tätigkeitsbereich zu dieser Zeit ausgesetzt war. Gleichzeitig bat die Beamtin die Betreuerin, diese Information für sich zu behalten.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Justizvollzugsanstalt einsaß und stets davon sprach, nach Freilassung seinen verräterischen Tatgenossen, der bei der Verurteilung glimpflicher als er davongekommen ist, bei nächstbester Gelegenheit „krankenhausreif“ schlagen zu wollen. Weil es bei der Beschimpfung an einer besonders schweren Rechtsbeeinträchtigung mangelt, war die Datenübermittlung unzulässig.

Anlasslose DNA-Analyse aller Männer

Nach dem Mord eines Kindes in Brandenburg wurde bundesweit erneut über Massengentests diskutiert. Nicht selten werden in Mordfällen ganze Hausgemeinschaften zum DNA-Test aufgefordert. Massentests wie im Fall eines 1998 in Niedersachsen vergewaltigten und ermordeten Kindes gab es in Berlin allerdings nicht. Damals wurden 16.000 Proben von Männern der Umgebung entnommen worden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder[69] hat den Vorschlag, den genetischen Fingerabdruck aller Männer zu erheben und rein vorsorglich zu speichern, entschieden zurückgewiesen. Eine Datenerhebung auf Vorrat – auch oder gerade zur Strafverfolgung –, die die Hälfte der Bevölkerung als potenzielle Straftäter behandelt, ist verfassungsrechtlich unzulässig.

4.1.3 Nachrichtendienste

Novellierung des G 10-Gesetzes

Das Bundesverfassungsgericht hatte in seiner Entscheidung vom 14. Juli 1999[70] die Erweiterung der Regelungen über die strategische Fernmeldekontrolle im Verbrechensbekämpfungsgesetz zwar für grundsätzlich verfassungsgemäß erklärt, jedoch einige Einzelbestimmungen des Gesetzes zu Art. 10 GG (G 10-Gesetz) beanstandet und dem Gesetzgeber zur Herstellung des verfassungsgemäßen Zustandes eine Frist bis zum 30. Juni 2001 gesetzt[71].

Entsprechend den Vorgaben des Verfassungsgerichtes wurden die Pflichten bei dem Umgang mit personenbezogenen Daten durch die Novelle verschärft und die parlamentarische Kontrolle verbessert, andererseits jedoch Eingriffe in Bürgerrechte vertieft[72].

So wurden die Befugnisse der Geheimdienste zum Abhören von Telefonaten erweitert. Sie dürfen nunmehr auch bei Straftaten wie Volksverhetzung, erpresserischem Menschenraub, Sprengstoffanschlägen, Geiselnahme von Deutschen im Ausland sowie schweren Eingriffen in die Verkehrssicherheit Verdächtige abhören, sofern sich diese Delikte gegen die freiheitlich-demokratische Grundordnung oder die Sicherheit von Bund und Ländern richtet. Die dabei gewonnenen

Derzeit erfolgt die Änderung des Gesetzes zur Ausführung des Gesetzes zu Artikel 10 Grundgesetz entsprechend der Novellierung des Gesetzes des Brief-, Post- und Fernmeldeverkehrs des Bundes.

[69] vgl. Anlagenband, a.a.O., I.2
[70] BVerfGE 100, S. 313 ff.
[71] JB 1999, 4.1.1
[72] Gesetz zur Neuregelung von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses vom 26. Juni 2001, BGBl. S. 1254 ff.

Daten können auch bei Verbotsverfahren verfassungswidriger Parteien genutzt werden. Bei Verdacht auf terroristische Gewalttaten ist die Kontrolle von Telefonaten, E-Mails und des konventionellen Briefverkehrs Einzelner durch die neuen Vorschriften zulässig.

Die Befugnisse des Bundesnachrichtendienstes zu „strategischen Beschränkungen“ der internationalen Telekommunikationsbeziehungen wurden auf alle „gebündelten Übertragungen“, also auch auf feste Leitungen, ausgeweitet.

Die Datenschutzbeauftragten des Bundes und der Länder hatten zuvor in ihrer Entschließung der 61. Konferenz am 8./9. März 2001 umfangreiche Kritik an dem Gesetzesvorhaben geäußert, die jedoch keinen wesentlichen Niederschlag auf das Verfahrensergebnis fand[73].

Positiv hervorzuheben ist lediglich die Erweiterung der Befugnisse des Parlamentarischen Kontrollgremiums (G 10-Kommission) und die damit verbundene Aufwertung seiner Bedeutung.

In einem Entschließungsantrag der Koalition ist festgehalten worden, dass die Bundesregierung dem Parlament nach zwei Jahren einen Bericht über die Erfahrungen mit der Novellierung des Gesetzes vorlegen soll.

Berliner Verfassungsschutz

Die Umorganisation der Berliner Verfassungsschutzbehörde[74] wurde im Berichtszeitraum weitgehend abgeschlossen. Datenschutzrechtliche Problemstellungen sind nicht in Erscheinung getreten, die Beratung konzentrierte sich auf die Einführung neuer informationstechnischer Verfahren[75]. Die Koordinationsgespräche wurden fortgesetzt.

4.2 Ordnungsverwaltung

4.2.1 Melde- und Personenstandswesen

Der Regierungsentwurf eines Dritten Gesetzes zur Änderung des Melderechtsrahmengesetzes[76] ist in den Bundestag eingebracht. Gegenüber dem Arbeitsentwurf wurde zumindest eine Widerspruchsmöglichkeit für Melderegisterauskünfte per Internet geschaffen. Weiterhin haben sich die betroffenen Meldebehörden bei der Einrichtung und Aufhebung von Auskunftssperren gegenseitig zu unterrichten, und von der ursprünglichen Absicht der gemeinsamen Nutzung der Melderegister mehrerer Meldebehörden zur Unterstützung melderechtlicher Aufgaben wurde Abstand genommen.

Die Sachdarstellung des Berliner Beauftragten für Datenschutz und Informationsfreiheit in Bezug auf das Dritte Gesetz zur Änderung des Melderechtsrahmengesetzes, das zum Ziel hat, im Rahmen einer umfassenden Änderung bisheriger melderechtlicher Regelungen die erforderlichen Rahmenbedingungen für die Nutzung moderner Informations- und Kommunikationstechnologien zu schaffen und vom Bürger als unnötig empfundene Meldepflichten abzuschaffen, ist zutreffend. Der Deutsche Bundestag hat das Gesetz am 25. März 2002 verabschiedet.

[73] vgl. Anlagenband, a.a.O., I.1
[74] JB 2000, 2.1.1
[75] vgl. 2.2
[76] JB 2000, 4.2.1

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Keine Berücksichtigung fanden die Forderungen in der Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder[77]

- zur Aufweichung der generellen Auskunftssperre zugunsten einer Risikoabwägung im Einzelfall,
- zur Abschaffung der Hotelmeldepflicht,
- bei der Weitergabe der Meldedaten an die politischen Parteien zum Zweck der Wahlwerbung die Widerspruchs- durch eine Einwilligungslösung zu ersetzen und
- auch bei Datenübermittlungen innerhalb des öffentlichen Bereiches zumindest Verfahren der fortgeschrittenen elektronischen Signatur gemäß den Regelungen des Signaturgesetzes einzusetzen.

Leider wird trotz der überzeugenden Begründung im Arbeitsentwurf auf die Abschaffung der erweiterten Melderegisterauskunft aufgrund eines berechtigten zugunsten eines rechtlichen Interesses verzichtet. Auch das Akteneinsichtsrecht für die in Akten gespeicherten Daten und Hinweise wurde nicht übernommen.

LEA arbeitet immer noch mit DDR-Daten

Wir hatten darüber berichtet, dass nach Ablauf von fast zehn Jahren deutscher Einheit noch immer nicht alle Meldestellen mit einem Online-Anschluss für das EWW-System ausgestattet sind[78]. Das Ziel ist im August 2000 endlich erreicht worden. Wir haben nun geprüft, ob die Meldekarteikarten aus DDR-Zeiten folgerichtig dem Zugriff der Meldebehörde entzogen wurden.

Die auf den Meldestellen im Ostteil der Stadt geführten Hauskarteien sind nach und nach mit dem Online-Anschluss an das EWW-System aus den Räumen der Meldestelle ausgelagert und weiter im dortigen Keller gelagert worden. Ende 2000 sind die in den Kellern der jeweiligen Ost-Meldestelle lagernden Hauskarteien zentral im Archiv des Landeseinwohneramtes zusammengefasst worden. Das Archiv bewahrt die Haupt- und Nebenkartei, die Kartei der Republik-Flüchtlinge und die Kartei der Rückkehrer sowie die West-Alt-Kartei auf. Die Kartei der Republik-Flüchtlinge und die der Rückkehrer enthalten über die Stadtgrenze hinausgehend offensichtlich sämtliche DDR-Flüchtlinge und Rückkehrer. Daneben existiert noch die verfilmte Kartei auf Filmrollen; hier sind die Karteikarten nach nicht mehr nachvollziehbaren Kriterien verfilmt worden. Der Datenbestand ist vollständig. Teilweise hat das Landesarchiv Filmrollen abgeholt. Die Ost-Karteien enthalten die bekannten melderechtsfremden Daten (beispielsweise PKZ, Wehrdienst, Haft, Ein- und Ausreisen). Die so genannte West-Alt-Kartei wurde bis Anfang der 80er Jahre parallel zu dem automatisierten Verfahren EWW geführt. Die Karteikarten der vor 1961 Verstorbenen oder Verzogenen befinden sich bei dem Landesarchiv.

Die Sachdarstellung des Berliner Beauftragten für Datenschutz und Informationsfreiheit über die Historie der im Ostteil der Stadt geführten Hauskarteien ist zutreffend. Nachdem nunmehr alle im Ostteil der Stadt gelegenen Meldestellen einen Online-Anschluss an das EWW-System erhalten haben, hat sich die Angelegenheit erledigt.

Der Senat legt in diesem Zusammenhang Wert auf die Feststellung, dass für die Zeit der aus technischen Gründen bedingten weiteren Nutzung der alten Hauskarteien sichergestellt war, dass die in den Karteien enthaltenen Daten nur im gesetzlich zulässigen Umfang genutzt wurden. Auf eine Bereinigung der Kartei und die Reduzierung des lesbaren Datenbestands auf die melderechtlich zu nutzenden Daten wurde aus verwaltungsökonomischen Gründen verzichtet.

Die Karteien „Republikflüchtige“ und „Rückkehrer“ wurden 1990 im Archivbereich des Landeseinwohnerramtes untergestellt. Eine Nutzung der Daten erfolgte nicht. Die Daten werden dem Landesarchiv Berlin voraussichtlich im Mai 2002 übergeben werden.

Die vom Berliner Beauftragten für Datenschutz und Informationsfreiheit in diesem Zusammenhang kriti-

[77] Entschließung zu „Novellierung des Melderechtsrahmengesetzes“. In: Anlagenband, a.a.O, I.1
[78] JB 1999, 4.2.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Die Löschungsfrist (§ 10 Abs. 4 MeldeG) ist für die Daten derjenigen, die länger als 30 Jahre verstorben oder aus Berlin weg- und nicht wieder zugezogen sind, verstrichen. Das Archiv hat bisher Auskunft über alle Datenbestände erteilt, die vorhanden sind. Die zeitliche Begrenzung hat dabei bisher keine Rolle gespielt. Eingehende Anfragen wurden drei Monate aufbewahrt und danach vernichtet. Das gilt auch für die Auskünfte, die über den Umfang einer einfachen Melderegisterauskunft (§ 28 Abs. 1 MeldeG) hinausgehen.

Das Landeseinwohneramt hat uns mitgeteilt, dass es für die melderechtsfremden Daten dem Grunde nach keine Verwendung hat und diese auch nicht weitergegeben wurden. Nach dem Einigungsvertrag sind die PKZ in allen Dateien zum frühestmöglichen Zeitpunkt zu löschen. Der Katalog der Daten, die die Meldebehörde speichern darf, ist abschließend in § 2 MeldeG festgelegt. Die in den Ost-Karteien über diesen Katalog hinausgehenden Daten werden daher unzulässigerweise gespeichert. Nachdem die Datenbestände aus dem Verwaltungsvollzug genommen und in das Archiv des Landeseinwohneramtes eingestellt wurden, ist die Forderung nach Schwärzung nicht mehr sachgerecht; es ist aber in geeigneter Weise sicherzustellen, dass diese Daten auch nicht ausnahmsweise für die im Gesetz genannten Zwecke (§ 10 Abs. 3 MeldeG) genutzt werden. Dazu hat das Landeseinwohneramt eine Geschäftsanweisung erlassen. Für das Führen oder eine weitere Aufbewahrung der Kartei der DDR-Republik-Flüchtlinge und der Rückkehrer existiert keine Rechtsgrundlage. Diese Karteien wurden dem Bundesarchiv und dem Landesarchiv angeboten. Das Landesarchiv will die Bestände übernehmen.

Die Löschung von Meldedaten ist in zwei Schritten zu vollziehen: Nach Ablauf von fünf Jahren nach dem Ende des Jahres des Wegzuges und der Auswertung der Rückmeldung oder des Todes des Einwohners sind die ersten Daten (§ 2 Abs. 1 Nr. 10 und § 2 Abs. 2 Nr. 1 a, 2, 5, 8 und 10 MeldeG) zu löschen und die übrigen gesondert aufzubewahren und durch technische und organisatorische Maßnahmen besonders zu sichern. Sie dürfen dann nur noch verarbeitet oder sonst genutzt werden, wenn dies zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot, zur rechtmäßigen Aufgabenerfüllung der Sicherheitsbehörden oder für Wahlzwecke unerlässlich ist oder wenn der Betroffene schriftlich eingewilligt hat. 30 Jahre nach dem Ende des Jahres des Wegzuges und der Auswertung der Rückmeldung oder des Todes des Einwohners sind auch die zu diesem Zeitpunkt noch gespeicherten Daten und Hinweise zu löschen. Somit sind die so genannten Archiv-Auskünfte nur in dem Zeitraum nach Ablauf von fünf bis 30 Jahren nach dem Ende des Jahres, in dem das Ereignis eingetreten ist, ausschließlich zu dem oben genannten Zweck zulässig. Auch das hat das LEA in einer Geschäftsanweisung geregelt.

Nach der Übergangsvorschrift des § 32 Abs. 3 MeldeG müssen diese Karteikarten nicht dem Landesarchiv sierte dreimonatige Aufbewahrung von Unterlagen, die Archivauskünfte betreffen, hat das Landeseinwohneramt in der in dem Jahresbericht erwähnten neuen Geschäftsanweisung auf zwei Jahre verlängert, so dass dem Petitum des Datenschutzbeauftragten nachgekommen ist.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

angeboten werden. Das LEA hat sicherzustellen, dass nach Ablauf von mehr als 30 Jahren nach Ablauf des Jahres des Eintritts des Ereignisses die Daten nach dem Melderecht nicht mehr genutzt – also auch keine Auskünfte an Dritte mehr erteilt oder die Daten an andere Behörden übermittelt – werden. Eine weitere Nutzung würde sich in diesem Fall ausschließlich nach dem Archivrecht richten.

Mit der nur dreimonatigen Aufbewahrung der Unterlagen wird das Auskunftsrecht des Betroffenen verkürzt. Er kann nicht nur Auskunft über die zu seiner Person gespeicherten Daten, sondern auch über die Empfänger von Übermittlungen der letzten zwei Jahre erhalten. Das Verfahren ist in der Geschäftsanweisung ebenfalls neu geregelt worden. Danach beträgt die Aufbewahrungsfrist jetzt die gesetzlich vorgeschriebenen zwei Jahre.

Nichts Neues beim Meldegesetz

Die Novellierung des Berliner Meldegesetzes hat sich zu einer ständigen Rubrik in den Jahresberichten entwickelt[79]. Der immer wieder angemahnte Entwurf zur Novellierung des Gesetzes liegt trotz zweier Beschlüsse des Abgeordnetenhauses[80] noch immer nicht vor. Somit sind das Erste und Zweite Melderechtsrahmenänderungsgesetz von 1994 und 2000 noch immer nicht in Landesrecht umgesetzt. Berlin bildet weiter das Schlusslicht im Meldewesen.

Stattdessen sind die Überlegungen über die Erweiterung der Online-Zugriffsberechtigungen auf das Melderegister weitergegangen[81]. Der Kreis soll um die Finanzbehörden sowie die Gerichte, Staats- und Amtsanwaltschaften erweitert werden.

Auch die BVG hat um die Unterstützung bei der Einrichtung eines direkten Zugriffes gebeten. Durch die Abfrage der Meldedaten soll eine Identitätsfeststellung der Fahrgäste vorgenommen werden, die ohne gültigen Fahrausweis angetroffen werden und keine Personaldokumente vorlegen können. Damit soll die Warte- und Bearbeitungszeit verkürzt werden, weil es regelmäßig einige Zeit dauert, bis die BVG-Mitarbeiter die Daten im Rahmen einer telefonischen Abfrage beim Dauerdienst der Meldebehörde erhalten.

Der Senat hat die Gründe, die zu einer Verzögerung der Novellierung des Berliner Meldegesetzes geführt haben, bereits in seiner Stellungnahme zum letztjährigen Jahresbericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit dargelegt. Im letzten Jahr konnten dann die Vorarbeiten für eine umfassende Novellierung des Melderechtsrahmengesetzes auf Bundesebene weitgehend abgeschlossen werden. Das Gesetz wurde am 25. März 2002 vom Deutschen Bundestag verabschiedet, so dass die damit verbundenen Änderungen nunmehr in der vom BlnBDI angemahnten Novellierung des Berliner Landesrechts mitberücksichtigt werden können.

Die vom BlnBDI angeführten Überlegungen über die Erweiterung der Online-Zugriffsberechtigungen auf das Melderegister sind zutreffend.

Personenstandswesen

Der Presse sind häufig bestürzende Berichte über geheime Geburten, Aussetzung oder gar Tötung von Neugeborenen zu entnehmen. Ursachen sind häufig Scham, Angst, aber auch Unkenntnis der Mütter über bestehende Handlungsmöglichkeiten. Die Schwangeren-Beratungsstellen sind gesetzlich (§ 17 Abs. 1 Nr. 4 Personenstandsgesetz - PStG) zur Anzeige einer Geburt verpflichtet. Dadurch wird in bestimmten Fällen eine effektive Beratung verhindert, weil die Mütter mit ihren Fragen und Problemen die Stellen nicht aufsuchen.

Auf Bundesebene besteht weitgehend Einvernehmen darüber, dass die Möglichkeit der anonymen Geburt gesetzlich geregelt werden soll.

Der Gesetzesentwurf zur sogenannten anonymen Geburt betraf – soweit es um die bisher vorgesehene Umsetzung im personenstandsrechtlichen Bereich geht – keine datenschutzrechtlichen Belange

Der benannte Entwurf ist jedoch zwischenzeitlich zugunsten eines zu dieser Thematik gebildeten interfraktionellen Arbeitskreises zurückgezogen worden. Der

[79] JB 2000, 4.2.1; JB 1999, 4.2.2; JB 1998, 4.2.2
[80] Abghs.-Drs. 13/ 3840. In: JB 1999, Anlage 2; Abghs.-Drs. 14/1462
[81] JB 1999, 4.2.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Damit Mütter in einer Konfliktsituation sich von einer geheimen Geburt und von der Aussetzung oder sogar Tötung ihres Neugeborenen abhalten lassen und an eine besonders dafür geeignete Schwangeren-Beratungsstelle wenden, gleichzeitig aber zunächst anonym bleiben können, hat die CDU/CSU-Fraktion einen Entwurf zur Änderung des PStG in den Deutschen Bundestag mit dem Ziel eingebracht, die Frist für die Anzeige zu verlängern. Die Schwangeren-Beratungsstellen haben dadurch Zeit, auf die Lösung der Konflikte der Mutter hinzuwirken und heimliche Geburten zu verhindern.

Nach In-Kraft-Treten des Lebenspartnerschaftsgesetzes[82] können gleichgeschlechtliche Lebenspartner eine amtlich eingetragene Lebenspartnerschaft eingehen. Mit dem Gesetz wurden über 60 Gesetze und Verordnungen geändert. So sind sich die Lebenspartner beispielsweise einander wie Eheleute zum Unterhalt verpflichtet, sie können einen gemeinsamen Namen wählen, sie müssen erklären, dass sie den Vermögensstand der Ausgleichsgemeinschaft vereinbart oder einen Lebenspartnerschaftsvertrag abgeschlossen haben, Lebenspartner und ihre Kinder werden in der Familienversicherung für die Krankenversicherung einbezogen, wenn sie kein eigenes Einkommen haben, auch bei der Pflegeversicherung gibt es künftig eine Mitversicherung. Darüber hinaus wird Lebenspartnerschaften ein umfangreiches Zeugnisverweigerungsrecht zugestanden.

Ein Ergänzungsgesetz zur Lebenspartnerschaft soll darüber hinaus eine Reihe von Verfahrensregelungen sowie zusätzliche Rechte und Pflichten enthalten, die der Zustimmung des Bundesrates bedürfen.

Das Abgeordnetenhaus von Berlin hat ein Gesetz zur Ausführung des Lebenspartnerschaftsgesetzes[83] verabschiedet. Danach sind die Standesämter für die Entgegennahme der Anträge zuständig und führen das Lebenspartnerschaftsbuch.

Arbeitskreis bringt einen gemeinsamen Antrag in den Deutschen Bundestag ein, um die gesetzlichen Bestimmungen abzuändern.

Der Senat begrüßt das Vorgehen des interfraktionellen Arbeitskreises, sämtliche infrage kommenden Regelungen im Personenstandsgesetz aufzunehmen.

4.2.2 Straßen- und Verkehrsverwaltung

Autobahnmaut

Bereits im Jahre 1995 haben wir ausführlich über Vorhaben berichtet, automatisierte Systeme zur Ermittlung und Abführung von Autobahngebühren einzuführen[84]. In jenem Jahr wurde auf der Autobahn A 555 zwischen Bonn und Köln ein Feldversuch mit verschiedenen technischen Lösungen zur Erfassung von Autobahngebühren durchgeführt. Das Ergebnis war, dass die automatische Erfassung der Autobahnmaut für Personenkraftwagen nicht eingeführt werden soll, obwohl auch prinzipiell datenschutzfreundliche Lösungen im Versuch erprobt wurden, und dass nur die Einführung des Autobahngebührenerfassungssystems für Lastkraftwagen von mindestens 12 Tonnen zulässigen Gesamtgewichts in Erwägung gezogen werden sollte.

[82] BGBl. 2001 I Nr. 9, S. 266 ff.
[83] GVBl. Nr. 27 vom 17. Juli 2001
[84] JB 1995, 3.3

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Danach war das Projekt über mehrere Jahre nicht mehr im Gespräch. Erst im Berichtsjahr wurde das Thema wieder aufgegriffen. Am 15. August 2001 beschloss das Bundeskabinett einen Gesetzentwurf zur Einführung eines solchen Mautsystems, mit dem u. a. ein automatisches System zur streckenbezogenen Autobahnmaut für Lastkraftwagen erhoben werden soll. Da das System das Satellitennavigationssystem GPS zur Ortung und die Mobilfunktelefonie zur Weiterleitung der Ortungsdaten verwenden soll, kommt es völlig ohne stationäre Erfassungssysteme aus.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die Bundesregierung aufgefordert, bei diesem Vorgehen, das technologisch auch auf Bundesstraßen und Personenkraftwagen ausgedehnt werden könnte, auch die datenschutzrechtlichen Anforderungen durchzusetzen, die im Wesentlichen auf dem Gebot der Datensparsamkeit beruhen, um die Schaffung differenzierter Bewegungsprofile über die Verkehrsteilnehmer zu verhindern[85].

Der Deutsche Bundestag hat in seiner 228. Sitzung am 22. März 2002 die vom Vermittlungsausschuss empfohlene Beschlussfassung zu dem Gesetz zur Einführung von streckenbezogenen Gebühren für die Benutzung von Bundesautobahnen mit schweren Nutzfahrzeugen angenommen. Der Anwendungsbereich des Gesetzes beschränkt sich auf die Regelung der Benutzung der Bundesautobahnen durch schwere Nutzfahrzeuge ab 12 Tonnen zulässigen Gesamtgewichts, so dass eine praktische Ausdehnung auf Bundesstraßen mit den Ortsdurchfahrten und Personenkraftwagen rechtlich nicht möglich ist.

In dem Gesetz sind datenschutzrechtliche Anforderungen beachtet. Es sieht die Erhebung, Verarbeitung und Nutzung von Daten durch den Betreiber vor. Insbesondere dürfen Daten über die Höhe der entrichteten Maut, die Strecke, für die die Maut entrichtet wurde, Ort und Zeit der Mautentrichtung und weitere für die Mauthöhe maßgebliche Merkmale ausschließlich zum Zwecke der Ausführung des Gesetzes verarbeitet und genutzt werden. Die zwingende Löschung von Daten ist ebenfalls geregelt.

Die Einzelheiten des Verfahrens der Erhebung der Maut sind einer Rechtsverordnung der Bundesregierung vorbehalten, so dass insofern noch abgewartet werden muss.

Parkerleichterungen aus gesundheitlichen Gründen

In Berlin wurde in den vergangenen Jahren in mehreren Bezirken eine Parkraumbewirtschaftung eingeführt. Das Parken in den betroffenen Bereichen ist grundsätzlich gebührenpflichtig. Personen, die aus gesundheitlichen Gründen auf die Benutzung eines Pkw angewiesen sind, können jedoch nach § 46 Abs. 1 Nr. 11 Straßenverkehrsordnung (StVO) für das Parken ohne Anwohnerparkausweis oder gebührenpflichtigen Parkschein eine Ausnahmegenehmigung bei der Straßenverkehrsbehörde beantragen. Der entsprechende Antrag einer Bürgerin wurde von dem Polizeipräsidenten in Berlin als unvollständig zurückgewiesen, da das von ihr eingereichte ärztliche Attest keine Angaben über die genaue Diagnose ihres Krankheitsbildes enthielt.

Es gibt keinen Rechtsanspruch auf eine Ausnahmegenehmigung nach § 46 Abs. 1 Nr. 11 StVO. Die Ertei-

[85] vgl. Entschließung der 62. Konferenz zu „LKW-Maut auf Autobahnen und allgemeine Maut auf privat errichteten Bundesfernstraßen“. In: Anlagenband, a.a.O., I.3

lung oder Versagung einer entsprechenden Genehmigung ist von der zuständigen Ordnungsbehörde als Ermessensentscheidung zu treffen. Im Rahmen der Ermessensausübung kann der Polizeipräsident in Berlin den Antragsteller zur Klärung des Sachverhaltes befragen und personenbezogene Daten erheben, soweit das zur Erfüllung seiner Aufgaben erforderlich ist (§ 18 ASOG).

Eingeschränkt wird diese Erhebungsbefugnis des Polizeipräsidenten in Berlin durch § 6 a BlnDSG. Danach ist die Verarbeitung von personenbezogenen Daten, die die Gesundheit betreffen, nur zulässig, wenn angemessene Garantien zum Schutz des Rechtes auf informationelle Selbstbestimmung bestehen und eine besondere Rechtsvorschrift, die den Zweck der Verarbeitung bestimmt, dies erlaubt (§ 6 a Abs. 1 BlnDSG) oder wenn der Betroffene in die Verarbeitung seiner Daten ausdrücklich eingewilligt hat (§ 6 a Abs. 2 BlnDSG).

Keine der genannten Voraussetzungen ist hier gegeben. Insbesondere existiert keine Rechtsvorschrift, die es dem Polizeipräsidenten in Berlin erlaubt, von dem Antragsteller im Antragsverfahren auf Ausnahmegenehmigung nach § 46 Abs. 1 Nr. 11 StVO ein fachärztliches Attest mit konkreten Angaben zum Krankheitsbild (Diagnose) einzufordern. Ausreichend und zulässig ist, wenn das ärztliche Gutachten allgemein bestätigt, dass die Benutzung des Pkw aus „gesundheitlichen Gründen“ erforderlich ist.

Der Polizeipräsident in Berlin ist unserer Empfehlung gefolgt und hat das Verfahren den datenschutzrechtlichen Anforderungen angepasst. Für eine Ausnahmegenehmigung nach § 46 Abs. 1 Nr. 11 StVO ist es zukünftig ausreichend, wenn der Antragsteller ein ärztliches Attest beibringt, welches ihm bescheinigt, dass die „Nutzung öffentlicher Verkehrsmittel gesundheitsbedingt nicht möglich ist“. Von der Pflicht, eine fachärztliche Diagnose anzugeben, wird in Zukunft abgesehen.

Um die Mobilität von Bürgerinnen und Bürgern mit bestimmten gesundheitlichen Beeinträchtigungen zu verbessern, haben die Senatsverwaltungen für Arbeit, Soziales und Frauen sowie für Stadtentwicklung beschlossen, den Kreis derjenigen zu erweitern, die über eine Genehmigung für Sonderparkplätze verfügen. Der Antrag auf Ausnahmegenehmigung, dem eine Bescheinigung über die Gesundheitsbeeinträchtigung des Landesamtes für Gesundheit und Soziales – Versorgungsamt – beizufügen ist, ist an den Polizeipräsidenten in Berlin zu richten. Eine Bürgerin, die ihrem Antrag lediglich eine Kopie ihres Schwerbehindertenausweises beigefügt hatte, war erstaunt, als der Polizeipräsident in Berlin mitteilte, er habe die Angelegenheit zur Prüfung an das Versorgungsamt übersandt.

Gesetzliche Grundlage für die Erweiterung des Kreises von Antragsberechtigten für eine Ausnahmegenehmigung ist § 46 Abs. 2 Satz 1 StVO. Danach können die genannten Senatsverwaltungen die Voraussetzungen bestimmen, nach denen nicht nur die durch § 46 Abs. 1

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Nr. 11 StVO berechtigten Schwerbehinderten mit außergewöhnlicher Gehbehinderung und Blinde, sondern auch Antragsteller mit einem geringeren Grad einer Gesundheitsbeeinträchtigung eine Ausnahmegenehmigung erhalten können. Die Datenerhebungsbefugnis für die zuständige Ordnungsbehörde ergibt sich auch hier aus § 18 ASOG.

Da im Antragsverfahren Daten über die Gesundheit des Antragstellers verarbeitet werden, ist eine Übermittlung der Antragsdaten – z. B. zur weiteren Prüfung der Voraussetzungen – an das Versorgungsamt nach § 6 a BlnDSG nur aufgrund einer Rechtsgrundlage oder mit Einwilligung des Antragstellers zulässig. Die genannten Voraussetzungen lagen im Fall der Antragstellerin nicht vor. Es gibt weder eine Rechtsgrundlage, auf die die Weiterleitung der Angelegenheit an das Versorgungsamt gestützt werden könnte, noch hat die Betroffene in die Datenübermittlung eingewilligt.

Wir haben empfohlen, dass die Antragsteller von dem Polizeipräsidenten in Berlin vor einer Weiterleitung der Angelegenheit an das Versorgungsamt ausführlich und schriftlich über das Verfahren und die Voraussetzungen für eine Ausnahmegenehmigung informiert werden. Insbesondere sind die Betroffenen darauf hinzuweisen, dass sie die erforderliche Bescheinigung über die Gesundheitsbeeinträchtigung selbst vom Versorgungsamt erhalten können. Die Übermittlung von Unterlagen aus dem Antragsverfahren an das Versorgungsamt darf nur mit ausdrücklicher Einwilligung des Betroffenen (vgl. § 6 a Abs. 2 Satz 1 BlnDSG) erfolgen.

Gemäß den getroffenen Verfahrensvereinbarungen sind die möglichen Anträge auf Parkerleichterungen für besondere Gruppen schwerbehinderter Menschen direkt bei dem für derartige Ausnahmegenehmigungen zuständigen Polizeipräsidenten in Berlin - LPVA III A – zu stellen. Dieser allein trifft eine Entscheidung auf der Basis des Straßenverkehrsrechts und der im Wege der Amtshilfe zur Vorlage bei ihm ausgestellten Bescheinigung des Versorgungsamtes. Nur die Entscheidung des Polizeipräsidenten stellt einen anfechtbaren Verwaltungsakt dar, nicht aber die lediglich im Binnenverhältnis erstellte Bescheinigung des Versorgungsamtes.

Entsprechend der vom Berliner Beauftragten für Datenschutz und Informationsfreiheit zu dieser Problematik abschließend geäußerten Empfehlung hat die Straßenverkehrsbehörde ein neues Antragsformular entwickelt.

Das vom BlnBDI genannte Problem betrifft im übrigen nur noch diejenigen schwerbehinderten Menschen, bei deren Feststellungsverfahren nach dem damaligen, inzwischen durch entsprechende Bestimmungen des Sozialgesetzbuch IX abgelösten Schwerbehindertengesetz noch nicht das Vorliegen der gesundheitlichen Voraussetzungen für die neuen zusätzlichen Regelungen zur Genehmigung von Parkerleichterungen geprüft werden konnte. Bei sämtlichen Erst- und Neufeststellungsanträgen seit September 2001 überprüft der Ärztliche Dienst des Versorgungsamtes von sich aus die Zugehörigkeit zu den vier abschließend aufgezählten Personengruppen. Im positiven Fall führt dies zu einer Ausstellung der Bescheinigung zur Vorlage beim Polizeipräsidenten zusammen mit dem Feststellungsbescheid des Versorgungsamtes.

Abgleich von Sozialdaten mit dem Kraftfahrzeugregister

Vom Landeseinwohneramt Berlin wurden wir darüber informiert, dass zusammen mit der Senatsverwaltung für Arbeit, Soziales und Frauen ein Verfahren entwickelt worden ist, in dem monatlich alle Sozialhilfe-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

empfänger, die älter als 18 Jahre sind, gegen den Datenbestand im Fahrzeugregister der Zulassungsstelle abgeglichen werden sollen. Dabei stellte sich die Frage, ob die sehr aufwendige Protokollierung der damit einhergehenden Datenübermittlungen an die Sozialbehörden (nach Angaben des Landeseinwohneramtes ca. 8,4 Millionen Protokollsätze in einem Zweijahreszeitraum) entfallen und durch andere Maßnahmen, die dem Auskunftsanspruch des Betroffenen genügen, ersetzt werden könnte.

Der regelmäßige, automatisierte Datenabgleich zwischen den Datenbeständen der Sozialämter und denen der örtlichen Fahrzeugregister zur Feststellung der „Eigenschaft als Kraftfahrzeugführer“ ist nach § 117 Abs. 3 Satz 3 Bundessozialhilfegesetz (BSHG) zulässig. Daraus ergibt sich nicht die Berechtigung für eine Online-Anbindung der Sozialämter an das örtliche Fahrzeugregister zum Zweck des einzelfallbezogenen automatisierten Abrufes. Die Regelung des § 117 Abs. 3 Satz 3 BSHG gestattet nur, die Datenbestände der Sozialämter und der Kfz-Zulassungsstelle bei dem Landeseinwohneramt miteinander abzugleichen, die Fälle, in denen eine Übereinstimmung festgestellt wird („Treffer“), aufzulisten und dem zuständigen Sozialamt mitzuteilen. Nach Durchführung des Abgleiches und Vorlage der „Treffer“ sind die vom Sozialamt übermittelten Daten nach § 117 Abs. 3 Satz 6 BSHG unverzüglich bei der Kraftfahrzeugzulassungsstelle zu löschen. Daraus ergibt sich, dass nach Übermittlung der „Trefferliste“ an die Sozialämter keine Daten bei dem Landeseinwohneramt verbleiben dürfen, die sich auf den durchgeführten Datenabgleich beziehen. Die Pflicht zur unverzüglichen Datenlöschung umfasst auch Protokolldaten, die anlässlich des Datenabgleiches erstellt worden sind.

Zur Realisierung bzw. Umsetzung der Auskunftsansprüche, die den Betroffenen nach § 16 Abs. 1 Nr. 3 BlnDSG zustehen, sind andere Maßnahmen erforderlich. Wir haben empfohlen, die Antragsteller auf Zulassung eines Kraftfahrzeuges ausführlich – unter Benennung der Rechtsgrundlage und Beschreibung des Verfahrensablaufes – über den möglichen Datenabgleich zwischen den Sozialbehörden und dem Kraftfahrzeugregister im Antragsverfahren zu informieren.

Das Landeseinwohneramt hat reagiert und den Text der Antragsvordrucke entsprechend ergänzt: Zukünftig werden die Antragsteller in einem „Hinweis zur Erhebung, Speicherung und Übermittlung der Daten“ u.a. über den automatischen Datenabgleich und seine Folgen aufgeklärt.

Kollegengespräche zur Aufklärung eines Verkehrsordnungswidrigkeitenverfahrens

Der Halter eines Pkw, dessen Fahrer bei einer Geschwindigkeitsübertretung fotografiert wurde, machte im Anhörungsverfahren keine Angaben zur Person des Fahrers. Da nicht ausgeschlossen werden konnte, dass er auch der Fahrer zur Tatzeit war, wurde der für den Wohnort des Halters zuständige Polizeiabschnitt von

Das vom Berliner Beauftragten für Datenschutz und Informationsfreiheit beschriebene Verfahren wird inzwischen zum Datenabgleich eingesetzt. Allerdings wird der Datenabgleich nicht monatlich, sondern jeweils alle drei Monate durchgeführt, und es werden nicht nur alle Sozialhilfeempfänger, die älter als 18 Jahre sind, erfasst, sondern auch die unter 18-jährigen, da auch diese als Fahrzeughalter in Betracht kommen.

Inhaltlich ist klarzustellen, dass der Datenabgleich zwischen dem Sozialamt und dem örtlichen Fahrzeugregister nicht der Feststellung der "Eigenschaft als Kraftfahrzeugführer", sondern der der "Eigenschaft als Kraftfahrzeug**halter**" dient.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

der Straßenverkehrsbehörde gebeten, diesen vorzuladen, anzuhören und unter Vorlage des Tatfotos die Identität und Personalien des Fahrers zur Tatzeit festzustellen. Nach vergeblichen Versuchen, den Halter an seiner Wohnanschrift zu erreichen, leitete der Kontaktbereichsbeamte den Vorgang an den Polizeiabschnitt weiter, in dem der Halter nach seiner Kenntnis seinen Dienst als Polizeibeamter versah. Der Betroffene wurde an seinem Arbeitsplatz im Polizeiabschnitt vom zuständigen Kollegen angesprochen und bestätigte, dass er der Fahrer zur Tatzeit gewesen sei.

Bereits im vergangenen Jahr haben wir über die Voraussetzungen einer zulässigen Datenerhebung in einem Verkehrsordnungswidrigkeitenverfahren berichtet[86]. Der vorliegende Fall gibt Anlass, diese Thematik erneut aufzugreifen. Rechtsgrundlage für das polizeiliche Handeln in einem Verkehrsordnungswidrigkeitenverfahren ist § 53 Abs. 1 Satz 1 Ordnungswidrigkeitengesetz (OwiG). Danach haben die Behörden und Beamten des Polizeidienstes nach pflichtgemäßem Ermessen Ordnungswidrigkeiten zu erforschen und dabei alle unaufschiebbaren Anordnungen zu treffen, um die Verdunkelung der Sache zu verhüten. Nach § 53 Abs. 1 Satz 2 OWiG haben sie bei der Erforschung von Ordnungswidrigkeiten – soweit das OWiG nichts anderes bestimmt – grundsätzlich dieselben Rechte und Pflichten wie bei der Verfolgung von Straftaten (vgl. § 163 StPO). Insofern kann sich die Polizei bei der Verfolgung von Verkehrsordnungswidrigkeiten auf den Grundsatz der freien Gestaltung des Ermittlungsverfahrens berufen. Dieser Grundsatz gilt jedoch nicht schrankenlos. Er wird begrenzt durch den Grundsatz der Verhältnismäßigkeit. Danach ist das polizeiliche Handeln nur zulässig, wenn es zur Erreichung des angestrebten Zweckes geeignet und erforderlich ist und der mit der Maßnahme verbundene Eingriff in die Rechte des Betroffenen nicht außer Verhältnis zur Bedeutung der Sache und der Stärke des bestehenden Tatverdachtes steht. Die gebotene Abwägung zwischen den in Betracht kommenden Maßnahmen, dem Anlass und den Auswirkungen des angeordneten Eingriffes ist unter Würdigung aller persönlichen und tatsächlichen Umstände des Einzelfalles vorzunehmen.

Davon ausgehend ist bei Eingriffsrechten, die den Verfolgungsbehörden im Strafverfahren zustehen, stets näher zu prüfen, ob und in welchem Umfang sie im Bußgeldverfahren gerechtfertigt sind. Zu berücksichtigen ist dabei ferner, dass der Vorwurf einer Straftat stets schwerer wiegt als der einer Ordnungswidrigkeit, so dass Maßnahmen, die im Strafverfahren erlaubt sind, im Bußgeldverfahren nicht oder nur bei Vorliegen besonderer Umstände gerechtfertigt sein können.

Im hier geschilderten Fall stellt die Weiterleitung des Vorganges an den Polizeiabschnitt, in welchem der Kfz-Halter seinen Dienst als Polizeibeamter versah, und die dortige Befragung zur Sache durch einen Arbeitskollegen oder Vorgesetzten einen erheblichen

Bei dem dargestellten Verfahren zur Aufklärung eines Verkehrsordnungswidrigkeitenverfahrens handelt es sich um einen besonders gelagerten Einzelfall, der sich nicht verallgemeinern lässt. Die Verhältnismäßigkeit der durchgeführten Maßnahme mag zweifelhaft sein.

[86] JB 2000, 4.2.3

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen dar. Dieser Eingriff entsprach nicht den Vorgaben des Grundsatzes der Verhältnismäßigkeit und war unzulässig.

Zwar war die Maßnahme geeignet, die Fahrzeugführerschaft des Halters zum Tatzeitpunkt festzustellen; sie war für diesen Zweck jedoch nicht erforderlich. Zur Identifizierung des Fahrers wäre es ausreichend gewesen, den Halter im Polizeiabschnitt seines Wohnortes zur Anhörung vorzuladen und ihn darauf hinzuweisen, dass bei seinem Nichterscheinen ein Abgleich des Tatfotos mit den Fotos in seinem Personalausweis- oder Passantrag (vgl. § 2 b Abs. 2 Nr. 3 Personalausweis- bzw. § 22 Passgesetz) erfolgt. Eine derartige Vorgehensweise wäre in jedem Fall ein milderes Mittel zur Identifizierung des Fahrers gewesen als die Befragung am Arbeitsplatz durch einen Kollegen oder Vorgesetzten.

Zu berücksichtigen ist aber, dass die konkrete Ausgestaltung des Ermittlungsverfahrens grundsätzlich im Ermessen der zuständigen Dienstkräfte liegt. Für die Beurteilung der Verhältnismäßigkeit kommt es entscheidend auf die ganz konkreten Umstände des Einzelfalles an, die sich rückblickend nur schwer nachvollziehen lassen.

4.3 Justiz und Finanzen

4.3.1 Justiz

In-camera-Verfahren eingeführt

Im Rahmen einer umfangreicheren Änderung der Verwaltungsgerichtsordnung (VwGO)[87] wurde ein Problem gelöst, auf das die Datenschutzbeauftragten seit langem hingewiesen haben[88]. Behörden sind zur Vorlage von Urkunden oder Akten und zu Auskünften im Verwaltungsprozess verpflichtet. Wenn das Bekanntwerden des Inhalts dem Wohle des Bundes oder eines deutschen Landes Nachteile bereiten würde oder wenn die Vorgänge nach einem Gesetz oder ihrem Wesen nach geheim gehalten werden müssen, kann die zuständige Oberste Aufsichtsbehörde, also das zuständige Ministerium, die Vorlage von Urkunden oder Akten und die Erteilung der Auskunft verweigern (§ 99 Abs. 1 VwGO). Zwar konnte bisher vom Gericht entschieden werden, ob hinreichend glaubhaft gemacht war, dass die gesetzlichen Voraussetzungen für die Verweigerung vorlagen. In die fraglichen Unterlagen selbst konnte das Gericht jedoch nicht Einsicht nehmen, da nach bisherigem Recht in diesem Fall die Unterlagen in den Prozess eingeführt und damit auch der klagenden Partei bekannt geworden wären.

Wir hatten diese Situation schon immer für unbefriedigend gehalten und vorgeschlagen, dass das Gericht unter Ausschluss der Parteien anhand der Unterlagen selbst über die Zulässigkeit der Verweigerung entscheidet (In-camera-Verfahren). Ganz im Sinne dieses Vorschlags hat das Bundesverfassungsgericht die Rechtslage im Jahr 1999 im Hinblick auf die Gewährleistung eines effektiven Rechtsschutzes für verfassungswidrig erklärt[89] und die Einführung eines In-camera-Verfahrens für rechtsstaatlich geboten gehal-

[87] Gesetz zur Bereinigung des Rechtsmittelrechts im Verwaltungsprozess vom 20. Dezember 2001 BGBl. S. 3987-3991
[88] JB 1982, 6.3
[89] Beschluss vom 27 Oktober 1999, Az.: 1 BvR 385/90

ten. Nunmehr entscheidet das Oberverwaltungsgericht ohne mündliche Verhandlung über die Rechtmäßigkeit. Dem Gericht sind hierzu die verweigerten Urkunden oder Akten vorzulegen oder die verweigerten Auskünfte zu erteilen. Das Verfahren unterliegt den Vorschriften des materiellen Geheimschutzes. In besonderen Fällen ist dem Gericht die Einsicht in die Räumlichkeiten der Obersten Aufsichtsbehörde zu gestatten. Die Entscheidungsgründe dürfen Art und Inhalt der geheim ehaltenen Urkunden oder Akten und Auskünfte nicht erkennen lassen (§ 99 Abs. 2 VwGO).

Amtsblätter im Internet

Ein Bürger beklagte sich über die Veröffentlichung der Amtsblätter im Internet, die in seinem Fall dazu führten, dass sein Name im Zusammenhang mit Zwangsversteigerungen und konkreten Zwangsversteigerungsobjekten genannt wird und bei Nutzung der Suchmaschine unter seinem Namen jeder gewöhnliche Internet-Nutzer binnen kurzer Zeit von den Zwangsversteigerungen Kenntnis erlangen kann. Da er als Immobilienverwalter auf guten Leumund angewiesen ist, sah er sich durch die Veröffentlichung seines Namens durch die in das Internet eingestellten Amtsblätter in seiner beruflichen Existenz erheblich gefährdet.

Nach dem Zwangsversteigerungsgesetz (ZVG) soll die Terminsbestimmung die Bezeichnung des zurzeit der Eintragung des Versteigerungsvermerkes eingetragenen Eigentümers sowie die Angabe des Grundbuch-Blattes, der Größe und des Verkehrswertes des Grundstückes enthalten (§ 38). Die Terminsbestimmung muss durch einmalige Einrückung in das für Bekanntmachungen des Gerichtes bestimmte Blatt öffentlich bekannt gemacht werden (§ 39 Abs. 1 ZVG).

Zweck der Veröffentlichung der personenbezogenen Daten in Amtsblättern ist vornehmlich die Information potenzieller Bieter sowie die Aufforderung zur Geltendmachung von Rechten Dritter in Zwangsversteigerungsverfahren. Insoweit verletzt diese Vorschrift auch nicht das grundrechtlich geschützte Persönlichkeitsrecht des Schuldners.

Allerdings entsteht durch die Veröffentlichung im Internet ein regional unbegrenzter (globaler) Zugriff auf diese Daten. Durch die Festlegung von bestimmten Suchkriterien können gezielt Profile zu einzelnen Personen definiert und automatisiert aus den Daten im Internet zusammengestellt werden. Wegen dieser gesteigerten Risiken und des damit verbundenen erheblichen Eingriffes in das Recht auf informationelle Selbstbestimmung des Betroffenen wurde die für die Einstellung von Amtsblättern im Internet zuständige Senatsverwaltung für Inneres um Abhilfe gebeten.

Ab Januar 2002 werden die Amtsblatt-Inhalte in einem grafischen Dateiformat (.tif) im Internet präsentiert werden, das die Indexierung in Suchmaschinen technisch ausschließt, da diese nur mit zeichenorientiertem Format möglich ist. Dies bedeutet, dass ein gezielter Zugriff auf die Amtsblatt-Daten nach wie vor möglich sein wird; eine ungezielte Suche mittels Suchwörtern

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

(Name des Schuldners) wird jedoch nicht mehr zu Amtsblatt-Eintragungen führen.

Ähnlich stellt sich die Problemlage bei der Normierung der Veröffentlichung von Insolvenz-Informationen im Internet dar. Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer Frühjahrskonferenz im April 2001 dazu eine entsprechende Entschließung gefasst[90].

Eine Reihe neuer Vorschriften zur Führung elektronischer Register bei der Justiz enthält das Gesetz über elektronische Register und Justizkosten für Telekommunikation vom 10. Dezember 2001[91].

Das Referat für Fahrerlaubnisse als Ermittlungsbehörde?

Die Staatsanwaltschaft bei dem Landgericht Berlin hatte sich mit der Bitte um Mitteilung an uns gewandt, ob Ersuchen der Fahrerlaubnisbehörde bei dem Landeseinwohneramt auf Übersendung der kompletten Ermittlungsakte rechtmäßig seien. Bedenken wurden insbesondere bei Jugendlichen bzw. Heranwachsenden und bei Bagatelldelikten ohne Bezug zum Straßenverkehr geäußert. Die Fahrerlaubnisbehörde stützte ihr Auskunftsersuchen dabei insbesondere auf die §§ 11, 14 Fahrerlaubnisverordnung (FeV).

Eine Einsichtnahme des Landeseinwohneramtes (LEA) in staatsanwaltschaftliche Ermittlungsakten ist ein Eingriff in das Selbstbestimmungsrecht des Betroffenen. Sie ist daher nur rechtmäßig, wenn eine entsprechende Ermächtigungsgrundlage vorhanden ist und ein Erfordernis für eine solche Akteneinsicht besteht. Eine solche Ermächtigungsgrundlage ergibt sich nicht aus den straßenverkehrsrechtlichen Regelungen des § 2 Abs. 8 Straßenverkehrsgesetz (StVG) i.V.m. § 11 Abs. 6 FeV.

Das LEA (Fahrerlaubnisbehörde) hat nach § 2 Abs. 7 StVG zu ermitteln, ob der Antragsteller zum Führen eines Kraftfahrzeuges geeignet und befähigt ist. Dazu hat es Auskünfte aus dem Verkehrszentralregister und dem Zentralen Fahrerlaubnisregister einzuholen. Nach § 2 Abs. 8 StVG kann das LEA anordnen, dass der Antragsteller ein medizinisch-psychologisches Gutachten beizubringen hat, wenn Tatsachen bekannt werden, die Bedenken gegen die Eignung oder Befähigung des Bewerbers begründen. Die Polizei hat entsprechende Tatsachen der Fahrerlaubnisbehörde nach § 2 Abs. 12 StVG mitzuteilen.

Eine Befugnis der Staatsanwaltschaft zur Übermittlung von Ermittlungsakten ist im StVG nicht geregelt.

Die von dem LEA genannten §§ 11, 14 FeV berechtigen zur Anordnung, dass der Betroffene zur Vorbereitung von Entscheidungen über die Erteilung oder Verlängerung einer Fahrerlaubnis ein medizinisch-psychologisches Gutachten beizubringen hat. Zu diesem Zweck teilt das LEA nach § 11 Abs. 6 FeV der

Die Rechtsausführungen des Berliner Beauftragten für Datenschutz und Informationsfreiheit sind zwar grundsätzlich zutreffend, aber unvollständig. Sie befassen sich nicht mit der Regelung des § 474 Abs. 3 StPO, wonach Akteneinsicht gewährt werden kann, wenn die Erteilung von Auskünften einen unverhältnismäßigen Aufwand bereiten würde oder die die Akteneinsicht begehrende Stelle unter Angabe von Gründen erklärt, dass die Erteilung einer Auskunft zur Erfüllung ihrer Aufgaben nicht ausreicht. Im Hinblick auf diese durch das StVÄG 1999 verschärften Anforderungen fordert die Staatsanwaltschaft andere Behörden auf, die Aktenanforderungsgesuche zu begründen.

Das Landeseinwohneramt Berlin hat die Verwaltungspraxis insoweit angepasst. Einzelanfragen werden entsprechend detailliert begründet.

[90] vgl, Anlagenband, a.a.O., I.2
[91] BGBl. S. 3422-3434

untersuchenden Stelle mit, welche Fragen im Hinblick auf die Eignung des Betroffenen zum Führen eines Kraftfahrzeuges zu klären sind, und übersendet ihr die vollständigen Unterlagen, soweit sie unter Beachtung der gesetzlichen Verwertungsverbote verwendet werden dürfen.

Befugnisse, die die Staatsanwaltschaft zur Übermittlung von Akten an das LEA berechtigen, sind in der FeV – insbesondere in den vom LEA genannten Vorschriften – nicht enthalten.

Auch in der Strafprozessordnung (StPO) ist keine entsprechende Ermächtigung vorhanden. Die Auskünfte aus Akten an öffentliche Stellen sind in § 474 Abs. 1, 2 StPO geregelt. Unter der Aufzählung des § 474 Abs. 1 StPO ist keine dem Landeseinwohneramt entsprechende Behörde genannt. Diese Regelung spricht im Gegenteil gerade gegen eine rechtmäßige Akteneinsicht durch weitere Behörden, da die Aufzählung der berechtigten Stellen nach allgemeiner Ansicht wegen der besonderen Sensibilität von Ermittlungsakten abschließend ist. Es bedarf vielmehr für Auskünfte und Einsichten nach § 474 Abs. 2 StPO jeweils einer gesonderten Vorschrift, die die Behörde dazu ermächtigt. Die Regelung betrifft daher allein das Verhalten der Justizbehörden und stellt keine Eingriffsermächtigung auf Seiten der Behörde (LEA) dar.

Nach § 474 Abs. 2 StPO sollen öffentliche Stellen grundsätzlich nur Auskünfte aus Akten erhalten. Die Auskünfte können erteilt werden, soweit sie für die in Abs. 2 Nr. 1 genannten Zwecke erforderlich sind oder soweit besondere gesetzliche Regelungen, wie etwa die durch das Justizmitteilungsgesetz eingeführten §§ 12 ff. Einführungsgesetz zum Gerichtsverfassungsgesetz (EGGVG), Übermittlungen von Amts wegen vorsehen.

Nach Nr. 45 Abs. 2 der Mitteilungen in Strafsachen sind sonstige Tatsachen, die in einem Strafverfahren bekannt werden, der nach § 68 Abs. 1 und 2 der Straßenverkehrszulassungsordnung (StVZO) zuständigen Verwaltungsbehörde mitzuteilen, wenn ihre Kenntnis aufgrund besonderer Umstände des Einzelfalles für die Beurteilung erforderlich ist, ob die Inhaberin oder der Inhaber einer Fahrerlaubnis zum Führen von Fahrzeugen ungeeignet ist. Dabei ist zu berücksichtigen, wie gesichert die zu übermittelnden Kenntnisse sind. Die Mitteilung ordnen Richterinnen oder Richter, Staatsanwältinnen oder Staatsanwälte an.

Daraus ergibt sich, dass eine Übermittlungsbefugnis der Staatsanwaltschaft von fahreignungsrelevanten Tatsachen an die zuständige Verwaltungsbehörde im Einzelfall besteht, nicht dagegen ein generelles Akteneinsichtsrecht durch das LEA (Fahrerlaubnisbehörde).

Unsere Rechtsauffassung wird im Ergebnis von dem Bundesministerium der Justiz geteilt, das die Übermittlung personenbezogener Daten an die Straßenverkehrsbehörde von einer Entscheidung der Staatsanwaltschaft abhängig macht und an das Gebot der Erforderlichkeit knüpft.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

4.3.2 Finanzen

Die Abgabenordnung: Endlich Fortschritte

Das Fehlen hinreichender datenschutzrechtlicher Bestimmungen in der Abgabenordnung (AO) wird von den Datenschutzbeauftragten seit vielen Jahren bemängelt. Dies lag im Wesentlichen an der ablehnenden Haltung der zuständigen Referenten in den Finanzministerien. Auch die Berliner Senatsverwaltung für Finanzen hat keinerlei Aktionen entfaltet, obwohl der Senat durch Beschluss des Abgeordnetenhauses zum Jahresbericht 1997 aufgefordert wurde, „sich auf Bundesebene für die Aufnahme datenschutzrechtlicher Bestimmungen in die Abgabenordnung einzusetzen". Bis heute sind nach unserem Kenntnisstand keine Bemühungen der Senatsverwaltung für Finanzen auf Bundesebene erfolgt, datenschutzrechtliche Bestimmungen in die Abgabenordnung aufzunehmen.

Es ist unzutreffend, dass die Senatsverwaltung für Finanzen keine Bemühungen zur Umsetzung des Beschlusses des Abgeordnetenhauses zur Aufnahme datenschutzrechtlicher Bestimmungen in die Abgabenordnung -AO- vornahm. Auf Anregung der Senatsverwaltung für Finanzen ist die diesbezügliche Überarbeitung der Abgabenordnung erneut zum Gegenstand der Erörterung durch die für Fragen der AO zuständigen Referenten der obersten Finanzbehörden des Bundes und der Länder gemacht worden (Sitzung AO II/2000).

Seit April 2001 besteht allerdings eine Bund-Länder-Arbeitsgruppe „Datenschutz in der Abgabenordnung". An ihr nehmen unter Leitung des Bundesministeriums der Finanzen Vertreter der Finanzministerien der Länder sowie des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz teil. Die Arbeitsgruppe erörtert den Bestand datenschutzrechtlicher Vorschriften in der Abgabenordnung sowie die Notwendigkeit, Vorschriften zu ändern oder neu zu schaffen. Seither hat sich das Klima deutlich verbessert. Vorstellungen über die Novellierung der AO sind entwickelt und sollen 2002 mit dem Ziel einer Gesetzesänderung erörtert werden, wenn diese auch in der laufenden Legislaturperiode nicht mehr zustande kommen kann. Zur Klimapflege soll 2002 auch eine Koordinierungsrunde mit Vertretern der Datenschutzbeauftragten und Vertretern der obersten Finanzbehörden der Länder unter Leitung des Bundesfinanzministeriums eingerichtet werden, die sich mit grundsätzlichen Fragen, die Anlass von Einzelbeanstandungen im Bereich des Verfahrensrechts sind, befassen und Lösungsempfehlungen für die jeweiligen Gremien erarbeiten soll.

Darauf folgend kam es schließlich unter zunächst erneutem Hinweis, dass die AO bereits eine Vielzahl bereichsspezifischer Datenschutzregelungen enthalte, im Ergebnis zu der vom BlnBDI begrüßten Entwicklung (Einrichtung einer Arbeitsgruppe auf Bundesebene, Koordinierungsrunde).

Zu der Koordinierungsrunde hat der Vertreter der Senatsverwaltung für Finanzen seine Bereitschaft zur Teilnahme erklärt.

Viertes Finanzmarktförderungsgesetz

Die Bundesregierung hat den Entwurf eines Gesetzes zur weiteren Fortentwicklung des Finanzplatzes Deutschland (Viertes Finanzmarktförderungsgesetz) eingebracht[92]. Das Ziel des Gesetzes ist es u. a., den Anlegerschutz zu verbessern und in diesem Zusammenhang auch die Aufsicht über die Kreditinstitute zu verbessern. Die Bundesanstalt für Finanzdienstleistungsaufsicht soll besondere Befugnisse im Vorfeld der Strafverfolgung erhalten. Es ist vorgesehen, ihr bei Anhaltspunkten für einen Verstoß gegen das Verbot von Insider-Geschäften bzw. von Kurs- und Marktpreismanipulationen das Recht einzuräumen, von den Wertpapierdienstleistungsunternehmen, den Emittenten und anderen am Handel beteiligten Unternehmen die Aufbewahrung von Verbindungsdaten der Teilnehmer an der Telekommunikation zu verlangen (Entwurf des § 16 b Wertpapierhandelsgesetz - WpHG). Der Bun-

In dem Entwurf eines 4. Finanzmarktförderungsgesetzes ist im Bereich der Steuergesetze vorgesehen, zur Bekämpfung der Geldwäsche einen § 31b AO einzufügen, der die Finanzbehörden verpflichtet, Tatsachen, die auf eine Straftat nach § 261 StGB schließen lassen, den Strafverfolgungsbehörden mitzuteilen. Die Durchbrechung des Steuergeheimnisses zur Durchführung eines entsprechenden Strafverfahrens ist durch diese neue Vorschrift ausdrücklich zulässig.
Eine zusätzliche Befugnis der Finanzbehörde ist in dieser Verpflichtung nicht zu erkennen.

[92] BR-Drs. 936/01

desrat hat eine entsprechende Änderung des Börsengesetzes (BörsG) für die Börsenaufsichtsbehörde empfohlen[93].

Die Bundesanstalt soll außerdem durch eine Änderung des Gesetzes über das Kreditwesen (KWG) (Entwurf des § 6 Abs. 5 KWG) eine zur Auskunft aus den Kundendateien berechtigte Stelle im Sinne des § 90 Abs. 3 Telekommunikationsdienstegesetz (TKG) werden. Berechtigte Stellen sind zurzeit nach § 90 Abs. 3 TKG die Gerichte, Strafverfolgungsbehörden, der Verfassungsschutz, der MAD und der BND. Außerdem ist vorgesehen, die Bundesanstalt auch als berechtigte Stelle in § 89 Abs. 6 TKG neben den Strafverfolgungsbehörden, dem Verfassungsschutz, dem MAD und dem BND sowie dem Zollkriminalamt aufzunehmen. Die in § 89 Abs. 6 TKG genannten Stellen sind berechtigt, zur Verfolgung von Straftaten und Ordnungswidrigkeiten Bestandsdaten der Telekommunikationsverträge abzufragen.

Die geplanten Regelungen stellen einen schwerwiegenden Eingriff in das Telekommunikationsgeheimnis dar. Die Bundesanstalt für Finanzdienstleistungen sowie die Börsenaufsichtsbehörde erhalten Befugnisse, die in dieser Form zum Teil nicht einmal den Strafverfolgungsbehörden in den §§ 100 ff. StPO eingeräumt werden. Es wird nicht nur das Zitiergebot nicht eingehalten – d.h., es fehlt ein Hinweis darauf, dass das Fernmeldegeheimnis eingeschränkt worden ist –, es fehlt auch bei dem Entwurf des § 16 b WpHG und des § 56 d BörsG an einer Zweckbindungsregelung, die sicherstellt, dass bei einer Übermittlung von Verbindungsdaten an die Aufsichtsbehörde die Daten nur für den Zweck der Prüfung eines Verstoßes gegen Verbotsvorschriften benutzt werden. Es ist fraglich, ob die Maßnahme verhältnismäßig ist.

Auch hinsichtlich der Erforderlichkeit einer Aufnahme der Bundesanstalt für Finanzdienstleistungen in § 89 Abs. 6 TKG als zur Abfrage von Bestandsdaten befugte Stelle bestehen Zweifel. Nach der Gesetzesbegründung soll gegen Marktmanipulation unter Zuhilfenahme des Internets vorgegangen werden. Hier hilft die Kenntnis der Bestandsdaten von Nutzern von Telekommunikationsdiensten jedoch gerade nicht weiter. Die Bundesanstalt ist zudem bereits jetzt als für Ordnungswidrigkeitenverfahren zuständige Behörde zu Datenabfragen nach § 89 Abs. 6 TKG für diese Verfahren befugt.

Zugriff des Betriebsprüfers auf die digitalen Unterlagen

Im Jahresbericht 2000[94] hatten wir über die Änderung der Abgabenordnung (AO) berichtet, die es den Betriebsprüfern des Finanzamtes erlaubt, bei Betriebsprüfungen vor Ort Einsicht in die digitalen Unterlagen eines Unternehmens zu nehmen und dabei auch das Datenverarbeitungssystem zu nutzen (§ 147 Abs. 6

[93] Beschluss vom 20. Dezember 2001 zu § 56 d Börsengesetz - BörsG, BR-Drs. 936/01, zu § 56 d Börsengesetz - BörsG
[94] JB 2000, 4.3.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

AO). Der Betriebsprüfer darf die Daten bei der Außenprüfung danach auch maschinell verwerten oder sich vom Unternehmen einen Datenträger zur Verfügung stellen lassen. Wir hatten darauf hingewiesen, dass der Betriebsprüfer bei seiner Prüfung auch auf personenbezogene Daten stoßen kann, deren Kenntnis für die Betriebsprüfung ohne Bedeutung ist. Da eine Begrenzung der Zugriffsbefugnisse des Steuerprüfers bei den meisten Untenehmen nur durch eine Systemänderung erreicht werden kann, hatte der Gesetzgeber den Unternehmen ein Jahr Zeit eingeräumt, um ihre Systeme entsprechend auf den Prüfzugriff vorbereiten zu können. Diese Übergangsfrist ist am 31. Dezember 2001 abgelaufen.

Die Unternehmen müssten inzwischen ihre Systeme dahingehend geändert haben, dass Zugriffsbefugnisse bzw. –abschottungen für die personenbezogenen Daten geschaffen worden sind, die nicht zu dem betriebsprüfungsrelevanten Datenbestand zählen. Das Problem des unbefugten Zugriffes betrifft zum einen personenbezogene Arbeitnehmerdaten, zum anderen aber auch Daten von Steuerpflichtigen, die einem besonderen Berufsgeheimnis unterliegen wie Ärzte und Rechtsanwälte.

Auch diese Daten, soweit sie dem Betriebsprüfer im Rahmen einer Prüfung bekannt würden, unterliegen dem Schutz der strafbewehrten Vorschrift des § 30 AO - Steuergeheimnis -.

Fragebogen zur Religionszugehörigkeit

Immer wieder erhalten wir Eingaben von Petenten, die sich über Fragebögen beschweren, in denen sie gegenüber den Kirchensteuerstellen Angaben über ihre Religionszugehörigkeit machen sollen. Besonders wenig Verständnis zeigen die Bürger, die bereits – zum Teil wiederholt – diesen Bogen ausgefüllt haben oder noch nie Mitglied einer öffentlich-rechtlichen Religionsgemeinschaft waren und somit keinen Nachweis über einen eventuellen Austritt erbringen können.

In der Regel geben wir diese Eingaben an die Datenschutzbeauftragten der Evangelischen Kirche Berlin-Brandenburg bzw. des Erzbistums Berlin ab. Die Kirchensteuerstellen sind zwar räumlich an die Finanzämter angegliedert, gehören rechtlich und organisatorisch aber zu den Kirchen. Sie unterliegen somit nicht der Kontrolle des Berliner Beauftragten für Datenschutz und Informationsfreiheit. Aufgrund des verfassungsrechtlich garantierten Selbstbestimmungsrechts der Kirchen gilt für sie nicht das Berliner Datenschutzgesetz, sondern vielmehr eigenes kirchliches Recht.

Um zur Information und Aufklärung der Bürger beizutragen, haben wir uns von den Datenschutzbeauftragten des Erzbistums Berlin und der Evangelischen Kirche in Berlin-Brandenburg die Schwierigkeiten, die für die Kirchen bei der Feststellung der Kirchenzugehörigkeit von Steuerpflichtigen bestehen und die zur Versendung der Fragebögen führen, erläutern lassen.

Die Kirchensteuerstellen wirken bei der Verwaltung der Kirchensteuern mit und unterstützen die Finanzämter dabei. Zu ihren Aufgaben gehört insbesondere die Feststellung der subjektiven Kirchensteuerpflicht. Dazu erhalten sie an personenbezogenen Daten die Steuernummer, Religionsmerkmal, Namen, Vornamen, Geburtsdatum, Anschrift sowie die Angabe, ab wann

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

das Steuerkonto aufgenommen wurde. In der Regel wird sich anhand dieser Angaben die rechtliche Zugehörigkeit bzw. Nichtzugehörigkeit zur evangelischen bzw. katholischen Kirche feststellen lassen. Eine weitergehende Prüfung der Religionszugehörigkeit erfolge nach Information des Datenschutzbeauftragten des Erzbistums Berlin nur in den Fällen, in denen Abweichungen zwischen vorliegender Grundinformation, Lohnsteuerkarte oder Angaben in der Steuererklärung auftreten. Der Fragebogen werde nur versandt, wenn die Zugehörigkeit zu einer Kirche nicht bereits eindeutig geklärt werden konnte. Hierbei ist problematisch, dass den Kirchensteuerstellen auch bei an sich eindeutigen Fällen die notwendigen Informationen nicht zur Verfügung stehen. Dies liegt zum Teil in dem fehlenden Abgleich zwischen kirchlichen Stellen und den Finanzämtern begründet (z. B. gibt ein Steuerpflichtiger nach einem Umzug gegenüber dem Landeseinwohneramt seine Kirchenzugehörigkeit nicht an, obwohl er tatsächlich nicht aus der Kirche ausgetreten ist), zum Teil in dem innerkirchlichen Organisationsaufbau. So würden die Daten über Kirchenmitglieder in der Gemeinde der Taufe geführt, nicht in der des Wohnsitzes. Aufgrund dieser Schwierigkeiten ließen sich auch ungewollte Mehrfachversendungen der Fragebögen nicht immer vermeiden. Eine andere Möglichkeit, die benötigten Angaben zu erhalten, stehe den jeweiligen Kirchensteuerstellen nicht zur Verfügung.

Zugriffsregelungen beim DCL-Verfahren

Steuerbürger stellen immer wieder erstaunt fest, dass innerhalb der Steuerverwaltung Informationsflüsse zwischen den verschiedenen Finanzämtern bestehen, die etwa dazu führen, dass Guthaben in der einen Steuerart mit Rückständen in anderen Steuerarten verrechnet werden. Wir haben die finanzamtsübergreifenden Zugriffsmöglichkeiten, die dazu bestehenden Regelungen und die technischen und organisatorischen Maßnahmen zur Benutzer-authentifizierung, zur Vergabe von Zugriffsberechtigungen, zur Protokollierung von Datenabfragen und zur Datenübertragung über das OFD-Netz kontrolliert.

Sowohl der Datenaustausch zwischen Steuerkonten desselben Steuerbürgers als auch das Verfahren der Aufrechnung sind gesetzlich begründet und rechtlich nicht zu beanstanden. Die dargestellte Praxis entspricht auch den Bedürfnissen der Bürger und der Verwaltung.

Wir haben dabei folgende Feststellungen getroffen:

Die *Benutzerauthentifizierung* enthielt leichte Schwachstellen, die das Risiko erhöhen, dass sich Benutzer unter fremder Identität am System anmelden und somit die Sicherheit hinsichtlich der Vertraulichkeit, Integrität, Verfügbarkeit und Revisionsfähigkeit der Datenverarbeitung beeinträchtigen.

Die minimale *Passwortlänge* betrug sieben Stellen, von denen jedoch zwei durch die Finanzamtsnummer des Benutzers belegt sind und somit nicht zum geheimen Teil des Passworts gehören. Damit hat der geheime Teil des Passworts nur noch eine Länge von mindestens fünf Stellen, was nicht als ausreichend angesehen werden kann, zumal die Passwörter systembedingt nur aus einem eingeschränkten Zeichenvorrat erstellt sein dürfen. Wir haben empfohlen, die Mindestpasswortlänge auf acht Stellen zu erhöhen, wenn auf die Vorga-

Der Empfehlung wird gefolgt; die minimale Passwortlänge wird auf acht Stellen erhöht.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats
be für die Belegung von zwei Stellen des Passworts mit der Nummer des Finanzamts nicht verzichtet werden kann.	
Es wird zwar nach 100 Tagen ein *Wechsel des Passworts* durch das System erzwungen und geprüft, ob das neue Passwort nicht mit dem abgelaufenen übereinstimmt. Damit wäre demzufolge lediglich ein regelmäßiger Wechsel zwischen zwei Passwörtern zu realisieren. Wir haben empfohlen, eine im Rahmen eines Versionswechsels bereitgestellte neue Funktionalität des Systems zu nutzen und eine Wiederverwendung bereits benutzter Passworte erst beim fünften Wechsel zu gestatten.	Der Empfehlung wird gefolgt; eine Wiederverwendung bereits benutzter Passworte wird künftig erst beim sechsten Wechsel möglich sein.
Wenn ein Benutzer sein Passwort ändern will, z. B. weil er glaubt, dass es Dritten bekannt geworden ist, hat er ein neues Passwort zu beantragen. Von der zuständigen Stelle wird daraufhin ein Einstiegspasswort vergeben, das nur für die sofortige Änderung verwendet werden darf. Dies ist zwar bei der Neueinrichtung von Benutzern und beim Vergessen von Passwörtern die übliche Verfahrensweise, jedoch entspricht eine solche Antragsprozedur nicht dem Stand der Technik, wenn das alte Passwort noch bekannt ist. Wir haben empfohlen zu prüfen, ob es die neue Systemversion ermöglicht, dass der Benutzer von sich aus das Passwort wechseln kann, wenn es ihm notwendig erscheint, denn bei allzu aufwendigem Verfahren besteht die Gefahr, dass auf eine notwendige Änderung des Passworts verzichtet wird. Anderenfalls wäre die Schaffung einer entsprechenden Routine in Eigenprogrammierung angezeigt.	Der Empfehlung wird gefolgt; bei bekanntem alten Passwort kann der Passwortwechsel nunmehr durch den Benutzer vorgenommen werden.
Auf eine regelmäßige Auswertung der *Protokolle der Systemanmeldungen* wird verzichtet, so dass die Hintergründe fehlerhafter Anmeldungen nicht geprüft werden. Damit besteht das Risiko, dass ein Benutzer, der sich unter einer fremden Benutzerkennung Zugang zum System verschaffen will, unentdeckt bleibt, wenn er seine Anmeldeversuche jeweils nach dem zweiten Versuch einstellt und diese erst dann fortsetzt, wenn er sicher sein kann, dass sich der rechtmäßige Benutzer zwischenzeitlich erfolgreich angemeldet hat. Unterstützt wird ein solches Vorgehen zudem dadurch, dass dem rechtmäßigen Benutzer nach erfolgreicher Anmeldung weder der Zeitpunkt der letzten ordnungsgemäßen Anmeldung noch eines fehlgeschlagenen Versuchs angezeigt wird. Wir haben empfohlen, die Anmeldeprotokolle einer kritischen Auswertung zu unterziehen und die systemseitig mögliche Anzeige der letzten erfolgreichen Anmeldung bzw. eines abgewiesenen Anmeldeversuchs zu aktivieren.	Der Empfehlung wird gefolgt; jeder unzulässige Anmeldeversuch wird protokolliert. Die Protokollierung wird in noch festzulegendem Umfang ausgewertet. Der rechtmäßige Benutzer erhält im Rahmen einer geänderten Anmeldeprozedur Meldung über den Zeitpunkt der letzten korrekten Anmeldung am System sowie über unzulässige Anmeldeversuche während des Zeitraums seit seiner letzten korrekten Anmeldung.
Die *Zugriffsberechtigungen* werden nach einem mehrstufigen Zuordnungssystem hinsichtlich der Endgeräte, Applikationen und Daten vergeben. Soweit dies von uns beurteilt werden kann, orientiert sich die Vergabe der Zugriffsrechte an den entsprechenden gesetzlichen Grundlagen und den tatsächlichen fachlichen Erfordernissen. Dies bedeutet, dass den Benutzern neben den Zugriffen auf die Steuerfälle ihrer Zuständigkeit im gewissen Umfang auch finanzamtsübergreifende	

Zugriffe gestattet werden, weil dies bei der Bearbeitung mancher Steuerfälle erforderlich ist.

Sofern weitreichende Zugriffsberechtigungen für größere Benutzerkreise fachlich erforderlich sind, sind missbräuchliche, weil zweckfremde Zugriffe technisch nicht zu verhindern. In diesen Fällen ist eine Protokollierung der Zugriffe vorzusehen, die es ermöglicht, zumindest in Stichproben die dienstliche Erforderlichkeit einzelner Abfragen zu prüfen.

Datenabfragen auf explizit den jeweiligen Benutzern zugewiesene finanzamtseigene Steuerkonten, finanzamtsübergreifende Abfragen, die lediglich der Zuständigkeitsklärung dienen, sowie Abfragen zur Zentralkartei durch die zentrale Stelle werden nicht protokolliert. Finanzamtsinterne Abfragen auf Speicherkonten außerhalb der eigenen Zuständigkeit, finanzamtsübergreifende Datenabfragen auf Speicherkonten, Abfragen zur Zentralkartei durch ausgewählte Finanzämter sowie finanzamtsinterne Abfragen zur Zentralkartei außerhalb der zentralen Stelle werden stichprobenweise protokolliert, wobei der Abfragegrund erfragt wird. Diese Protokolle werden entsprechend einer vorgegebenen Quote geprüft. Andere finanzamtsübergreifende Speicherkontenabfragen und finanzamtsübergreifende Abfragen zur Zentralkartei außerhalb der zentralen Stelle werden vollständig protokolliert. Dabei ist auch hier stichprobenhaft der Abfragegrund einzugeben. Die solcherart protokollierten Abfragen werden anschließend vollständig überprüft.

Die differenzierte automatisierte Protokollierung einschließlich der Eingabe des Abfragegrundes erscheint wegen der unterschiedlichen datenschutzrechtlichen Risiken der Abfragearten sachgerecht. Allerdings ergab die Kontrolle der *Abfragebegründungen*, dass häufig allzu pauschale und wenig aussagekräftige Begründungen abgeliefert wurden. Offenbar wird auch die Prüfung in den einzelnen Finanzämtern uneinheitlich vorgenommen, da in bestimmten Finanzämtern immer alles in Ordnung zu sein scheint und in anderen Finanzämtern differenzierte Nachforschungen vorgenommen werden. Klärungsbedürftig sind noch Aussagen aus den Berichten der Finanzämter, die von fehlenden Begründungen sprechen, obwohl die Angabe von Begründungen in den zufällig auftretenden Begründungsfällen technisch erzwungen werden sollte.

Das Verfahren zur Prüfung protokollierter Abfragen wird neu geregelt um damit die Möglichkeit der Aufdeckung von Missbrauchsfällen weiter zu verbessern. Die dargestellten Fälle des gänzlichen Fehlens von Abfragebegründungen sind nach Erkenntnissen der Oberfinanzdirektion Berlin auf technische Probleme zurückzuführen, die zwischenzeitlich behoben sind. Die Finanzämter sind angewiesen, Fälle des Fehlens von Abfragebegründungen besonders zu prüfen und aufzuklären.

4.4 Sozialordnung

4.4.1 Personaldaten

Arbeitnehmerdatenschutz

Obwohl Probleme beim Umgang mit Personaldaten in Verwaltungen und Unternehmen häufig sind und auch Arbeits- und Verwaltungsgerichte intensiv beschäftigen[95], ist der Arbeitnehmerdatenschutz nach wie vor nicht angemessen geregelt. Lediglich im Beamtenrecht finden sich spezielle Bestimmungen (z. B. §§ 56 ff.

[95] vgl. Gola, Peter; Wronka, Georg: Handbuch zum Arbeitnehmerdatenschutz.3. Aufl. i.V. Frechen: Datenkontext 2002

Berliner Landesbeamtengesetz - LBG). Bei Arbeitsverhältnissen muss auf die allgemeinen Bestimmungen des BDSG oder auf die in der Rechtsprechung entwickelten Grundsätze zurückgegriffen werden. Nicht nur die Datenschutzbeauftragten haben dies seit vielen Jahren bemängelt, auch der Bundestag hat mehrfach die Bundesregierung aufgefordert, einen entsprechenden Gesetzentwurf vorzulegen[96]. Für die laufende Legislaturperiode war erneut angekündigt worden, dass das Bundesministerium für Arbeit und Sozialordnung einen Vorschlag vorlegen würde. Dies ist aber wiederum unterblieben.

Wirkung eines allgemeinverbindlich erklärten Tarifvertrages

Die Tarifvertragsparteien im Berliner Gebäudereinigerhandwerk haben in einem Tarifvertrag die Gründung einer Prüf- und Beratungsstelle vereinbart. Sie hat insbesondere die Aufgabe, durch Beratung und Prüfung sowie durch gerichtliche Geltendmachung auf die Gewährung tariflicher Ansprüche und Einhaltung tariflicher Vorschriften über Einkommen und Arbeitsbedingungen hinzuwirken und hierdurch den Schutz der Arbeitnehmer zu verbessern. Unter anderem enthält der Tarifvertrag folgende Regelungen:

- *§ 5 Abs. 1: Die Arbeitgeber sind verpflichtet, der Prüf- und Beratungsstelle zu melden, welche Beiträge sie zur Unfallversicherung abführen.*
- *§ 5 Abs. 2: Die Beitragsmeldung umfasst Namen und Anschrift des Arbeitgebers, seine Betriebsnummer und den fällig gewordenen Beitrag sowie alle zur Ermittlung des Beitrages notwendigen Daten.*
- *§ 5 Abs. 3: Auf besondere Anforderung der Prüf- und Beratungsstelle sind Namen und Anschriften der Beschäftigten und vom Tarifvertrag erfassten Arbeitnehmer mitzuteilen und alle zur Prüfung der Gewährung tariflicher Leistungen und Einhaltung tariflicher Vorschriften über Arbeitsbedingungen notwendigen Daten aufgeschlüsselt auf die einzelnen Arbeitnehmer zu melden.*

Der Tarifvertrag wurde allgemeinverbindlich erklärt, d. h., er entfaltet seine Wirkung auch gegenüber nicht tarifgebundenen Arbeitgebern und Arbeitnehmern.

Eine Gruppe von nicht tarifgebundenen Gebäudereinigern war der Auffassung, dass der allgemeinverbindlich erklärte Tarifvertrag ihre Datenschutzinteressen verletze, da die Gesellschafter der Beratungsstelle (eine GmbH) gleichzeitig ihre Konkurrenten seien und sie so ausforschen könnten. Auch seien die Datenschutzinteressen ihrer Mitarbeiter nicht gewahrt.

Eine tarifvertragliche Regelung kann als andere Rechtsvorschrift im Sinne des § 4 Abs. 1 BDSG die Datenverarbeitungen rechtfertigen. Die durch den Tarifvertrag möglichen Einschränkungen gelten im Falle der Allgemeinverbindlichkeitserklärung auch für die nicht tarifgebundenen Unternehmer und Arbeitnehmer.

[96] BT-Drs 12/2948, vgl. auch 16. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz, 18.1

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Die Tatsache allein, dass Gesellschafter der Prüf- und Beratungsstelle selbst Gebäudereinigungsunternehmen unterhalten, die sich im direkten Wettbewerb zu den zu prüfenden Unternehmen befinden, reicht nicht aus, um bereits die missbräuchliche Verwendung der zur ordnungsgemäßen Durchführung der Prüf- und Beratungstätigkeit erforderlichen Informationen unterstellen zu können.

Die nach § 5 Abs. 1 und 2 Tarifvertrag erhobenen Daten dürften kaum geeignet sein, um ein Konkurrenzunternehmen auszuforschen. Wir haben allerdings den Geschäftsführern der Prüf- und Beratungsstelle empfohlen, bei einem Auskunftsverlangen eines Gesellschafters nach § 51 a GmbHG auf Einsicht in personenbezogene Daten zu prüfen, ob dem Gesellschafter eine derartige Einsicht nach § 51 a Abs. 2 GmbHG verweigert werden kann. Danach dürfen die Geschäftsführer die Auskunft und die Einsicht verweigern, wenn zu besorgen ist, dass der Gesellschafter sie zu gesellschaftsfremden Zwecken verwenden und dadurch der Gesellschaft oder einem anderen Unternehmen ein nicht unerheblicher Nachteil zugefügt wird.

Die Prüf- und Beratungsstelle wird unsere Anregung aufgreifen und außerdem jede Datenübermittlung personenbezogener Daten an die Gesellschafter dokumentieren. Wir haben gegenüber der Prüf- und Beratungsstelle darauf hingewiesen, dass die Datenübermittlungsregelung des § 5 Abs. 3 Tarifvertrag datenschutzrechtlich bedenklich ist, insbesondere da nicht ausgeschlossen werden kann, dass auch sensitive Arbeitnehmerdaten an die GmbH übermittelt werden müssen. Aus rechtsstaatlicher Sicht ist insbesondere problematisch, dass unklar bleibt („auf besondere Anforderung“), in welchen Fällen die Prüf- und Beratungsstelle von ihrem Recht nach § 5 Abs. 3 Tarifvertrag Gebrauch machen wird. Auch lässt sich aufgrund der unklaren Formulierung nicht eindeutig feststellen, welche Daten im Einzelnen angefordert werden können. Die Prüf- und Beratungsstelle hat sich aufgrund unserer Bedenken bereit erklärt, § 5 Abs. 3 Tarifvertrag bis auf weiteres nicht anzuwenden.

Privatisierung eines Krankenhauses

Ein Krankenhaus sollte privatisiert werden. Hierzu wurde ein Überleitungsvertrag mit dem privaten Betreiber geschlossen. Bezüglich der Personalakten enthielt der Überleitungsvertrag folgende Regelung:

„...im Zuge des Betriebsübergangs auf die Gesellschaft werden die Personalakten der Arbeitnehmerinnen und Arbeitnehmer, deren Arbeitsverhältnisse auf die Gesellschaft übergehen, unter Beachtung der einschlägigen datenschutzrechtlichen Regelungen übereignet.“

Hiervon ausgenommen wurden Nebenakten, die den Zusatzfragebogen zur Überprüfung durch die Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (BStU) beinhalten. Der neue Betreiber verpflichtete sich, die sich aus derartigen Unterlagen und Mitteilungen ergebenden Informationen nicht zu Lasten

betroffener Arbeitnehmerinnen und Arbeiternehmer zu verwenden.

Trotz des Betriebsübergangs liegt bei der Privatisierung eines staatlichen Krankenhauses eine Datenübermittlung vor, da die speichernde Stelle (hier der Bezirk) nicht untergeht.

Der neue Betreiber des Krankenhauses tritt nach § 613 a Bürgerliches Gesetzbuch (BGB) in die Rechte und Pflichten aus den im Zeitpunkt des Übergangs bestehenden Arbeitsverhältnissen ein. Nach § 28 BDSG dürfen alle personenbezogenen Daten an den neuen Betreiber übergeben werden, die erforderlich sind, um bezüglich der bestehenden Arbeitsverhältnisse alle bestehenden Rechte und Pflichten wahrzunehmen bzw. zu erfüllen.

Trotz des Betriebsübergangs werden die bisherigen Arbeitsverhältnisse fortgesetzt. Weder an der Tätigkeit noch an dem Aufgabenfeld der jeweiligen Mitarbeiter ändert sich etwas. Die mit dieser Tätigkeit in Verbindung stehenden Personaldaten stehen auch dem neuen Träger zu, da sie unmittelbar das gleiche Arbeitsverhältnis betreffen. Der Arbeitnehmer hat auch kein berechtigtes Interesse daran, dem neuen Arbeitgeber gegenüber wie ein neuer Arbeitnehmer aufzutreten, über den noch keine Daten erhoben worden sind (alte Fehlzeiten und arbeitsrechtliche Verfehlungen wirken also fort). Zumindest teilweise dürften die Personalakten sensitive Daten im Sinne des § 3 Abs. 9 BDSG enthalten (Schwerbehinderung, Gewerkschaftszugehörigkeit etc.). Die Übermittlung derartiger Daten ist nach § 28 Abs. 6 Nr. 3 BDSG zulässig, soweit 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.

Eine Übermittlung von Daten, die ausschließlich das öffentlich-rechtliche Arbeitsverhältnis betreffen, ist demgegenüber nur dann rechtmäßig, wenn diese Daten im Rahmen des Vertragsverhältnisses zwischen Arbeitnehmer und privatrechtlichem Arbeitgeber erforderlich sind. Dies dürfte in der Regel nicht der Fall sein (z. B. bei Unterlagen der BStU).

Konkurrentenklage

Zwei Berliner Universitäten baten um Auskunft, ob in einem Bewerbungsverfahren dem unterlegenen Bewerber bei der Mitteilung, dass die Auswahlentscheidung auf eine andere Person gefallen ist, auch der Name des erfolgreichen Bewerbers benannt werden muss bzw. darf.

Nach der Rechtsprechung des Bundesverfassungsgerichts ist dem unterlegenen Bewerber um eine Stelle die Möglichkeit einzuräumen, mit einer Klage auf Neubescheidung Rechtsschutz gegen die Ablehnung seiner Bewerbung in Anspruch zu nehmen[97]. Im Rah-

[97] Beschluss vom 19. September 1989, Az.: 2 BvR 1576/88

men dieses Verfahrens kann die vorausgegangene Auswahlentscheidung auch auf einen möglichen Verstoß gegen Artikel 33 Abs. 2 GG überprüft werden. Eine solche Klage kann aber nach der endgültigen Besetzung der umstrittenen Planstelle durch den erfolgreichen Mitbewerber von vornherein keinen Erfolg mehr haben, da dessen Ernennung nicht mehr rückgängig gemacht werden könnte. Eine rechtzeitige Klage in diesem Zusammenhang setzt daher voraus, dass der unterlegene Bewerber innerhalb einer für seine Rechtsschutzentscheidung ausreichenden Zeitspanne vor der Ernennung des Mitbewerbers durch eine Mitteilung der ausschreibenden Stelle Kenntnis vom Ausgang des Auswahlverfahrens erlangt.

Eine Übermittlung von personenbezogenen Daten des erfolgreichen Bewerbers liegt im Rahmen der Zweckbestimmung des vertragsähnlichen Vertrauensverhältnisses, soweit die Namensnennung erforderlich ist, um die Rechte der unterlegenen Bewerber zu gewährleisten (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Bei Datenübermittlungen in diesem Umfang kann davon ausgegangen werden, dass die Übermittlung zur Wahrung berechtigter Interessen eines Dritten (des unterlegenen Bewerbers) erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat (§ 28 Abs. 3 Satz 1 Nr. 1 BDSG). Wer an einer öffentlichen Ausschreibung teilnimmt, muss von vornherein davon ausgehen, dass in dem dargestellten Umfang seine personenbezogenen Daten an Dritte - hier unterlegene Bewerber - übermittelt werden. Zu der gleichen Wertung kommt man auch bei dem bei Beamten anzuwendenden Personalaktenrecht. Nach § 56 d Abs. 2 LBG dürfen Auskünfte an Dritte erteilt werden, wenn die Auskunftserteilung aufgrund höherrangiger Interessen eines Dritten zwingend erforderlich ist. Das Rechtschutzinteresse des unterlegenen Bewerbers ist hier höher zu gewichten als das Datenschutzinteresse des betroffenen Beamten. Da nicht jeder unterlegene Bewerber versuchen wird, seine Einstellung im Klageweg zu erzwingen, ist die automatische Namensnennung nicht erforderlich und damit rechtswidrig.

Bürgernaher öffentlicher Dienst

Immer mehr öffentliche Stellen erwarten von ihren Mitarbeitern, dass sie gegenüber dem Bürger den vollständigen Namen bekannt geben. So enthalten teilweise dienstliche E-Mail-Adressen den Vornamen des Bediensteten, der Mitarbeiter wird aber auch aufgefordert, etwa bei belastenden Verwaltungsakten seinen vollständigen Namen anzugeben. In der Notaufnahme eines öffentlichen Krankenhauses wurde das Personal aufgefordert, Namensschilder mit Vor- und Zunamen zu tragen.

Die Verarbeitung und Nutzung personenbezogener Daten ist nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit dies im Rahmen der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen erforderlich ist. Für die Zuteilung der in einer Behörde eingehenden

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

E-Mails ist die Nennung des vollständigen Namens auf der E-Mail-Adresse nicht erforderlich. Auch der Adressat eines (belastenden) Veraltungsaktes oder der Patient in der Notaufnahme benötigt den vollständigen Namen des öffentlich Bediensteten nicht.

Zu berücksichtigen ist allerdings, dass es in der Privatwirtschaft bei Dienstleistungen immer mehr üblich ist, dass sich Mitarbeiter mit Vor- und Nachnamen vorstellen, um eine größere Kundennähe zu zeigen. Auch im öffentlichen Dienst soll die Nennung des vollständigen Namens als Element der Verwaltungsreform zu einer größeren Bürgernähe führen. Insofern ist der Wunsch des Arbeitgebers nach vollständigem Namen durchaus nachvollziehbar.

Auf Seiten der Arbeitnehmer gibt es allerdings verschiedene Beweggründe, sich gegen die Preisgabe des vollständigen Namens zu wehren. So kann etwa bei Vornamen wie Achmed oder Moses auf die Religionszugehörigkeit des Arbeitnehmers (sensitives Datum, vgl. § 3 Abs. 9 BDSG) geschlossen werden. Insbesondere weibliches Krankenhauspersonal möchte nicht, dass Patienten aufgrund des vollständigen Namens die Möglichkeit haben zu versuchen, private Kontakte zu knüpfen. Insbesondere bei belastenden Verwaltungsakten (Nichtgewährung einer Baugenehmigung, Verweigerung von Sozialhilfe, Ausweisungsverfügung etc.) befürchten betroffene Mitarbeiter private Belästigungen, die bis zu persönlichen Bedrohungen für die Mitarbeiter und ihre Familien führen können.

Das berechtigte Anliegen einer bürgernahen Verwaltung darf nicht dazu führen, dass Mitarbeiter zur Bekanntgabe ihres Vornamens gezwungen werden. Wir empfehlen deshalb, dass jedem Mitarbeiter ein Widerspruchsrecht gegen die Preisgabe seines Vornamens eingeräumt werden sollte.

So sinnvoll aus reformerischer Sicht der persönliche Kontakt zwischen Verwaltung und Bürger mit voller Nennung von Vor – und Zunamen ist, sollte dies keinen verpflichtenden Charakter haben. Insoweit stimmt der Senat dem Votum des Berliner Beauftragten für Datenschutz und Informationsfreiheit zu, Mitarbeiterinnen und Mitarbeitern der Verwaltung ein Widerspruchsrecht gegen die Angabe des Vornamens einzuräumen.

Leichtfertiger Umgang mit Personaldaten

In mehreren Fällen haben wir einen leichtfertigen Umgang mit Personaldaten festgestellt:

Die Mitarbeiter eines Bauamtes müssen zur Verbesserung der Arbeitsorganisation (Koordinierung) in einer Liste den Dienstbeginn und das Dienstende eintragen. Diese Liste ist nicht nur allen Mitarbeitern, sondern auch den Besuchern des Bezirksamtes frei zugänglich (die Liste befindet sich im Flur).

In einem Krankenhaus wird ein Ordner geführt, in dem die (für die Mitarbeiter attraktiven) Bereitschaftsdienste und Rufbereitschaftsdienste geführt werden. Dieser Ordner ist allen Mitarbeitern zugänglich, so dass Mitarbeiter Auswertungen vornehmen können, wer bei der Zuteilung von Diensten bevorzugt bzw. benachteiligt wurde.

In einem anderen Krankenhaus wird ein Bereitschaftsdienstbuch geführt, in dem dokumentiert werden muss, welcher Zeitaufwand für die ärztliche Tätigkeit jeweils

erforderlich war. Dieses Dienstbuch ist für die Ärzte und Krankenschwestern einsehbar.

Arbeitnehmerdaten dürfen nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG als Mittel für die Erfüllung eigener Geschäftszwecke genutzt werden, soweit dies im Rahmen der Zweckbestimmung des Vertragsverhältnisses mit dem Betroffenen erforderlich ist. Arbeitnehmerdaten können danach verarbeitet und genutzt werden, soweit dies zur Koordinierung des Dienstbetriebes, zur angemessenen Kontrolle des Einzelnen oder allgemein für Controlling-Maßnahmen (Qualitätssicherung) erforderlich ist. Die personenbezogenen Daten der Arbeitnehmer sollten aber nur denjenigen zugänglich gemacht werden, die diese Daten zur Umsetzung des jeweiligen Zwecks auch benötigen.

Zur Koordinierung der Bauamtsmitarbeiter ist es nicht erforderlich, den genauen Dienstbeginn und das Dienstende einzutragen, für die Koordinierung erforderlich ist nur das Ein- bzw. Austragen des jeweiligen Mitarbeiters. Wir haben deshalb empfohlen, bei der Liste auf eine genaue Zeitangabe zu verzichten. Die Liste sollte nur denjenigen zugänglich sein, die diese für ihre Koordinierungsaufgabe benötigen, dies sind jedenfalls nicht die Besucher des Bezirksamtes.

Der Ordner mit den Bereitschaftsdiensten ist insbesondere von denen einzusehen, die die Stundenpläne erstellen und koordinieren. Über die Bereitschaftsdienste anderer Kollegen ist der einzelne Mitarbeiter nur insoweit zu informieren, als dies für seine Arbeit erforderlich ist. Nicht vertretbar ist, dass die Mitarbeiter nicht nur den gesamten Monatsdienstplan einsehen können, sondern auch die Diensthäufigkeit bei den einzelnen Kollegen über einen längeren Zeitraum (hier ab Januar 2000).

Dem Bereitschaftsdienstbuch in der Notaufnahme kann entnommen werden, mit welchem Zeitaufwand ein bestimmter Arzt eine bestimmte Leistung erbracht hat. Dies soll zur Qualitätssicherung des Bereitschaftsdienstes erforderlich sein. In dem Krankenhaus ging man davon aus, dass es rechtmäßig sei, wenn das „Kollektiv“ jeden einzelnen Mitarbeiter kontrolliert. Da diese Kontrolle aber nur dem Chefarzt zusteht, darf das Bereitschaftsdienstbuch auch nur diesem zugänglich sein. Wir haben deshalb empfohlen, das Bereitschaftsdienstbuch durch Bereitschaftsdienstbögen zu ersetzen, die an den Chefarzt weitergeleitet werden.

4.4.2 Gesundheit

Patientendaten im Leistungssystem

Immer wieder haben wir Hilferufe der Krankenhäuser erhalten, weil die Krankenversicherungen Krankenhausentlassungsberichte anforderten, obwohl dies in dem Leistungssystem des Sozialgesetzbuchs V so nicht vorgesehen sei. Die Krankenversicherungen verweigerten im Gegenzug die Zahlung der Krankenhauskosten. In einem konkreten Fall lautete das Anforderungsschreiben der Krankenkasse wie folgt:

Zwar trifft es zu, dass der Begriff des Krankenhausentlassungsberichts im Sozialgesetzbuch Fünftes Buch (SGB V) nicht verwandt wird. Daraus wird jedoch nicht einhellig gefolgert, dass die zunehmende Praxis der Krankenkassen, von den Krankenhäusern ärztliche Unterlagen wie Entlassungsberichte anzufordern, um die Notwendigkeit und Dauer der stationären Behandlung (über)prüfen zu können, rechtswidrig ist.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

„Krankenhausbehandlung zu Lasten der gesetzlichen Krankenversicherung kann nur gewährt werden, wenn eine medizinische Notwendigkeit erkennbar ist. Aus den eingereichten Unterlagen (Verlängerungsbericht vom 24. Oktober 2000, 18. Januar 2001) war eine medizinische Notwendigkeit für eine stationäre Behandlung über den 27. Oktober 2000 hinaus nicht erkennbar. Der medizinische Dienst der Krankenversicherungen (MDK) hat lediglich eine beratende Funktion. Ob und in welchem Umfang der MDK eingeschaltet wird, entscheidet die Krankenkasse. Über die zu erteilende Kostenübernahme kann ebenfalls nur die jeweilige Krankenkasse entscheiden. Neue medizinische Gesichtspunkte, die eine erneute Überprüfung rechtfertigen würden, haben Sie uns nicht mitgeteilt. Nach Übersendung neuer medizinischer Stellungnahmen (z. B. Entlassungsbericht oder Kopie der Krankenakte) für den ärztlichen Dienst der BKK Berlin sind wir gern bereit, den o. g. Fall erneut zur Beurteilung vorzulegen. Wir möchten nochmals darauf hinweisen, dass die Entscheidung über das Vorliegen eines Leistungsanspruchs auf Krankenhausbehandlung allein der Krankenkasse obliegt. Der MDK hat lediglich die Aufgabe, den Versicherungsträger gutachterlich nach Maßgabe des § 275 Sozialgesetzbuch Fünftes Buch (SGB V) zu beraten.“

Die bislang dazu ergangene Rechtssprechung spricht den Krankenkassen vielmehr das Recht zu, zur diesbezüglichen Prüfung Behandlungsunterlagen oder auch sonstige Berichte anzufordern. Nach Ansicht der Gerichte ergibt sich dies bereits aus dem Umstand, dass die Krankenkassen nach dem Gesetz dazu verpflichtet sind, die Notwendigkeit und Wirtschaftlichkeit der Leistungen zu überprüfen. Die Krankenhäuser sind daher nach Ansicht des Bundessozialgerichts auch dazu verpflichtet, aussagefähige Dokumentationen über die Notwendigkeit der Behandlung zu führen.

Dieses Schreiben kennzeichnet das derzeitige Klima zwischen den Leistungspartnern, den Krankenhäusern und Krankenversicherungen. In einer spektakulär gewordenen Entscheidung des Landessozialgerichts vom 14. März 2001[98] wurde erwähnt, dass wegen Zahlungsverweigerung bei den Berliner Sozialgerichten „bisher ca. 5.600 Rechtsstreite herbeigeführt“ wurden. In der Presse[99] wurden die Worte der Richter aus der Verhandlung zitiert: „Wohl aber leidet die Rechtsstaatlichkeit in Berlin, wenn Behörden einander vor Gericht zögen, statt die gesetzlich vorgeschriebenen Schlichtungsregularien zu benutzen.“ Das Bundessozialgericht hat in der Revision das Urteil des Landessozialgerichtes am 13. Dezember 2001 zugunsten der Berliner Krankenhäuser bestätigt[100].

Soweit der Berliner Beauftragte für Datenschutz und Informationsfreiheit auf die Entscheidungen des Landessozialgerichts vom 14. März 2001 und des Bundessozialgerichts vom 13. Dezember 2001 Bezug nimmt, ist darauf hinzuweisen, dass es in diesen Entscheidungen nicht um die Frage nach der Zulässigkeit der Anforderung von Entlassungsberichten geht.

Die Berliner Krankenkassen hatten vielmehr wegen der von ihnen festgestellten überlangen Verweildauern der Patienten in Berliner Krankenhäusern die Kostenübernahmeerklärungen befristet und die Rechnungen der Krankenhäuser nur bis zum Datum des Fristendes bezahlt. Die Krankenkassen vertraten die Ansicht, dass die Krankenhäuser wegen der vergleichsweise überlangen Verweildauern die Notwendigkeit der stationären Behandlung über das Fristende hinaus darzulegen und zu beweisen hätten.

§ 112 Abs. 1 Satz 1 SGB V verpflichtet die Landesverbände der Krankenkassen und die Verbände der Ersatzkassen gemeinsam mit der Landeskrankenhausgesellschaft sowie die Mitgliedskassen, verbindliche Verträge zur Sicherstellung von Art und Umfang der Krankenhausbehandlung zu schließen. Die Regelungen dieser „Krankenhausüberprüfungsverträge“[101] verfeinern die Verpflichtungen der Krankenhäuser und der Krankenhausärzte sowie der Krankenkassen zu einer engen und zügigen Zusammenarbeit. Dieser vom Landessozialgericht Berlin als rechtlich unbedenklich qualifizierte Vertrag ist von den Krankenversicherungen gekündigt worden und wird derzeit vor der Schlich-

Das Landessozialgericht Berlin und das Bundessozialgericht entschieden, dass dieses Vorgehen nicht mit dem zwischen den Landesverbänden der Krankenkassen und der Berliner Krankenhausgesellschaft nach § 112 SGB V geschlossenen Vertrag über die Allgemeinen Bedingungen der Krankenhausbehandlung vereinbar sei. Um die Entscheidung des Krankenhausarztes über die Notwendigkeit und Dauer der Krankenhausbehandlung in Zweifel zu ziehen, müssten die Krankenkassen das in dem Vertrag vorgesehene sog. gestufte Verfahren einhalten, das heißt, einen Kurzbericht

[98] Az.: L 9 KR 203/00
[99] „Richterschelte für die Politik“. In: FAZ vom 29. März 2001, S. BS 1
[100] Az.: B 3 KR 11/01 R
[101] Vertrag zur Überprüfung der Notwendigkeit und Dauer der Krankenhausbehandlung im Sinne des § 112 Abs. 2 Nr. 2 SGB V

tungsstelle verhandelt. Die Versicherungen wollen eigene ärztliche Dienste neben dem Medizinischen Dienst der Krankenkassen einführen und die Überlassung des Krankenhausentlassungsberichtes durch eine Neufassung des Vertrags rechtlich absichern. Eine abschließende rechtliche Überprüfung des neuen Formulierungsentwurfs der Arbeitsgemeinschaft der Berliner Krankenkassen konnte noch nicht stattfinden. Fest steht jedoch, dass sich der Maßstab für die Zulässigkeit derartiger Vereinbarungen aus dem SGB V selbst ergeben muss. Mit dem Vertrag können keine zusätzlichen im Sozialgesetzbuch noch nicht enthaltenen Mitteilungspflichten begründet werden. Wir haben die Arbeitsgemeinschaft der Berliner Krankenkassen über diese rechtliche Grundvoraussetzung informiert und um deren rechtliche Einschätzung gebeten.

anfordern und ggf. eine Prüfung durch den Medizinischen Dienst einleiten.

Die für die Aufsicht über die Krankenkassen zuständige Senatsverwaltung hat immer wieder an die Beteiligten appelliert, diese Streitigkeit einvernehmlich beizulegen, bzw. sich anstelle der unsinnigen Klageflut auf einige wenige Musterprozesse zu verständigen. In Teilen ist eine außergerichtliche Streitschlichtung auch gelungen. Im Rahmen der Verhandlungen über das Budget 2000-2006 konnte die Arbeitsgemeinschaft der Krankenkassenverbände Berlin mit der Vivantes GmbH, Träger von 10 ehemaligen städtischen Krankenhäusern des Landes Berlin, eine Einigung über die sozialgerichtlichen Verfahren erzielen. In den Häusern der für Wissenschaft sowie für die Krankenkassenaufsicht zuständigen Senatsverwaltungen geführte Konsensgespräche mit den Universitätskliniken blieben hingegen ohne Erfolg.

Die Krankenkassen haben von dem Kündigungsrecht der Krankenhausüberprüfungsverträge gemäß § 112 Absatz 4 SGB V Gebrauch gemacht.

Bei den Verhandlungen über einen Neuabschluß stimmt der Senat mit der Auffassung des BlnBDI überein, dass die neuen Verträge nicht im Widerspruch zum SGB V stehen dürfen. Soweit damit allerdings die Frage nach der Zulässigkeit der Anforderung sogenannter Entlassungsberichte verbunden wird, verweist der Senat auf die eingangs erfolgten Ausführungen.

Datentransparenz

Die Kostensteigerung oder besser gesagt Kostenexplosion im Gesundheitswesen war auch die Ursache für die Entwicklung eines Arbeitsentwurfs des Bundesministeriums für Gesundheit für ein „Gesetz zur Verbesserung der Datentransparenz und des Datenschutzes in der gesetzlichen Krankenversicherung (Transparenzgesetz – GKV–TG). Dieser Entwurf ist im Zusammenhang mit den Maßnahmen zur Gesundheitsreform 2000 entstanden und soll dem Ziel dienen, unter Beibehaltung oder gar Verbesserung der Qualität der Versorgung im Gesundheitssystem (Qualitätssicherung) die entstehenden Kosten unter Kontrolle zu bekommen.

Die Landesdatenschutzbeauftragten haben zur Unterstützung des Bundesbeauftragten für den Datenschutz den Arbeitsentwurf kritisch überprüft und auf die Schwachstellen des Gesetzentwurfs hingewiesen, damit diese in künftigen Beratungen verbessert werden können. Auch bei diesem Gesetz muss das Ziel sein, den „gläsernen Patienten“ bei der gesetzlichen Krankenversicherung zu vermeiden. Die Verarbeitung von Nutzungs- und Leistungsdaten lässt Dateien und Register entstehen, die eine Sicherung der Patientenrechte auf Wahrung des Arztgeheimnisses und des Datenschutzes unmöglich machen, wenn nicht entsprechende Sicherungsklauseln eingebaut werden. Die Datenschutzbeauftragten haben zuverlässige Pseudonymisierungsverfahren verlangt und gefordert, Lösungen zu entwickeln, die dem Prinzip der Datensparsamkeit entsprechen. Das Bundesministerium für Gesundheit hat dem Bun-

desbeauftragten für den Datenschutz mitgeteilt, es werde das Konzept und die datenschutzrechtlichen Äußerungen hierzu prüfen und in die weiteren Überlegungen einbeziehen. Es ist derzeit jedoch nicht abzusehen, ob und wann dieses Gesetz endgültig verabschiedet wird.

Beihilfedaten

Das Abgeordnetenhaus hat in seiner Sitzung vom 27. September 2001 beschlossen:

„Der Senat wird aufgefordert, darauf hinzuwirken, dass die Krankenkassen des Landes Berlin bei ihren Informationssystemen eine Protokollierung aller Zugriffe einschließlich der Identität des Anfragenden einführen, um unberechtigte Zugriffe zu verhindern bzw. aufklären zu können."

Hintergrund war, dass die gesetzliche Krankenversicherung eine standardisierte Software nutzt, die Vorkehrungen zum Schutz vor unberechtigten Datenzugriffen nicht beinhaltet. Dies erweckte die Sorge, wie denn die Gesundheitsdaten der Beamten im staatlichen Beihilfeverfahren geschützt sind.

Im Rahmen der Beihilfeabrechnung werden keine spezifischen medizinischen Daten oder Diagnosen erfasst, sondern lediglich abrechnungsrelevante Daten. Dies sind: Rechnungsdatum und Rechnungsbetrag, deren Art (beispielsweise „ärztliche oder zahnärztliche Leistungen") sowie die darauf gewährte Beihilfe.

Eine Ausnahme bilden Aufwendungen, bei denen die Gewährung von Beihilfen an die Einhaltung bestimmter Fristen gebunden ist. Hier werden zusätzlich auch weitere Informationen archiviert, z. B. bei Sehhilfen, bei denen die Gläserstärke gespeichert wird, weil erst nach dem Ablauf von drei Jahren eine Beihilfe zu unveränderter Glasstärke geleistet werden darf. Für die Überwachung von Genehmigungsdaten werden ebenfalls weitere Daten abgelegt, beispielsweise die Anzahl der genehmigten psychiatrischen Sitzungen.

Für die Mitarbeiter der Beihilfestelle gibt es enge Zuständigkeitsregelungen, die den Zugriff nur auf bestimmte Fälle zulassen. Die Zugriffe sind dem Beihilfeabrechnungssystem (BABSY) nur im Rahmen der Benutzerprofile möglich. Bei jeder Änderung werden automatisch alle Benutzerprofile gedruckt und diese Unterlagen werden sechs Jahre lang aufbewahrt. Aufgrund der restriktiven Zugriffsrechte wird eine Protokollierung der Zugriffe nicht vorgenommen. Ein Zugriff auf zentral gespeicherte Arbeitsunfähigkeitsbescheinigungen mit Angabe der Diagnose wie bei den gesetzlichen Krankenversicherungen ist im Beihilfeabrechnungssystem nicht möglich. Die auf den eingereichten Rechnungen enthaltenen medizinischen Angaben werden gleichfalls nicht gespeichert. Das automatische Beihilfeabrechnungssystem wurde von uns unter datensicherheitstechnischen Gesichtspunkten überprüft und ergab, dass auch in technisch-organisatorischer Hinsicht keine Risiken bestehen, wie sie in den Dateien der Krankenversicherungen auftreten können.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Arztgeheimnis und Abschiebehaft

Abschiebegefangene fühlen sich nach ihrem eigenen Bekunden häufig nicht adäquat durch Angehörige des Polizeiärztlichen Dienstes behandelt. Wegen des fehlenden Vertrauens versuchen Abschiebegefangene gelegentlich Kontakt zu einem Arzt/einer Ärztin ihres Vertrauens außerhalb des Polizeiärztlichen Dienstes herzustellen. Von einem Interessenvertreter für Abschiebegefangene wurde der Standpunkt vertreten, dass nach seiner Auffassung eine Entbindung von der ärztlichen Schweigepflicht gegenüber der Haftvollzugsverwaltung durch den Patienten gegenüber dem hinzuzuziehenden Arzt nicht zur Auflage gemacht werden dürfe. Dies wird aber verlangt, bevor zugestimmt wird.

Die ärztliche Versorgung der Abschiebehäftlinge ist in § 11 Abschiebegewahrsamsgesetz geregelt. Eine freie Arztwahl ist dort ausdrücklich nicht vorgesehen, sondern nur ein Anspruch auf ärztliche Behandlung durch den „bestellten ärztlichen Dienst“. Die Senatsverwaltung für Inneres hat trotzdem unter Ziff. 2.7.5 Abs. 2 Gewahrsamsordnung die Möglichkeit einer an Bedingungen geknüpften Arztwahl eingeräumt: nämlich, dass die Zustimmung erteilt werden kann, wenn der Häftling den in Aussicht genommenen Arzt und die ärztlichen Mitarbeiter des Polizeipräsidenten in Berlin von der Schweigepflicht entbindet. Diese Bedingung ist unbedenklich. Denn wenn die Verwaltung den Häftlingen durch die Ausführungsvorschriften ein größeres Wahlrecht bei der Arztwahl einräumt, als das Gesetz selbst vorgesehen hat, kann sie die Inanspruchnahme dieses Rechts auch mit Auflagen und Bedingungen versehen, soweit es mit den gesetzlichen Zielen noch im Einklang steht. Die Bedingungen und Auflagen verletzen nicht den Grundsatz der Verhältnismäßigkeit, weil einerseits Häftlinge ärztlich fachgerecht versorgt, andererseits missbräuchliche Inanspruchnahmen der Vergünstigungen ausgeschlossen werden müssen. Sie sollen nicht den Häftling, der einen anderen Arzt wünscht, willkürlich schlechter stellen, sondern vielmehr eine notwendige Voraussetzung dafür sein, dass beurteilt werden kann, ob eine zusätzliche ärztliche Behandlung während der Abschiebehaft im überwiegenden gesundheitlichen Interesse eines Abschiebehäftlings erforderlich ist und angeordnet werden muss. Im Vergleich zu Strafgefangenen, die dem Strafvollzugsgesetz unterliegen, liegt sogar eher eine, wenn auch geringfügige, Besserstellung der Abschiebehäftlinge vor.

Wechselnde Verantwortung für Patientenunterlagen

Schon mehrfach hatten wir das Thema herrenloser Patientenunterlagen mit unterschiedlichen Institutionen erörtert. Es kommt immer wieder vor, dass Ärzte ihre Praxis hinterlassen, ohne dass der Verbleib der Patientenunterlagen hinreichend gesichert ist.

Die erbrechtliche Verantwortung der gesetzlichen Erben, beim Verkauf der Praxis die Verantwortung des

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Praxiskäufers (wobei die Zustimmung des Patienten für den Zugriff des Praxisnachfolgers gegeben sein muss) oder die standesrechtliche Verpflichtung, für die Patientenunterlagen Vorsorge auch für den Fall zu treffen, dass die Praxis aufgegeben und die ärztliche Tätigkeit beendet wird, bieten oft keinen hinreichenden Schutz für die Patientendaten in der Alltagswirklichkeit. Insbesondere dann nicht, wenn der Arzt die Aufbewahrung definitiv ablehnt und dabei auch strafrechtliche Risiken in Kauf nehmen will, wenn er keinen Praxisnachfolger findet, der diese Pflichten übernimmt, oder wenn er ohne Erben verstirbt. Zwar ist im letzten Fall der Fiskus Erbe mit der Folge, dass er auch die Pflichten in Bezug auf die Patientendokumentation als Fiskus miterbt, jedoch ergibt sich daraus noch keine Garantie für den fortdauernden Schutz der ärztlichen Schweigepflicht.

In Verhandlungen mit der Ärztekammer und der Senatsverwaltung für Arbeit, Soziales und Frauen unter Einbeziehung des Gesamtverbandes der Deutschen Versicherungswirtschaft e. V. wurden einige Modelle für eine Regelung dieser Situation erwogen, ohne dass jedoch eine befriedigende Lösung für den Verbleib tatsächlich herrenloser Patientenunterlagen gefunden wurde. Es wurde dabei die Auffassung vertreten, dass der Fiskus als Erbe die Verwaltung der Patientenunterlagen übernehmen müsse. Dies wurde kontrovers zwischen der Ärztekammer und der Senatsverwaltung diskutiert. Es ist zwar nicht zu leugnen, dass Kosten entstehen, wenn Unterlagen in größerem Umfang verwaltet werden müssen. Dies zeigt auch die Verwaltung des Aktenbestandes aus ehemaligen Einrichtungen des DDR-Gesundheitswesens, der nach der Vereinigung von den Gesundheitsämtern übernommen wurde.

Von der für die Aufsicht über die Ärztekammer zuständigen Senatsverwaltung ist eine Problemlösung für die allerdings geringe Zahl der Fälle beabsichtigt, in denen die Funktion der Ärztekammer als Berufsvertretung der Ärzte deutlich wird. Die abschließende Regelung eines praktikablen Verfahrens, in dem ggf. auch andere Organisationen in Anspruch genommen werden, ist noch nicht festgelegt.

Dieser historische Ausnahmefall kann jedoch nicht Maßstab für ein brauchbares Konzept des in Zukunft anfallenden Patientenaktenbestandes sein. Wir empfehlen, Vorschläge, herrenlose Patientenunterlagen durch eine öffentliche Stelle zu übernehmen, weiterhin zu prüfen und dabei auch über kostendämpfende Maßnahmen nachzudenken. Wenn die Patientendaten wirklich herrenlos sind, wäre in erster Linie daran zu denken, diese Unterlagen den Patienten selbst auszuhändigen, soweit diese noch auffindbar sind. Es könnten Kostenträger gefunden werden, die zumindest in Höhe der Erbmasse herangezogen werden könnten. Schließlich muss daran gedacht werden, dass diese Unterlagen nicht auf ewig, sondern nur für einen Zeitraum von zehn Jahren nach Abschluss der Behandlung aufzubewahren sind. Und letztlich darf nicht vernachlässigt werden, dass angesichts der allgemeinen Übung, bei einem Praxisverkauf auch die Patientenunterlagen mitzuveräußern, die Herrenlosigkeit von Patientenunterlagen ohnehin nur einen Ausnahmefall bildet.

Zu prüfen war für uns die Frage, wie mit Patientenunterlagen des geschlossenen Krankenhauses Moabit zu verfahren ist. Keine Bedenken bestanden, dass einer Übertragung der Krankenhausfunktionen auf andere Krankenhausträger auch die Übertragung der diesbe-

Für die Patientenunterlagen des geschlossenen Krankenhauses Moabit zeichnet sich unter Beachtung des § 9 Krankengeschichtenverordnung eine Übernahme in das Archiv eines anderen Krankenhauses ab.

züglichen Patientendokumentationen folgt, weil die ärztlichen Garantien erhalten bleiben. Darüber hinaus aber müssen die Patientenunterlagen des Krankenhauses Moabit, so wie es die Krankengeschichtenverordnung vorsieht, im Einvernehmen mit dem zuständigen Bezirksamt so versorgt werden, dass Unbefugte nicht Einsicht nehmen können (§ 9 Krankengeschichtenverordnung).

Die orwellsche Angst im Operationssaal

„Big Brother im Operationssaal!" "Videoüberwachung von OP-Sälen schreckt Ärztekammer auf!" „Kameras im OP-Bereich gehören zum Sicherheitskonzept eines Berliner Privatkrankenhauses - Klinikärzte wollen von den „geschickt getarnten" Kameras im OP lange nichts gewusst haben. Auch Patienten waren ahnungslos - „Schwere Eingriffe in das Vertrauensverhältnis zum Arzt und in die Persönlichkeitsrechte der Patienten" - So lauteten die Schlagzeilen in einigen Zeitungen"[102].

Die Überprüfung ergab, dass in dem betroffenen privaten Krankenhaus die angstvollen Erwartungen nicht bestätigt wurden. Es gab zwar einige Mängel, weil die tatsächlich vorhandenen festinstallierten Kameras keine Funktionsanzeige aufwiesen und von Laien schon wegen ihrer Gestalt kaum als Videokamera erkennbar waren, jedoch konnten wir mit den uns zur Verfügung stehenden Überprüfungskompetenzen keine „skandalöse Videoaufzeichnung" erkennen.

Nach § 6 b BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) für die Aufgabenerfüllung öffentlicher Stellen oder zur Wahrnehmung des Hausrechts prinzipiell zulässig. Sie kann aber auch zur „Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke" erforderlich und zulässig sein, wenn keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Ein Operationssaal ist natürlich kein öffentlicher Raum im Sinne dieser Vorschrift. Die Zulässigkeit der Videoüberwachung im privaten Bereich ist daher mit der Rechtsprechung des Bundesgerichtshofs am Recht des eigenen Bildes zu messen[103]. Die spezialgesetzliche, der Gewährleistung des Rechts am eigenen Bild dienende Regelung des § 22 Kunsturhebergesetz (KUG) gewährt zwar keinen Schutz gegen die Herstellung von Abbildungen, sondern nur gegen deren unzulässige Verbreitung oder öffentliche Zurschaustellung. Der Bundesgerichtshof geht jedoch davon aus, dass das Recht am eigenen Bild eine besondere Erscheinungsform des allgemeinen Persönlichkeitsrecht darstellt. Die Herstellung eines Bildnisses ohne Einwilligung des Abgebildeten stellt damit einen unzulässigen Eingriff in dessen nach § 823 Abs. 1 BGB geschütztes allgemeines Persönlichkeitsrecht dar. Dabei wird das allgemeine Persönlichkeitsrecht des Betroffenen nicht nur im Fall einer „Bildniserschleichung" verletzt, in dem etwa

[102] Focus 5/2001, S. 2; Ärztezeitung vom 30. Januar 2001; Berliner Ärzte 3/2001, S. 7
[103] Urteil vom 25. April 1995, Az.: VI ZR 272/94 (KG). In: NJW 1995, S. 1955 ff.

Abbildungen einer Person in deren privatem Bereich gefertigt werden in der Absicht, sie der Öffentlichkeit zugänglich zu machen. Vielmehr kann auch die Herstellung von Bildnissen einer Person, insbesondere die Filmaufzeichnung mittels Videogerät, einen unzulässigen Eingriff in das Persönlichkeitsrecht des Betroffenen darstellen.

Diesem gewichtigen Eingriff in das allgemeine Persönlichkeitsrecht standen auf der anderen Seite keine diesen aufwiegenden Gründe entgegen, die sich aus rechtlich geschützten Belangen der Klinik ergeben könnten. Auch das Eigentumsrecht und die Verfügungsbefugnis am Operationssaal rechtfertigen diesen Eingriff gegenüber dem allgemeinen Persönlichkeitsrecht von Patienten und ärztlichen Mitarbeitern bzw. Belegärzten nicht. Wir haben deshalb auf die Erforderlichkeit einer ausdrücklichen Zustimmung sowohl der Ärzte wie auch der Patienten hingewiesen. Patienten und Ärzte sind über die Existenz solcher Kameras aufzuklären. Die Zugriffsmöglichkeiten aufgezeichneter Daten sind auf Zwecke der ärztlichen Behandlung zu begrenzen.

Externe Schreibdienste

Ein datenschutzrechtliches Risiko stellen gerade im medizinischen Bereich externe Schreibbüros dar. Wir empfehlen, weiterhin auf externe Schreibdienste möglichst zu verzichten und stattdessen die Schreibkräfte in das Krankenhaus hineinzuholen.

Wir haben uns mit der Berliner Krankenhausgesellschaft darauf verständigt, dass dann, wenn externe Schreibdienste gleichwohl eingeschaltet werden sollen, die Patientendaten beim Schreibdienst anonymisiert werden sollten, so dass eine Zuordnung der sensiblen Patientendaten ausschließlich dem Krankenhaus, nicht aber dem Schreibbüro möglich ist. Ferner sollten bei der Vergabe von Schreibarbeiten an externe Schreibdienste folgende datenschutzrechtliche Optionen gewährleistet werden:

- Kontrollmöglichkeit und Kontrollpflicht über das Schreibbüro durch das Krankenhaus,
- Festlegung der Datensicherheitsmaßnahmen durch das Krankenhaus (z. B. Zugang zu den Daten nur mit einem Passwort, Löschung der Daten, Transport in verschlossenen Koffern) und schriftliche Bestätigung der Durchführung dieser Maßnahmen durch das Schreibbüro,
- Kündigungsrecht bei einem Verstoß gegen datenschutzrechtliche Bestimmungen.

Ergänzend hierzu sollte eine Einwilligungserklärung der Patienten eingeholt werden. Diese Erklärung sollte insbesondere folgende Punkte berücksichtigen:

- Dem Patienten muss eine echte Wahlmöglichkeit gegeben sein.
- Hat der Patient nicht eingewilligt, muss sichergestellt werden, dass die ihn betreffenden Schreibarbeiten im Krankenhaus selbst durchgeführt werden.

- Der Patient muss darüber aufgeklärt werden, dass seine Daten u. U. bei einem externen Schreibbüro nicht denselben Schutz genießen wie im Krankenhaus (Wegfall des Beschlagnahmeverbotes).
- Den Patienten sollten Name und Anschrift des Schreibdienstes bekannt gegeben werden.
- Auch bei Vorliegen einer Einwilligung dürfen Unterlagen nur im unbedingt erforderlichen Umfang an den externen Schreibdienst weitergegeben werden.

Kontrolle eines Krankenhauses der Vivantes GmbH

Die bezirklichen Krankenhäuser, die nicht geschlossen worden sind, wurden zu Beginn des Berichtsjahres privatisiert und unter dem Dach des Unternehmens Vivantes GmbH zusammengefasst. Für diese Krankenhäuser galt bis Ende 2000 das Berliner Datenschutzgesetz, danach das Bundesdatenschutzgesetz, das überdies im Laufe des Jahres wesentlich geändert worden ist. Wir haben eines dieser Krankenhäuser einer kursorischen datenschutzrechtlichen Kontrolle unterzogen. Wir können nur hoffen, dass das Kontrollergebnis nicht für die privatisierten Krankenhäuser repräsentativ ist. Wir haben nämlich schwerwiegende organisatorische und technische Mängel festgestellt, z. B.:

- Die Struktur der Informationstechnik erwies sich als nicht prüffähig. Übersichten, die bis 2000 nach dem Berliner Datenschutzgesetz erstellt werden mussten, existierten ebenso wenig wie Übersichten, die nach den danach anzuwendenden Bundesdatenschutzgesetzen zu fertigen waren. Auf unsere Anforderung zur Vorbereitung der Kontrollmaßnahme wurde eilig eine Übersicht über existierende IT-Systeme erstellt, aus der jedoch relevante Informationen über die in den Netzen fließenden Daten nicht entnommen werden konnten. Der Versuch, vor Ort zu genaueren Erkenntnissen zu gelangen, scheiterte an widersprüchlichen Aussagen über Art und Umfang der Vernetzung und möglicher Datenzugriffe. Angebliche Einzelrechner und angeblich isolierte lokale Netze erwiesen sich bei genauerem Hinsehen als vernetzt. Aus diesem Grunde konnten in dem Krankenhaus IT-Sicherheits- und Datenschutzrisiken nicht erfasst, damit schon gar nicht beherrscht werden. Die innerbetriebliche Organisation des Krankenhauses wurde den besonderen Anforderungen in keiner Weise gerecht, ein bedeutender Verstoß gegen Satz 1 der Anlage zu § 9 BDSG.
- Die unterirdischen Gewölbe und Gänge des Krankenhauses waren für Außenstehende ohne weiteres unbemerkt und schon gar nicht kontrolliert zu betreten. Damit gelangte man zu lebenswichtigen Infrastrukturen einschließlich der Glasfaserleitungen des Krankenhausnetzes. Durch diese Gänge gelangte man auch ungehindert in einen ansonsten zugangsgeschützten Raum mit IT-Infrastruktureinrichtungen (Wiring Center) einer Abteilung. Damit lagen erhebliche Risiken für die Zutrittskontrolle nach Nr. 1 der Anlage zu § 9 BDSG vor.

- Der Zugriff an Patientendaten wurde nicht über individuelle Passwörter, sondern über Gruppenpasswörter gesteuert. Damit lagen Schwächen der Zugangs- und Zugriffskontrolle nach Nr. 2 und 3 der Anlage zu § 9 BDSG vor. Die gesetzlich verlangte Eingabekontrolle nach Nr. 5 der Anlage zu § 9 BDSG war überhaupt nicht möglich, weil diese verlangt, dass die Person individuell in ein Protokoll aufgenommen werden muss, die Dateneingaben durchführt.
- Aktive IT-Systeme konnten von öffentlichen Fluren aus ungehindert erreicht werden. Eine Zutritts- und Zugangskontrolle nach Nr. 1 und 2 der Anlage zu § 9 BDSG fand nicht statt.

4.4.3 Soziales

Entschädigung für politisch und rassisch Verfolgte

Aufgrund der Novellierung des BDSG und des BlnDSG bedurfte das Entschädigungsverfahren für die politisch und rassisch verfolgten Opfer des Nationalsozialismus einer neuen Verfahrensgestaltung. Nach § 33 Gesetz über die Anerkennung und Versorgung der politisch, rassisch oder religiös Verfolgten des Nationalsozialismus (PrVG) und § 176 Abs. 1 Bundesentschädigungsgesetz (BEG) ist die Entschädigungsbehörde verpflichtet, von Amts wegen alle für die Entscheidung über den Antrag erheblichen Tatsachen auch in gesundheitlicher Hinsicht und zum gesetzlichen Verfolgungstatbestand (Verfolgung aus rassischen, ethnischen, politischen, religiösen Gründen) zu ermitteln. Die Erhebung, Verarbeitung und Übermittlung von Daten betrifft somit „besondere Daten“ im Sinne des § 3 Abs. 9 BDSG.

Für solche Daten ist die Verarbeitungsbefugnis nach § 28 Abs. 6 BDSG eingeschränkt, so dass hier eine Einwilligung der leistungsberechtigten Antragsteller erforderlich ist. Sie sind verpflichtet, auf die für ihren Anspruch erheblichen Tatsachen hinzuweisen. Daraufhin erfolgen in der Regel von der Entschädigungsbehörde Anfragen, insbesondere bei Finanzamt, Sozialamt, Sozialversicherungsträger, Ausländerbehörde, Einbürgerungsamt, Versorgungsamt, Berufsgenossenschaft sowie darüber hinaus bei der Jewish Claims Conference, dem Deutschen Roten Kreuz, dem Roten Kreuz Moskau, der Stiftung Hilfe für Opfer der NS-Willkürherrschaft, bei Einrichtungen der Jüdischen Gemeinde sowie des Office for Personal Compensation from Abroad und der Israelischen Nationalversicherung. Die Antragsteller werden darauf hingewiesen, dass Anfragen nur erfolgen, soweit sie nach dem vorgetragenen Sachverhalt für die Bearbeitung des Antrages erforderlich sind. Die Anfragen erfolgen im Interesse einer sachgerechten Leistungsprüfung. In einer ausdrücklichen Erklärung wird die Entschädigungsbehörde vom Antragsteller beauftragt, die zur Antragsbearbeitung erforderlichen Auskünfte einzuholen; die betroffenen Stellen werden von der Schweigepflicht entbunden. In einer gesonderten Einwilligungserklärung werden auch Ärzte, Krankenhäuser, Sozialversicherungen usw. von der Schweigepflicht entbunden,

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

um den Entschädigungsbehörden nach § 192 BEG die zur Antragsbearbeitung erforderlichen Auskünfte, soweit sie die Gesundheit der Antragsteller betreffen, zu erteilen. Dies entspricht der Zielsetzung des § 192 BEG, das Antragsverfahren so unbürokratisch wie möglich und auch so zügig wie möglich und zur Entlastung der Antragsteller durchzuführen. Durch die Neufassung der Einwilligungserklärung ist es gelungen, einige Irritationen, die durch eine zuvor geänderte Fassung der Erklärung entstanden waren, auszuräumen.

Die Polizei will eine Mutter verhaften

„*In unserem Jugendamt erschienen kürzlich zwei Kriminalbeamte, wiesen sich ordnungsgemäß aus und baten um Auskunft, in welche Kita das Kind einer bestimmten mit Haftbefehl gesuchten Mutter geht. Einen gerichtlichen Beschluss über diese Auskunft konnten die Beamten nicht vorlegen“, schrieb uns ein Jugendamt.*

Das Jugendamt möchte wissen, zu welchen Auskünften seine Mitarbeiter berechtigt bzw. verpflichtet sind. Die Antwort ergibt sich aus den Vorschriften der §§ 67 ff. Sozialgesetzbuch Zehntes Buch (SGB X). Nach § 68 Abs. 1 SGB X dürften zur Erfüllung von Aufgaben der Polizeibehörden nur Name, Vorname, Geburtsdatum, Geburtsort, derzeitige Anschrift, derzeitiger oder zukünftiger Aufenthalt sowie Namen und Anschriften des derzeitigen Arbeitgebers übermittelt werden. Der Kitaaufenthalt eines Kindes des Gesuchten ist dort nicht benannt, so dass eine Offenbarung nach § 68 SGB X nicht in Frage kommt. Die Offenbarungsbefugnis nach § 73 SGB X „zur Durchführung eines Strafverfahrens“ kommt hier nicht in Betracht. Denn für die Durchführung eines Strafverfahrens bedarf es einer richterlichen Anordnung, aus der sich Art und Umfang der zur offenbarenden Daten ergeben. Wird die richterliche Anordnung vorgelegt, ist ihr allerdings auch Folge zu leisten, soweit nicht Anhaltspunkte für eine prozessrechtliche Beschwerde erkennbar sind.

Die Senatsverwaltung für Bildung, Jugend und Sport hat in einem Fall der Beschlagnahme von Akten eines Jugendamts auf Grund richterlichen Beschlusses das betroffene Bezirksamt ersucht, hiergegen Beschwerde zum Landgericht Berlin zu erheben, um den Schutz der Sozialdaten sicher zu stellen. Ein anderes Bezirksamt hatte bereits zehn Jahre zuvor auf diese Weise die Verwertung zu Unrecht beschlagnahmter Unterlagen verhindert. Das neue Verfahren ist noch nicht abgeschlossen.

Zu der vom Berliner Beauftragten für Datenschutz und Informationsfreiheit vertretenen Rechtsauffassung ist Folgendes anzumerken:

Gemäß der vom Senat erlassenen „Allgemeinen Anweisung über die Übermittlung von Sozialdaten nach §§ 68 ff des SGB X vom 26.01.1999 dürfen nach § 68 Abs. 1 SGB X u.a. der derzeitige und zukünftige Aufenthalt der Betroffenen an die Polizeibehörden übermittelt werden. Dazu wird unter Punkt II.2. der Anweisung ausgeführt, dass bei Vorliegen eines Haftbefehls in jedem Fall der momentane oder wiederkehrende Aufenthalt in der Dienststelle eines Sozialleistungsträgers mitzuteilen ist. Der Senat hält die Rechtsauffassung der Polizei für vertretbar, wonach auch Angaben des Jugendamts zum Aufenthalt des Kindes der betroffenen Person in einer in seinen Zuständigkeitsbereich fallenden Kindertagesstätte von der Übermittlungsbefugnis mitumfasst sind, da diese Daten wiederum Rückschluss auf den – wiederkehrenden tatsächlichen – Aufenthalt der mit Haftbefehl gesuchten Person geben.

Wenn die Vollstreckung eines Haftbefehls nur auf diesem Wege möglich ist, sind diese Daten der Polizei bekannt zu geben. Dass in solchen Fällen in besonderer Weise auf die Verhältnismäßigkeit bei der Vornahme der Haftbefehlsvollstreckung zu achten ist, ist selbstverständlich.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Der ungeeignete Heimleiter

In einem Anordnungsverfahren wurde dem Träger eines Heimes die Weiterbeschäftigung eines Heimleiters aufgrund von Feststellungen untersagt, die unter anderem die persönliche Integrität des Heimleiters betrafen. Zur Begründung der Ungeeignetheit des Heimleiters waren eine rechtskräftige Verurteilung und ein Ermittlungsverfahren, das eingestellt worden war, herangezogen worden. Dem Träger des Heimes wurde eine angemessene Sachverhaltsschilderung gegeben.

Das Bezirksamt bat uns um fachliche Einschätzung, ob die in der Person des Heimleiters liegenden Versagungsgründe dem Träger des Heimes offenbart werden durften.

Nach § 13 Heimgesetz i. V. m. § 3 Abs. 1 der Verordnung über personelle Anforderungen für Heime konnte dem Träger des Heimes die Weiterbeschäftigung des Betroffenen als Heimleiter wegen dessen persönlicher Ungeeignetheit untersagt werden. Für die Untersagungsverfügung bestand eine Begründungspflicht. Diese entspricht einer Übermittlungsbefugnis bzw. -pflicht. Aus der Überwachungs- und Beratungsaufgabe ergibt sich eine Prüfpflicht der Heimaufsicht über die die Eignung des Heimleiters betreffenden Umstände. Durch diese Vorschriften soll dem Schutzgedanken gegenüber allen Heimbewohnern Rechnung getragen werden. Da der Träger eines Heimes das Arbeitsverhältnis mit dem Heimleiter nicht kündigen kann, wenn er nicht über hinreichende Kündigungsgründe im Sinne des Arbeitsrechtes verfügt, erstreckt sich die Begründungspflicht für die Untersagungsandrohung auch auf die persönlichen Mängel des Heimleiters, da ohne deren Weiterleitung der Heimträger das Dienst- oder Arbeitsverhältnis nicht wirksam auflösen kann. Gerade zum Schutz minderjähriger Kinder vor sexuellem Missbrauch oder Kindesmisshandlung muss der Träger eines Heimes darauf achten, dass er geeignete Dienstkräfte einstellt und weiterbeschäftigt, die der Verantwortung ihrer Aufgabe gewachsen sind, und er muss darauf achten, dass die Eignung der Heimleiter und Mitarbeiter objektiv und zweifelsfrei gegeben ist.

Mit dem zugrundeliegenden Vorgang sind die Senatsverwaltung für Bildung, Jugend und Sport bzw. das Landesjugendamt nicht befasst gewesen, da es sich ganz offensichtlich nicht um eine Jugendhilfeeinrichtung im Sinne des § 45 SGB VIII handelte. Die Handhabung dieses Vorganges durch Bezirksamt und Datenschutzbeauftragten entspricht jedoch vollständig auch dem Schutzgedanken des SGB VIII; das Landesjugendamt wird in gleich gelagerten Fällen ebenso verfahren.

4.4.4 Bauen, Wohnen, Umwelt

Liegenschaftskataster im Internet

Von der Senatsverwaltung für Stadtentwicklung wurden wir gebeten, uns zu den datenschutzrechtlichen Aspekten einer Bereitstellung von Daten aus dem Automatisierten Liegenschaftskataster im Internet zu äußern.

Die Bereitstellung von Daten aus dem Liegenschaftskataster im Internet stellt eine Einrichtung eines automatisierten Abrufverfahrens nach § 15 BlnDSG dar. Die Einrichtung von automatisierten Abrufverfahren für Daten aus dem Liegenschaftskataster ist durch § 17 Abs. 7 Satz 3 Vermessungswesengesetz (VermG) auf Behörden und öffentliche Stellen begrenzt.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Allerdings ist „Jedermann“ berechtigt, für Einzelfälle schriftliche Auskünfte aus dem Liegenschaftskataster zu erhalten (§ 17 Abs. 1 VermG). Weitere Voraussetzungen für den Auskunftsanspruch gibt es nicht. Eine Differenzierung nach bestimmten Datenarten entsprechend ihrer Sensibilität (z. B. Eigentümerangaben, allgemeine Grundstücksangaben) ist ebenfalls nicht gesetzlich vorgegeben. Die Regelung entspricht damit grundsätzlich den Vorgaben des „Jedermann-Privilegs“ in § 15 Abs. 4 BlnDSG, wonach es keiner eigenständigen gesetzlichen Regelung bedarf, um einen automatisierten Abruf der Daten aus dem Liegenschaftskataster zuzulassen. Vor diesem Hintergrund wäre eine Aufhebung der Einschränkungen für die Einrichtung eines automatisierten Abrufverfahrens in § 17 Abs. 7 Satz 3 VermG möglich.

Unberücksichtigt bliebe dabei jedoch, dass eine Veröffentlichung der Daten aus dem Liegenschaftskataster im Internet für die Betroffenen (z. B. Grundstückseigentümer, Nutzungsberechtigte usw.) – im Vergleich zum bestehenden Auskunftsverfahren – eine erheblich gesteigerte Eingriffsintensität bedeutet. Der Betroffene hat keine Wahl- bzw. Widerspruchsmöglichkeit. Seine Daten werden zwangsweise im Liegenschaftskataster erfasst. Während bei den bisherigen Formen des Abrufverfahrens die Übermittlung der personenbezogenen Daten regional begrenzt an einen konkret definierten Benutzerkreis erfolgt und eine Verbindung zu anderen Datenbeständen nur in Ausnahmefällen zulässig und möglich ist, bietet die Veröffentlichung der Daten im Internet weitergehende – die Persönlichkeitsrechte der Betroffenen erheblich beeinträchtigende – Möglichkeiten.

Die Veröffentlichung im Internet ermöglicht einen regional unbegrenzten Zugriff auf die Daten. Durch die Festlegung von bestimmten Suchkriterien können gezielt Profile (z. B. Konsumentenverhalten) zu einzelnen Personen definiert und automatisiert aus den Daten im Internet zusammengestellt werden.

Angesichts dieser Risiken und des damit verbundenen erheblichen Eingriffes in das Recht auf informationelle Selbstbestimmung des Betroffenen bestehen erhebliche Bedenken dagegen, dass die Daten über Eigentümer, Nutzungsberechtigte usw. aus dem Liegenschaftskataster im Internet bereitgestellt werden. Diese Bedenken bestehen insbesondere auch vor dem Hintergrund, dass unsere Empfehlung aus dem Jahr 1998[104], das Vermessungswesengesetz zu ändern und eine Auskunft aus dem Liegenschaftskataster – soweit sie sich auf die Daten zum Grundstückseigentümer, Nutzungsberechtigten usw. bezieht – nur nach Darlegung eines berechtigten Interesses zuzulassen, bisher von der Senatsverwaltung für Stadtentwicklung nicht aufgegriffen worden ist.

Im Vermessungswesen werden insbesondere die im Liegenschaftskataster enthaltenen Informationen über Grundstücke und Gebäude, Eigentümer, Erbbau- und Nutzungsberechtigte sowie über die in der Kaufpreissammlung enthaltenen Daten über den Grundstücksmarkt automatisiert geführt. Durch die zunehmende Verbreitung des Internet wurden in den letzten Jahren elektronische Medien auch in der Berliner Verwaltung für viele Tätigkeiten eingesetzt. Die damit verbundenen Erweiterungen der technischen Kommunikationsmöglichkeiten und die Forderungen der Wirtschaft, Informationen aus der Kaufpreissammlung und aus dem Liegenschaftskataster mit Hilfe des Internet verfügbar zu machen, machen es nunmehr erforderlich, die derzeitigen vom Berliner Beauftragten für Datenschutz und Informationsfreiheit bislang als vorbildlich bezeichneten bereichsspezifischen Datenschutznormen des Liegenschaftskatasters (vgl. Jahresbericht 1995) zu novellieren.

[104] JB 1998, 4.4.4

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Da durch die gesamtheitliche datenschutzrechtliche Sicht auf die Übermittlung personenbezogener Daten im Vermessungswesen mehrere Rechtsnormen zu ändern sind, ist beabsichtigt, die Änderungen wegen ihres Gesamtzusammenhanges in einem Artikelgesetz zur Anpassung der rechtlichen Rahmenbedingungen für den Einsatz elektronischer Medien im Vermessungswesen zusammenzufassen.

Anfang Dezember 2001 sind die Novellierungsansätze der Senatsverwaltung für Stadtentwicklung anhand eines Textentwurfes mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit eingehend diskutiert worden. In diesem Zusammenhang ist der im Jahresbericht 2001 genannten Empfehlung des BlnBDI Rechnung getragen worden.

Ordnungswidrigkeitenverfahren - Pflichtangaben im Anhörungsbogen

In einem Ordnungswidrigkeitenverfahren erhielt ein Petent vom Bauaufsichtsamt einen Anhörungsbogen mit Fragen zum Vor- und Familiennamen (Geburtsnamen), Geburtsdatum und –ort, zur Wohnanschrift, telefonischen Erreichbarkeit, zum Familienstand, zu Namen und Anschrift des gesetzlichen Vertreters, Beruf und monatlichem/wöchentli-chem Einkommen. Er wurde darauf hingewiesen, dass er keine Angaben zur Sache machen müsse, zu den Angaben der Personalien jedoch gesetzlich verpflichtet sei. Nur bei der Frage zum monatlichen/wöchentlichen Einkommen wurde auf die Freiwilligkeit der Angaben verwiesen. Ausführungen zur Rechtsgrundlage, aus der sich die Auskunftspflicht ergibt, waren dem Anhörungsbogen nicht zu entnehmen.

Geht es um die Feststellung seiner Identität, ist der Betroffene in einem Ordnungswidrigkeitenverfahren zur Auskunft über die Angaben zur Person verpflichtet (§ 111 OWiG i.V.m. § 163 b Abs. 1 StPO).

Die Verweigerung von Angaben über den Vor- und Familiennamen, ggf. Geburtsnamen, Ort und Tag der Geburt, Familienstand, Beruf, Wohnort, Wohnung und Staatsangehörigkeit wird mit einem Bußgeld sanktioniert (§ 111 Abs. 1 OwiG). Damit begründet diese Regelung jedoch noch keine Auskunftspflicht des Betroffenen für einen bestimmten Zweck (z. B. der Identitätsfeststellung). Sie knüpft vielmehr an andere Vorschriften an, in denen die Voraussetzungen und vor allem auch der Umfang der Auskunftspflicht festgelegt sind. Die Ermächtigung der Ordnungsbehörde, die Identität des Betroffenen festzustellen, lässt sich aus § 163 b Abs. 1 StPO ableiten. Danach dürfen von der Ordnungsbehörde die Personalien ermittelt werden, die für die eindeutige Feststellung einer Person und ihrer späteren Erreichbarkeit erforderlich sind. Es handelt sich dabei um Angaben zum Familien- und Vornamen, Geburtsnamen, Geburtstag und -ort und Wohnort. Nur zu diesen Angaben ist der Betroffene verpflichtet. Nicht erforderlich zur Feststellung der Identität sind dagegen Angaben zum Familienstand und zum Beruf. Entsprechende Fragen im Anhörungsbogen sind vom Betroffenen nur freiwillig zu beantworten.

Weitere Angaben, die sich auf das soziale Umfeld und die Lebensumstände des Betroffenen beziehen und Bedeutung für die Schuld und Schwere des Tatvorwurfes haben können, dürfen nach § 163 StPO ermittelt werden. Angaben über das Einkommen können z. B. als Grundlage für die Bemessung der Tagessatzhöhe bei einer Geldstrafe oder für eine Geldzahlung nach § 153 a Abs. 1 Nr. 2 StPO herangezogen werden. Der Betroffene ist jedoch nicht verpflichtet, diese Angaben zu machen. Die Erhebung dieser Daten kann nur auf die freiwillige Mitwirkung des Betroffenen gestützt werden. Darüber ist dieser nach §§ 163 a, 136 Abs. 1 Satz 2 bis 4 StPO ausführlich und verständlich zu belehren.

Ordnungswidrigkeitenverfahren - Speicherung von Wiederholungsfällen

Gegen einen Hundehalter wurde von der zuständigen Ordnungsbehörde ein erhöhtes Bußgeld „wegen des wiederholt frei Laufen lassens von zwei Hunden“ in einer öffentlichen Grünanlage verhängt. Der Vorsatz des Betroffenen wurde mit einem in der Vergangenheit liegenden gleichartigen Vorfall begründet. Auf Nachfrage wurde uns bestätigt, dass die Daten der Betroffenen (Personalien, begangene Ordnungswidrigkeit, Tatort, Tatzeit) auch nach Abschluss des Ordnungswidrigkeitenverfahrens weiter gespeichert bleiben.

Die Höhe des Bußgeldes ist nach pflichtgemäßem Ermessen zu berechnen (§ 17 OWiG). Dabei können Vorahndungen zum Nachteil des Betroffenen bei der Bemessung des zu verhängenden Bußgeldes als Teil des Tatvorwurfes berücksichtigt werden, wenn sie in einem sachlichen und zeitlichen Zusammenhang zur neuen Ordnungswidrigkeit stehen. Daten aus einem abgeschlossenen Vorgang können damit für die Zukunft gespeichert werden. Allerdings sind die Anforderungen an den sachlichen und zeitlichen Zusammenhang restriktiv auszulegen. Die Speicherdauer darf den Zeitraum nicht überschreiten, in dem der Betroffene mit der Berücksichtigung der Ordnungswidrigkeiten hätte rechnen müssen. Davon ist auszugehen, wenn sich der Wiederholungsfall innerhalb der in § 31 OWiG genannten Zeiträume für die Verfolgungsverjährung ereignet.

Ordnungswidrigkeitenverfahren – Auskünfte an den Anzeigenerstatter

Ein Anwohner, der sich durch die Lautstärke eines Straßenfestes beeinträchtigt fühlte, erstattete beim Umweltamt eine Anzeige gegen den Veranstalter wegen Lärmbelästigung. Auf Nachfrage wurde ihm einen Monat später bestätigt, dass gegen den Veranstalter ein Ordnungswidrigkeitenverfahren eingeleitet worden sei. Angaben dazu, ob – wenn ja, mit welchem Ergebnis – das Verfahren abgeschlossen worden sei, wurden ihm unter Hinweis auf den Datenschutz verweigert.

Die Übermittlung von personenbezogenen Daten durch das Umweltamt an einen privaten Dritten ist nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene darin eingewilligt hat (§ 13 BlnDSG). Für

Datenübermittlungen aus einem Ordnungswidrigkeitenverfahren besteht eine derartige Rechtsgrundlage in § 406 e Abs. 1, Abs. 5 StPO i.V.m. § 46 Abs. 1, Abs. 3 Satz 4 OWiG. Danach kann ein Rechtsanwalt für den Verletzten die Akten einsehen bzw. es kann dem Verletzten unmittelbar Auskunft aus den Akten gewährt werden. In beiden Fällen ist Voraussetzung, dass der Verletzte ein berechtigtes Interesse darlegt und schutzwürdige Interessen des Betroffenen oder anderer Personen dem Auskunftsinteresse nicht entgegenstehen. Die Entscheidung, ob Akteneinsicht oder -auskunft zu gewähren ist, trifft die Verwaltungsbehörde, die das Verfahren durchführt, und zwar nach Abschluss des Verfahrens.

Verletzter in einem Bußgeldverfahren ist derjenige, der durch die Ordnungswidrigkeit unmittelbar an seinem Körper, Eigentum oder Vermögen geschädigt wurde. Von einem berechtigten Interesse des Verletzten ist auszugehen, wenn dieser z. B. zivilrechtliche Ansprüche verfolgt oder abwehrt oder die Auskünfte in einem Verwaltungsstreitverfahren, Wideraufnahmeverfahren oder für ein Wiedereinsetzungsgesuch benötigt. Kein berechtigtes Interesse liegt vor, wenn die Auskunft lediglich der Ausforschung des Betroffenen dient oder auf bloße Neugier zurückzuführen ist. In die Abwägung zwischen dem berechtigten Interesse des Auskunftsuchenden und den schutzwürdigen Belangen des Betroffenen sind alle maßgeblichen Umstände einzubeziehen. Erhebliches Gewicht kann hierbei Angaben über die wirtschaftlichen Verhältnisse oder die Geschäftsgeheimnisse des Betroffenen zukommen. Die Akteneinsicht bzw. -auskunft kann im Zweifel auch auf einzelne Aktenteile beschränkt werden.

Im vorliegenden Fall lag die Wohnung des Auskunftsuchenden in unmittelbarer Nähe des Straßenfestes. Durch die Überschreitung der Lärmschutzbestimmungen wurde er zwar in seinen Rechten verletzt. Da er jedoch kein berechtigtes Interesse an der Auskunftserteilung darlegen konnte, wurde diese von der Ordnungsbehörde zutreffend – unter Hinweis auf den Datenschutz – verweigert.

4.5 Wissen und Bildung

4.5.1 Statistik

5. Dezember 2001: Test für registergestützte Volkszählung

Ende Juli 2001 verabschiedete der Bundestag ein Gesetz zur Vorbereitung eines registergestützten Zensus. Hauptbestandteil ist das Zensustestgesetz[105]. Seit dem Jahresbericht des Berliner Datenschutzbeauftragten von 1996 – damals unter der Überschrift „Volkszählung 2001, 2002, 2003 ...?“ - begleiteten wir die einsetzende Methodendiskussion[106]. Auch jetzt ist noch nicht absehbar, wann nach Auswertung der Tests eine Ent-

[105] Gesetz zur Vorbereitung eines Registergestützten Zensus vom 27. Juli 2001, BGBl. I S. 1882-1886
[106] JB 1996, 4.5.3

scheidung zwischen einem registergestützten Zensus oder einer klassischen Volkszählung fällt.

Der für den Zeitraum ab 5. Dezember 2001 anberaumte Probelauf für die Volkszählung soll erweisen, ob eine Zusammenführung der Daten aller Melderegister beim Statistischen Bundesamt und die Koppelung mit Dateien der Bundesanstalt für Arbeit ein Ergebnis erbringt, das dem einer herkömmlichen Volkszählung ähnlich ist.

Das Modell eines registergestützten Zensus sieht vor,

- auf flächendeckende Begehungen wie in früheren Volkszählungen zu verzichten und stattdessen die Bevölkerungsdaten der Einwohnermelderegister auszuwerten,
- diese Daten vor der statistischen Verwendung auf Fehler (Doppeleintragungen) zu untersuchen und durch Nachfragen bei den Betroffenen statistikintern, also ohne Auswirkungen auf das Melderegister, zu bereinigen,
- verschiedene Dateien - so auch die der Bundesanstalt für Arbeit - zur Erwerbstätigkeit mit den Daten aus den Einwohnerregistern zu verknüpfen,
- eine postalische Gebäude- und Wohnungszählung bei den Gebäudeeigentümern durchzuführen und neben Gebäude- und Wohnungsangaben auch die Namen der Wohnungsinhaber zu erfragen,
- Haushaltszusammenhänge nicht mehr durch die Befragung der Betroffenen, sondern aus den vorliegenden Informationen maschinell zu erzeugen,
- durch die Kombination der verschiedenen Dateien Inplausibilitäten einzelner Datenbestände aufzudecken und durch Nachfragen statistikintern zu bereinigen.

Im Ergebnis würde dann für jede Person ein Zensusdatensatz erzeugt, der in allen Merkmalskombinationen sowohl sachlich als auch regional tief gegliederte statistische Auswertungen erlaubt.

Im Zensustestgesetz sind umfangreichere Erhebungen als bei einem späteren registergestützten Zensus erforderlich. Um das Ergebnis der Tests bewerten zu können, ist parallel dazu wie bei einer klassischen Volkszählung eine Begehung der ausgewählten Gebäude und eine Befragung aller dort lebenden Personen notwendig. Mit drei verschiedenen Tests wird die Geeignetheit dieser neuen Methode überprüft. Dazu werden aus allen Meldebehörden die Daten der Einwohner, die am 1. Januar, am 15. Mai und am 1. September geboren sind oder ein unvollständiges Geburtsdatum haben, an das Statistische Bundesamt übermittelt. Die Datensätze werden im Statistischen Bundesamt zentral daraufhin geprüft, ob für jede Person nur ein Hauptwohnsitz bzw. ob eine Hauptwohnung für eine Person mit Nebenwohnsitz gegeben ist. Zugleich sollen damit die Übermittlungswege und die Liefermöglichkeiten der Gemeinden getestet werden.

Mit einer weiteren zweistufigen Stichprobe werden bundesweit etwa 38.000 Gebäude mit etwa 250.000 Wohnungen und 550.000 Personen überprüft. Für die in diesen Gebäuden lebenden Personen werden von den betroffenen Gemeinden die Datensätze angefordert. Mittels einer Begehung durch Zähler der statistischen Landesämter und einem Vergleich mit den übermittelten Melderegisterdaten wird festgestellt, wie hoch die Über- oder Untererfassung in den Registern ist. Obwohl in Berlin nur 320 Adressen erfasst sind, sind unter diesen Anschriften ca. 12.000 Personen gemeldet. In einer Unterstichprobe soll dann für einen Teil dieser Gebäude der Eigentümer postalisch nach Gebäude- und Wohnungsangaben sowie den Namen der Wohnungsinhaber befragt werden. Damit soll festgestellt werden, inwieweit die Eigentümer zu einzelnen Wohnungen korrekte Angaben machen und ob sie die für die Haushaltegenerierung benötigten Namen der Wohnungsinhaber sowie die Zahl der Wohnungsnutzer angeben können. In einem weiteren Test sollen - wie im Jahresbericht 2000 bereits dargestellt - maschinell die Bewohner zu Haushalten zusammengeführt werden. Dies ist das Kernstück des Modells, aber auch der mit Abstand komplizierteste Teil. Denn auch die Interviewer müssen nicht nur wie bei bisherigen Zählungen fragen, wer zu dem oder den in der Wohnung lebenden Haushalten gehört, sondern auch die Merkmale erfragen, die bei der maschinellen Generierung der Haushalte benötigt werden. Nur so lassen sich Programmfehler aufdecken.

Aber genau solche Fragen sind für die Betroffenen allerdings nur schwer als für die Statistik erforderlich nachvollziehbar.

Beispiele aus dem Fragebogen:

Sind Sie mit der ersten Person verheiratet oder mit ihr (oder deren Ehegatten) verwandt oder verschwägert? Falls ja, in welcher Beziehung stehen Sie zur ersten Person? Falls nein, sind Sie Lebenspartner der ersten Person? In welcher Beziehung stehen Sie zum Lebenspartner der ersten Person (Tochter/Sohn, (Groß-) Mutter, (Groß)-Vater oder sonstige verwandte oder verschwägerte Person bzw. sonstige nichtverwandte Person)?

Das Statistische Landesamt begegnete möglichen Problemen jedoch nicht unvorbereitet. Die Medien wurden informiert und griffen das Thema, wenn auch nicht unkritisch, auf. Alle Hinweise unserer Behörde zu den Anschreiben an die Auskunftspflichtigen sowie zur Schulung der Interviewer wurden berücksichtigt. So wurden zum Beispiel die Informationsschreiben in sechs Sprachen verfasst.

Obwohl durch die Stichprobenauswahl in Berlin vor allem in großen Gebäuden mit einem hohen Anteil ausländischer Bewohner, sogar in einer Wohnunterkunft für Wohnungslose und in Gebäuden in sozialen Brennpunkten zum Teil ohne funktionsfähige Briefkästen und Hausbeleuchtung zu befragen war, trafen die Interviewer auf eine große Akzeptanz. Etwa 80 %

der Haushalte waren nach der schriftlichen Ankündigung unmittelbar zu den Interviews bereit und fast alle anderen Haushalte machten von ihrem Recht auf Selbstausfüllung Gebrauch. Der Anteil der zunächst erklärten Verweigerungen lag unter 3 %.

Wege zu einer besseren informationellen Infrastruktur

Seit 1998 informierten wir in den Jahresberichten darüber, wie unsere Behörde datenschutzrechtliche Aspekte in der öffentlich geführten Diskussion zwischen empirischen Wirtschaftsforschern und Vertretern der amtlichen Statistik einbringen konnte. Bekanntlich setzte die Bundesministerin für Bildung und Forschung 1999 eine „Kommission zur Verbesserung der informationellen Infrastruktur zwischen Wissenschaft und Statistik“ ein. Diese Kommission legte im März ihre Ergebnisse vor. Sie erarbeitete 36 Vorschläge, in denen auch die von uns unterbreiteten Ideen Berücksichtigung fanden. Dies sind insbesondere

- eine Empfehlung an den Gesetzgeber, ein Forschungsgeheimnis unter Einschluss eines Zeugnisverweigerungsrechts und Beschlagnahmeverbots einzuführen,
- gesetzliche Regelungen zur exakten Verknüpfung von Erhebungsdaten mit Registerdaten in abgeschotteten Forschungs- oder Statistikbereichen zu schaffen,
- durch das Gastwissenschaftlermodell Forscher nach den entsprechenden Datenschutzverpflichtungen Mitarbeiterinnen und Mitarbeitern von statistischen Ämtern oder anderen datenhaltenden Einrichtungen gleichzustellen und ihnen somit eine wissenschaftliche Nutzung dieser Daten zu erlauben,
- ein gemeinsames Forschungsprojekt von Wissenschaft und amtlicher Statistik zu Möglichkeiten der faktischen Anonymisierung von Unternehmens- und Betriebsdaten durchzuführen,
- die Einrichtung von Forschungsdatenzentren mit der Möglichkeit, der kontrollierten Ferndatenverarbeitung als einzig gangbarem Weg auch besonders sensible und kaum anonymisierbare Daten für Forschungszwecke zu öffnen,
- die Weiterentwicklung des Mikrozensus und der Übergang zu einer unterjährigen Erhebung sowie eines Access-Panels für die Ziehung freiwilliger Haushaltsstichproben[107].

Auf Grundlage der Empfehlungen der Kommission wurde vom Bundesministerium für Bildung und Forschung ein Gründungsausschuss für einen Rat für Sozial- und Wirtschaftsdaten eingerichtet. Dieser Gründungsausschuss hat die Aufgabe, Vorschläge für die Umsetzung der Empfehlungen der KVI zu erarbeiten. Diese betreffen insbesondere

[107] JB 2000, 4.5.3

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

- die Einrichtung von Forschungsdatenzentren,
- die Einrichtung eines Servicezentrums bzw. Servicenetzes,
- Prioritätensetzung bei Pilotprojekten, wie z. B. die Bereitstellung von Scientific Use Microdata Files oder Metadatenbanken, sowie
- die Einrichtung des Rates für Sozial- und Wirtschaftsdaten.

Gleichwohl werden durch die statistischen Landesämter wie auch das Statistische Bundesamt erste Schritte in Richtung der Schaffung von Forschungsdatenzentren getan.

All diese Vorschläge und Denkrichtungen zeigen, dass auch unter strikter Wahrung des Statistikgeheimnisses und des Datenschutzes sowohl dem Anliegen der Forschung als auch den verfassungsrechtlich gesetzten Grundlagen der Arbeit der amtlichen Statistik entsprochen werden kann.

4.5.2 Schule und Sport

Die Arbeiten am Schulreformgesetz gehen weiter

Im Jahresbericht 1999[108] verwiesen wir auf einige datenschutzrechtlich noch nicht ausgereifte und bedenkliche Vorschläge im Entwurf für ein neues Schulgesetz. Im März 2001 legte die Projektgruppe „Schulreform“ der Senatsverwaltung für Schule, Jugend und Sport einen überarbeiteten Entwurf zur öffentlichen Diskussion vor. Im Unterschied zum Entwurf von 1999 waren in diesen Entwurf schon Lösungsansätze für die datenschutzrechtlichen Probleme, die mit den Reformansätzen verbunden sind, aufgenommen worden. In einer ausführlichen Diskussion versuchten wir gemeinsam mit der Projektgruppe der Senatsverwaltung Lösungen zu finden. Um hier dem Ansatz des Schulreformgesetzes als einheitliche Rechtsgrundlage für das Berliner Schulrecht zu entsprechen, bemühten wir uns in unserem Vorschlag um kompakte und übersichtliche Regelungen, die eine künftige Anwendung erleichtern.

Mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit wurden intensive Gespräche über die datenschutzrechtlich relevanten Aspekte des Schulreformgesetzentwurfes geführt. Seine Änderungs- und Konkretisierungsvorschläge sind im Wesentlichen in die Überarbeitung des Entwurfes eingegangen.

Neue Verwaltungsvorschriften der Schulverwaltung

Im vergangenen Jahr bereitete die Senatsverwaltung für Schule, Jugend und Sport einen Neuerlass der Ausführungsvorschriften (AV) über den Schulpsychologischen Dienst, zur Förderung bei besonderen Lese- und Rechtschreibschwierigkeiten und über Schülerausweise vor. In den Entwürfen wurden unsere Hinweise vollständig berücksichtigt.

Die Ausführungsvorschriften (AV) über den Schulpsychologischen Dienst sind seit dem 1. Februar 2002 in Kraft. Die Hinweise des BlnBDI wurden vollständig berücksichtigt.

Insbesondere bei der Diskussion der AV Schulpsychologie und der AV Lese- und Rechtschreibschwäche zeigte sich, dass die rechtliche Stellung der Schulpsychologen einer grundsätzlichen Klärung bedarf. Hier befindet sich unsere Behörde in einer vielschichtigen Diskussion mit Schulpsychologen und Vertretern der Schulverwaltung. Gegenwärtig wird der Entwurf einer

Der Diskussionsprozess über Funktion und Inhalt einer datenschutzrechtlichen Hilfestellung für Schulpsychologinnen und Schulpsychologen sowie weitere im Schulpsychologischen Dienst tätige Personen ist noch nicht abgeschlossen. Die Senatsverwaltung für Bildung, Jugend und Sport hat den Beirat für Schulpsychologie um Stellungnahme gebeten. Vor der Entscheidung wird noch eine Abstimmung mit dem BlnBDI erfolgen.

[108] vgl. JB 1999, 4.5.2

datenschutzrechtlichen Handreichung für Schulpsychologen diskutiert.

Schulen im Internet

Eine kursorische Prüfung der Internet-Angebote Berliner Schulen hat als positives Ergebnis gezeigt, dass außer bei einzelnen Artikeln, die durch Schülerredakteure unterzeichnet sind, keine kompletten Namen von Schülern veröffentlicht werden. Zumeist werden die Aktivitäten von Kursen und Arbeitsgemeinschaften sowie bestimmte Schülerprojekte so dargestellt, dass lediglich die Vornamen genannt werden und auch die Bilder meist nur eine Gruppe von Schülern zeigen. Aber auch bei solchen Veröffentlichungen gilt Folgendes: Eine Veröffentlichung von Einzelfotos mit Namen (Passfotos) durch die Schule ist unzulässig, da die Schule selbst mit Ausnahme der Verarbeitung von Passfotos für Schülerausweise keine Befugnis hat, Einzelfotos von Schülern herzustellen, zu speichern oder gar zu veröffentlichen. Auch mit Einwilligung der Erziehungsberechtigten oder volljährigen Schüler unter der Homepage der Schule ist eine Veröffentlichung unzulässig, da ihre Tragweite bei einer Internet-Veröffentlichung durch die Einwilligungserklärung kaum abgedeckt werden kann. Anders, wenn Fotos von schulischen Aktivitäten oder auch Fotos großer Schülergruppen beispielsweise bei Sport- und Schulfesten oder Jahrgangsfotos in das Internetprogramm eingestellt werden sollen. In diesem Fall, insbesondere wenn diese Fotos nicht mit ohnehin unzulässigen Namenslisten korrespondieren, wird, die Einwilligung der Erziehungsberechtigten bzw. volljährigen Schüler vorausgesetzt, kaum etwas auszusetzen sein. Um hier eine Identifizierung vorzunehmen, ist ein Zusatzwissen erforderlich, das nur durch eine unmittelbare Beziehung zur Schule bzw. den Schülern, Lehrern oder Eltern erlangt werden kann.

Schmierereien am Schulgebäude

Mit viel Aufwand und unterstützt von älteren Schülern, Lehrern und Eltern wurden in einer Schule verschiedenste Schmierereien und Schriftzüge an Wänden, Türen und auf Tischen beseitigt. Nach einigen Wochen schien diese Arbeit jedoch umsonst gewesen zu sein, da schon wieder neue Schmierereien die Schule verunstalteten. Die Lehrerschaft überlegte, da für die Schmierereien wohl nur Schüler der eigenen Schule in Frage kamen, ob eine Schriftprobenkartei angelegt werden soll.

Weder im Berliner Schulgesetz noch in der Schuldatenverordnung findet sich eine Rechtsgrundlage für eine solche Maßnahme. Eine Schriftprobenkartei an der Schule ist damit rechtswidrig. Was soll die Schule also tun? Sie könnte sich mittels einer Anzeige an die Polizei wenden, die dann nach der Strafprozessordnung Ermittlungen aufnimmt. Dies hätte jedoch zur Folge, dass die Verschmutzungen von Anfang an als Straftat verfolgt und damit mögliche pädagogische Lösungen durch die Nutzung der Palette der Erziehungs- und Ordnungsmaßnahmen erschwert werden. Auch führt

dies zur Speicherung personenbezogener Daten von Schülern im polizeilichen Informationssystem. Das Berliner Schulrecht sieht zunächst immer den Vorrang pädagogischer Maßnahmen vor.

Die Schule kann aber unter Hinweis auf die Verschmutzungen selbst im Rahmen ihres Hausrechts Ermittlungen anstellen. Sie könnte beispielsweise auch von verdächtigen Schülern zum Zweck der Klärung der Angelegenheiten eine Schriftprobe verlangen. Eine karteimäßige Speicherung auf Vorrat ist jedoch unverhältnismäßig und hat im Hausrecht keine Rechtsgrundlage.

Sportvereine im Internet

Zufällig entdecken die Eltern eines 15-jährigen Mädchens unter der Homepage des Sportvereins ihrer Tochter diese mit Passbild, Altersangabe und vollem Namen auf einer Ehrentafel, mit der der Verein sportliche Erfolge veröffentlicht. Auch eine Reihe von anderen 13- bis 17-jährigen Sportlerinnen und Sportler sind auf dieser Ehrentafel verzeichnet. Eine Einwilligung der Eltern zu dieser Veröffentlichung lag nicht vor.

Welche Daten ein Verein über seine Mitglieder speichern darf und in welchem Umfang auch Übermittlungen an andere Vereinsmitglieder oder Dritte zulässig sind, richtet sich nach den Bestimmungen des Bundesdatenschutzgesetzes. So kann ein Verein per Satzung bestimmte Vorschriften zur Erhebung und Speicherung personenbezogener Daten seiner Mitglieder erlassen, wenn dies zur Erfüllung eigener Geschäftszwecke und zur Wahrung berechtigter Interessen des Sportvereins erforderlich ist. Der Verein hat jedoch zu prüfen, ob Gründe entgegenstehen, die zu der Annahme führen, dass schutzwürdige Interessen seiner Vereinsmitglieder überwiegen. Auch mit der Veröffentlichung verfolgt der Verein bestimmte durch Satzung vorgegebene Zwecke. Er hat aber auch abzuwägen, ob diesen Veröffentlichungen schutzwürdige Belange entgegenstehen. Dabei hat der Verein insbesondere die Eingriffstiefe, die mit einer Veröffentlichung verbunden ist, abzuschätzen. Ein Aushängen von Teilnehmern oder Siegern beispielsweise in einer Sporthalle, in den Vereinsräumen oder auch die Veröffentlichung von Wettkampfergebnissen in einer Vereinszeitung bzw. zusammengefasste Veröffentlichungen in Presse, Rundfunk und Fernsehen bei aktuellen sportlichen Berichterstattungen haben in jedem Fall nur einen eingeschränkten und zeitlich begrenzten Empfängerkreis.

Grundsätzlich anders verhält es sich bei Veröffentlichungen im Internet. Bekanntlich ist fast jeder Begriff und damit auch jeder Name im Internet suchfähig, wenn die Seiten nicht mit einer no-robot-Funktion für die meisten Suchmaschinen gesperrt sind oder die Veröffentlichung lediglich in einer geschlossenen Benutzergruppe, d. h. passwortgeschützt erfolgt. Hinzu kommt, dass nur selten einmal ins Netz gestellte Seiten und Informationen wieder entnommen werden. Bei einer Veröffentlichung im Internet kann damit nicht abgeschätzt werden, ob bei den vielfältigen Nutzungs-

möglichkeiten dieser Informationen schutzwürdige Belange der betroffenen Sportler beeinträchtigt werden. Deshalb ist eine Veröffentlichung ohne Einwilligung nicht zulässig. Normalerweise kann es beim Leistungssport oder in anderen begründeten Fällen zum Vereinszweck gehören, Erfolge einzelner Mitglieder im Internet und damit auch international zu verbreiten (§ 28 Abs. 1 S. 1 Ziff. 1 BDSG).

Wir können daher nur empfehlen, alle Mitglieder des Vereins um eine Einwilligungserklärung zu bitten, in der der namentlichen Veröffentlichung von Sportergebnissen oder Wettkampfnominierungen zugestimmt wird. Sollten weitere Informationen wie in der oben beschriebenen Ehrentafel in das Angebot aufgenommen werden, wäre eine besondere Einwilligung, insbesondere auch für die Veröffentlichung von Einzelfotos erforderlich. Wird die Einwilligung verweigert, so ist nur eine anonymisierte Darstellung der Ergebnisse des Vereins möglich. Von besonderer Bedeutung ist in diesem Zusammenhang die Veröffentlichung von Daten Minderjähriger, für die zusätzlich die Einwilligung der Erziehungsberechtigten vorzuliegen hat. Nicht zu empfehlen ist, dass der Verein durch Satzung festlegt, grundsätzlich personenbezogene Daten im Internet zu veröffentlichen. Damit wäre zwar formal eine Rechtsgrundlage geschaffen, nach der es einer Einwilligung der Betroffenen nicht mehr bedarf. Sie dürfte aber wenigstens bei Minderjährigen rechtlich kaum haltbar sein und sogar regelmäßig satzungsmäßigen Zielen jedes Sportvereins entgegenlaufen. Was für eigene Vereinsmitglieder gilt, muss selbstverständlich auch bei der Veröffentlichung von Nominierungen für Wettkämpfe bei Sportlern anderer Vereine gelten. Hier könnte mit den Anmeldeunterlagen für das Turnier auch um die Einwilligung zur Internet-Veröffentlichung gebeten werden.

4.5.3 Wissenschaft und Forschung

Datenschutzgerechte Forschung

Auch in diesem Jahresbericht wollen wir wieder eine Auswahl von Forschungsprojekten kurz vorstellen, für die es gelang, mit zum Teil erheblichem Beratungsaufwand bei Wahrung der informationellen Selbstbestimmung der Betroffenen einen optimalen Datenzugang für die Forscher zu ermöglichen.

Von Forschern befragt wurden:

- Frauen nach Fehlgeburten und dem Verlauf einer neuen Schwangerschaft,
- Schüler zur sozialen Ungleichheit unter Kindern in Schulklassen,
- Nierenkranke über den Einfluss von im Verlauf ihres Lebens genommener Schmerzmittel als mögliche Ursache für ihre Erkrankung,
- Jugendliche mit angeborenen Herzfehlern über den Erfolg von Rehabilitationsbehandlungen,

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

- Frauen zur Verschreibungspraxis, zum Nutzen und zur Sicherheit oraler Kontrazeptiva,
- Krankenhauspatienten zur Qualität ihrer Betreuung,
- Sozialhilfeempfänger und eine Vergleichsgruppe aus der Gesamtbevölkerung zur Gesundheitssituation, Lebenszufriedenheit und Lebensgewohnheiten,
- Kita-Kinder über die Wirkung von Tabak- und anderer Werbung,
- Patienten mit chronisch entzündlichen Darmerkrankungen zur ihrer Lebensqualität und zum Gesundheitsverhalten,
- Personen, die sich mit Farben, Lacken, Klebern oder Pestiziden vergiftet haben, zu den auslösenden Ursachen, den Wegen sowie den aufgenommenen Mengen der Gifte,
- Patienten mit chronischen Schmerzen zur Wirkung von Akupunkturbehandlungen,
- Schüler zur politischen Sozialisation in Ost- bzw. Westberliner Familien,
- Schulanfänger zu mathematischen Vorkenntnissen,
- Teilnehmer des Berlin-Marathons zu Auswirkungen und Nebenwirkungen intensiven Trainings,
- Kinder und Jugendliche zwischen 11 und 15 Jahren zum Gesundheitszustand und zum Gesundheitsverhalten,
- Schüler, die Schulunfälle erlitten, und deren Lehrer zu Unfallrisiken und Unfallschwerpunkten im Schulalltag,
- Auszubildende und junge Fachkräfte zu ihrer regionalen Mobilität, insbesondere möglicher Ost-West-Wanderungen,
- in Berlin lebende Türken zur Lebenseinstellung, zu Lebensgewohnheiten und Integrationsproblemen,
- Kinder mit Neurodermitis oder Asthma über den Erfolg von wohnortnahen Rehabilitationsmaßnahmen.

Akteneinsicht nahmen Forscher in

- Unterlagen über den Rehabilitationsverlauf von Patienten nach endoprotetischer Versorgung des Knie- oder Hüftgelenks,
- anonymisierte Auszüge aus dem Bundeszentralregister von jungendlichen Teilnehmern an sozialen Trainingskursen,
- anonymisierte Unterlagen von Therapiezentren zur Optimierung des Krankentransportes,
- anonymisierte Auszüge aus dem Bundeszentralregister von behandelten und unbehandelten Sexualstraftätern,
- anonymisierte Unterlagen von Personen, die unter Drogen Kraftfahrzeuge gelenkt haben,

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

- Unterlagen über Verkehrsunfälle mit Fußgängern im Zusammenhang mit der Auswirkung unterschiedlicher Pkw-Karosserieformen,
- Unterlagen über die Spendenpraxis in der Bundesrepublik Deutschland bis zur Wiedervereinigung,
- Erfahrungsberichte deutscher Fremdsprachenassistenten in Großbritannien,
- Unterlagen über Sozialhilfeleistungen für den Zweiten Armuts- und Reichtumsbericht der Bundesregierung.

Darüber hinaus wurden Forscher zu folgenden Themen beraten:

- zur Anonymisierung von Blutproben für eine epidemiologische Untersuchung zum Nijmegen Breakage Syndrom,
- zur Anonymisierung einer Studie über den Charlottenburger SA-„Mördersturm 33“ (1928 bis 1932),
- über den Zugang zu Adressdaten zu Unternehmen mit hochgradigen Innovationen in technologieintensiven Branchen,
- zum Aufbau eines Kompetenznetzes und eines Referenzpanels für Lymphknotenpathologie,
- zur Gewinnung von Schülern zur Evaluation von Englisch-Leistungstests,
- zur Pseudonymisierung einer Langzeitstudie zu Musikgewohnheiten und über Hörschäden bei Jugendlichen,
- zur anonymisierten Veröffentlichung von Verzeichnissen zu einer Sammlung von Feldpost aus dem Zweiten Weltkrieg im Internet,
- zur Anonymisierung von Operationsdaten über die Verträglichkeit implantierter Kunststoffnetze bei Knochenbrüchen,
- zur Gewinnung von Jugendlichen für den Test eines Verfahrens zum Messen von Gehirnaktivitäten beim Erkennen von Gesichtern,
- zur anonymisierten Auswertung von Daten der Krankenkassen und der Ärzte bei der Behandlung chronisch kranker Kinder,
- zur Sicherung der Rechte der Probanden bei einer Studie über die Verträglichkeit neuer Antibiotika im Zusammenhang mit einer Genotypisierung,
- für eine Untersuchung der Verbreitungswege von Tuberkulose durch genetische Identifikation des Erregers und zur Nutzung von Daten der Gesundheitsämter und Befragung der Erkrankten.

4.6 Wirtschaft

4.6.1 Das Datenschutzniveau in Berliner Großunternehmen

Vor der Novellierung des Bundesdatenschutzgesetzes prüften die Aufsichtsbehörden bei privaten Eigenverarbeitern die Einhaltung der Vorschriften des Datenschutzgesetzes nur, wenn ihnen hinreichende Anhaltspunkte für einen Gesetzesverstoß vorlagen (Anlasskontrolle). Nach der Novellierung des Bundesdatenschutzgesetzes sind die Aufsichtsbehörden verpflichtet, von Amts wegen die Einhaltung datenschutzrechtlicher Bestimmungen zu prüfen.

In Vorbereitung auf diese neue gesetzliche Situation führten wir seit November 2000 erste Informationsgespräche mit den betrieblichen Datenschutzbeauftragten der größten Berliner Unternehmen, um uns über das Datenschutzniveau dieser Unternehmen zu informieren.

Insgesamt kann festgehalten werden, dass die Mehrzahl der Unternehmen die Bedeutung des informationellen Selbstbestimmungsrechts als Wirtschaftsfaktor (Kunden- und Mitarbeiterzufriedenheit) durchaus erkannt haben. So hatten einzelne der überprüften Unternehmen den Datenschutz vorbildlich organisiert. Bei anderen Unternehmen allerdings hatte man den Eindruck, als werde der Datenschutz als lästige Pflichtaufgabe angesehen.

Das BDSG enthält zwar keine genauen Regelungen zu der Frage, zu welchem Anteil ein betrieblicher Datenschutzbeauftragter mit anderen Aufgaben beschäftigt werden darf. Die Bedeutung des informationellen Selbstbestimmungsrechts gebietet es aber, dass ein Unternehmen ab einer gewissen Größe einen Datenschutzbeauftragten beschäftigt, der sich ausschließlich den gesetzlichen Aufgaben als betrieblicher Datenschutzbeauftragter widmen kann. Bedenkt man, dass das novellierte Bundesdatenschutzgesetz dem betrieblichen Datenschutzbeauftragten neue Aufgaben, etwa Vorabkontrollen, zuweist, ist in Großunternehmen sogar zu überlegen, ob es nicht erforderlich wäre, dass der betriebliche Datenschutzbeauftragte durch Mitarbeiter unterstützt wird. Dies gilt insbesondere in den Unternehmen, in denen im großen Umfang personenbezogene Daten verarbeitet werden.

Die Bandbreite der Kapazität, die die betrieblichen Datenschutzbeauftragten für ihre Tätigkeit verwendeten, schwankte zwischen 100 % und 5 %. Insbesondere in den beiden Unternehmen, in denen die Kapazität unter 50 % lag (5 % bzw. 20 %), haben wir darauf hingewiesen, dass die Bestellung eines Scheindatenschutzbeauftragten nicht den Vorgaben des § 4 f BDSG entspricht. In mehreren Fällen wurde aufgrund unserer Initiative die Kapazität des Datenschutzbeauftragten auf 100 % aufgestockt.

In einem Fall erschien zweifelhaft, ob der betriebliche Datenschutzbeauftragte die nach § 4 f Abs. 2 Satz 1 BDSG erforderliche Sachkunde besaß. Dem Daten-

schutzbeauftragten war im August 2001 noch nichts bekannt über die Novellierung des Bundesdatenschutzgesetzes. Hier haben wir Schulungen angeregt.

Einige der Datenschutzbeauftragten arbeiteten als Konzerndatenschutzbeauftragte. Hier war teilweise nicht beachtet worden, dass der betriebliche Datenschutzbeauftragte bei der jeweiligen verantwortlichen Stelle (juristische Person) als Datenschutzbeauftragter zu bestellen ist. Eine Bestellung für den gesamten Konzern erfüllt demgegenüber nicht die Voraussetzungen des § 4 f BDSG.

Bei mehreren Unternehmen bestanden bezüglich der Umsetzung einiger neuer Vorschriften des Bundesdatenschutzgesetzes Unsicherheiten. Teilweise hatte man sich auch nach dem 23. Mai 2001 noch keine Gedanken über wichtige Gesetzesänderungen gemacht, wie etwa die Regelungen bezüglich internationaler Datenflüsse nach §§ 4 b ff. Mehrmals mussten wir auch auf die in § 6 b BDSG konstituierten Beschränkungen bei der Beobachtung öffentlich-zugänglicher Räume mit optisch-elektronischen Einrichtungen hinweisen.

4.6.2 Banken

Datenübermittlung an Untersuchungsausschuss des Abgeordnetenhauses

Der Untersuchungsausschuss „Bankgesellschaft/Parteispenden“ des Berliner Abgeordnetenhauses hat einen Beweiserhebungsbeschluss gefasst, der teilweise die Bankgesellschaft Berlin betrifft und die Anforderung von Akten, Auflistungen und sonstigen Unterlagen zum Inhalt hat. Insbesondere ging es dabei um bestimmte Kredite sowie die Fondgeschäfte der Bankgesellschaft. Die Berliner Bankgesellschaft bat um Überprüfung, ob sie die geforderten Beweismittel dem Abgeordnetenhaus zur Verfügung stellen darf oder ob hiergegen die Datenschutzinteressen ihrer Mitarbeiter und Kunden sprechen.

Die Zulässigkeit der Datenübermittlung an das Abgeordnetenhaus setzt nach § 4 Abs. 1 BDSG eine Rechtsvorschrift voraus. Da das BDSG selbst keine Rechtsgrundlage für die Datenübermittlung an den Untersuchungsausschuss enthält, kommt als sonstige Rechtsvorschrift im Sinne des § 4 Abs. 1 BDSG insbesondere § 13 Abs. 1 Satz 1 des Gesetzes über die Untersuchungsausschüsse des Abgeordnetenhauses von Berlin (UAG) in Betracht. Danach ist jedermann verpflichtet, Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, auf Aufforderung des Untersuchungsausschusses für die Dauer des Verfahrens zur Verfügung zu stellen. Bei § 13 UAG handelt es sich zwar um eine landesrechtliche Rechtsvorschrift; aber auch landesrechtliche Rechtsvorschriften können Bearbeitungsvorgänge nicht-öffentlicher Stellen zulassen, wenn der Landesgesetzgeber wie bei der Schaffung des UAG eine nach der Kompetenzverteilung des Grundgesetzes bestehende Zuständigkeit in Anspruch genommen hat.

Der Untersuchungsausschuss hat die Befugnis zur Erhebung der nach dem Untersuchungsauftrag gebotenen Beweise (Art. 48 Abs. 2 Satz 3 Verfassung von Berlin, § 10 UAG). Die Befugnis ist demnach beschränkt auf die Beweiserhebung, die zur Klärung des Untersuchungsauftrags notwendig ist bzw. nach pflichtgemäßer Einschätzung als notwendig angesehen wird. Entsprechend dieser Voraussetzung ist auch § 13 Abs. 1 Satz 1 UAG auszulegen, d. h., dass für die Prognose über die Bedeutung der Beweismittel nicht schon jede Vermutung und entfernte Möglichkeit der Erheblichkeit des Gegenstandes genügt. Vielmehr muss eine gewisse Wahrscheinlichkeit hierfür gegeben sein.

Die Herausgabe der Gegenstände darf grundsätzlich nicht – soweit Daten von Bankkunden betroffen sind – einen Verstoß gegen das Bankgeheimnis darstellen. Das Bankgeheimnis des privatrechtlich organisierten Bankgewerbes ist gewohnheitsrechtlich anerkannt und wird in gesetzlichen Vorschriften, wie beispielsweise § 30 a AO, und in der Rechtsprechung vorausgesetzt. Das Bankgeheimnis umfasst die Pflicht zur Verschwiegenheit über Kundendaten und zugleich das Recht zur Verschwiegenheit gegenüber Auskunftsuchenden. Diese Verschwiegenheitspflicht ist als Nebenpflicht Bestandteil des Vertrages zwischen Bank und Kunden. Nach der gewohnheitsrechtlichen Ausgestaltung des Bankgeheimnisses gilt es jedoch nicht unbeschränkt. Eine Weitergabe von Kundendaten ist zulässig, wenn der Kunde eingewilligt hat, wenn gesetzliche Bestimmungen dies gebieten oder der Fall einer zulässigen Bankauskunft vorliegt. Da auch hier (wie bei § 4 Abs. 1 BDSG) eine landesrechtliche Datenübermittlungsnorm genügt, ist vorliegend nicht von einem Verstoß gegen das Bankgeheimnis auszugehen.

Die Datenübermittlung durch die Bankgesellschaft an den Untersuchungsausschuss, die die Vorgaben des § 13 UAG beachtet, war damit rechtmäßig.

Ein überraschender Kontoauszug

Der Kontoauszug eines Bankkunden enthielt bei einer Überweisung den zusätzlichen Hinweis, dass der Adressat der Überweisung von Beruf Obergerichtsvollzieher ist. Dies überraschte den Bankkunden, insbesondere da er auf seinem Überweisungsformular keinen entsprechenden Hinweis gegeben hatte. Der Überweisungsauftrag des Kunden enthielt eine Ungenauigkeit, so dass er nicht maschinell bearbeitet werden konnte. Es wurde festgestellt, dass der Kunde an einen Empfänger überweisen wollte, an den auch andere Kunden sehr häufig Geld überweisen (so genannter Großempfänger). Man hat anschließend, wie in derartigen Fällen üblich, die komplette Angabe zu dem Empfänger hinzugefügt.

Das Datum, dass der Kunde an einen Obergerichtsvollzieher überwiesen hat, darf von der Bank als Mittel für die Erfüllung eigener Geschäftszwecke genutzt werden, wenn es der Zweckbestimmung des Vertragsverhältnisses mit dem Betroffenen dient. Für die Überwei-

sung selbst war die Berufsangabe des Adressaten nicht erforderlich. Sie diente ausschließlich der technischen Erleichterung der Durchführung des fehlerhaft ausgefüllten Überweisungsauftrages. Dies rechtfertigt die von der Bank vorgenommene Datennutzung im Regelfall noch nicht. Dies gilt umso mehr, als nach § 3 a Satz 1 BDSG die Ausgestaltung und Auswahl von Datenverarbeitungssystemen sich an dem Ziel auszurichten haben, so wenig personenbezogene Daten wie möglich zu nutzen. Insofern ist der Bank zu empfehlen, das Überweisungssystem so umzustellen, dass bei ungenauen Überweisungsaufträgen ohne zusätzliche Erschwernisse auf Zusatzangaben zum Empfänger verzichtet werden kann.

Wir haben gegenüber der Bank darauf hingewiesen, dass derartige Ergänzungen bei Großempfängern wie der Bewag oder der GASAG noch hinnehmbar seien. Wir haben allerdings empfohlen, bei „sensitiven und sonstigen problematischen Empfängerkategorien“ wie Gerichtsvollziehern, Ärzten etc. auf die Verwendung der Zusätze zu verzichten.

4.6.3 Auskunfteien

Kunden von Auskunfteien als Geschäftsgeheimnis

Bis zur Novellierung des Bundesdatenschutzgesetzes konnten die Betroffenen bei Auskunfteien nur Auskunft über die Datenempfänger verlangen, wenn sie begründete Zweifel an der Richtigkeit der Daten geltend machten. Der Gesetzgeber hat die Rechte der Betroffenen gegenüber Auskunfteien verbessert.

Sie können nun nach § 34 Abs. 1 Satz 3 Auskunft über den Empfänger (den Kunden) der Auskunftei verlangen, sofern nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt. Die Mehrzahl der Auskunfteien geht davon aus, dass grundsätzlich der Name ihres Kunden ein überwiegendes Geschäftsgeheimnis darstellt. Es sei nur dann nicht von dem Überwiegen des Geschäftsgeheimnisses auszugehen, wenn fehlerhafte Daten übermittelt worden seien. Um eine Abwägung zwischen informationellem Selbstbestimmungsrecht und Geschäftsgeheimnis vornehmen zu können, verlangen Auskunfteien teilweise von den Betroffenen, dass sie ihr Informationsinteresse besonders begründen.

Schon der Wortlaut „sofern nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt“ (§ 34 Abs. 1 Satz 3 BDSG) lässt erkennen, dass der Gesetzgeber die überwiegende Bedeutung des Geschäftsgeheimnisses gegenüber dem informationellen Selbstbestimmungsrecht als Ausnahme ansieht. Das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt nur dann, wenn keine begründeten Zweifel an der Richtigkeit der übermittelten Daten bestehen und aufgrund besonderer Umstände davon ausgegangen werden kann, dass die Bedeutung des Geschäftsgeheimnisses höher zu gewichten ist als das Informationsinteresse des Betroffenen.

Hiervon kann etwa ausgegangen werden, wenn aufgrund objektiver Umstände zu vermuten ist, dass der Geschäftspartner der Auskunftei die Anfrage nicht stellen würde, wenn er damit rechnen müsste, dass sein Kunde hierüber informiert würde (nachbarschaftliches Näheverhältnis zwischen Kunde und Betroffenem, Betroffener würde bei Kenntnis des Auskunftsvorgangs dem Kunden der Auskunftei den Auftrag nicht mehr erteilen etc.). Nur wenn ausnahmsweise die Vermutung besteht, dass das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegen könnte, besteht Veranlassung, den Betroffenen um eine Begründung seines Informationsinteresses zu bitten.

Scoring-Verfahren der SCHUFA

Im Jahresbericht 2000[109] haben wir darüber informiert, dass die SCHUFA zugesagt hatte, die rechtswidrige negative Beeinflussung des Score-Wertes durch Selbstauskünfte bis Mitte 2001 zu beenden. Inzwischen hat uns die SCHUFA auf Nachfrage mitgeteilt, die Zusage könne nicht eingehalten werden. Aufgrund „technischer Probleme“ sei erst mit einer Umsetzung der Zusage bis Mitte 2002 zu rechnen.

In einem Anerkenntnisurteil des Amtsgerichts Hamburg vom 27. Juni 2001[110] ist die SCHUFA verurteilt worden, es einem bestimmten Kläger gegenüber zu unterlassen, bei der Bearbeitung von Auskunftsbegehren der kreditgebenden Wirtschaft hinsichtlich der Bonität des Klägers einen „Score-Wert“ nach dem Score-System der SCHUFA an den Auskunftbegehrenden zu übermitteln. Durch das Anerkenntnis konnte die SCHUFA verhindern, dass das *Scoring-Verfahren* vor einem Zivilgericht auf seine Rechtmäßigkeit überprüft wurde.

Im Anschluss an dieses Urteil räumt die SCHUFA nunmehr den Betroffenen das Recht ein, gegen die Übermittlung des Score-Wertes an einen Vertragspartner der SCHUFA Widerspruch einzulegen. Es liegen allerdings noch keine Erfahrungswerte darüber vor, wie die Vertragspartner der SCHUFA im Rahmen einer Bonitätsprüfung das Fehlen eines Scoring-Wertes bewerten werden. Insofern kann nicht ausgeschlossen werden, dass der Widerspruch gegen die Übermittlung des Scoring-Wertes auch mit Nachteilen verbunden sein kann.

Die SCHUFA hat sich - entgegen ihrer bisherigen Haltung - außerdem bereit erklärt, den Kunden den aktuellen Scoring-Wert mitzuteilen.

4.6.4 Verkehrsunternehmen

Der moderne Pranger

Verschiedene Unternehmen sind dazu übergegangen, ihre „schlechten Kunden“ in speziellen Warndateien ins Internet einzustellen. Noch weiter ging ein Berliner Speditionsunternehmen, das eine Warndatei ins Inter-

[109] vgl. 4.6.2
[110] Az.: 9 C 168/01

net einstellte, in die die Branchenkollegen schlechte Erfahrungen mit Kunden einmelden konnten. Diese Informationen waren auf der Website des Transportunternehmens abrufbar.

Das geschäftsmäßige Speichern personenbezogener Daten zum Zwecke der Übermittlung ist nach § 29 Abs. 1 Nr. 1 BDSG zulässig, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Speicherung hat. Die auf der Internet-Seite des Speditionsunternehmens enthaltenen Schuldnerdaten verletzen die schutzwürdigen Interessen des Betroffenen schon deshalb, weil die Angaben der Gläubiger nicht überprüfte und mit großer Wahrscheinlichkeit sehr subjektive Informationen über Kunden enthalten. Häufig behaupten Unternehmen etwa, ein Kunde habe eine Forderung nicht beglichen, obwohl dieser eine Einrede geltend machen kann wie z. B. Schlechtleistung, positive Forderungsverletzung etc.

Die Veröffentlichung von Daten im Internet stellt eine Übermittlung von Daten an eine beliebige Anzahl von Personen dar. Die Übermittlung dieser Daten wäre nur zulässig, wenn der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat (§ 29 Abs. 2 Satz 1 Nr. 1 a) und Nr. 2 BDSG). Diese Vorgaben erfüllt das Speditionsunternehmen nicht, da nicht überprüft werden kann, ob derjenige, der sich mit Hilfe der Website der Spedition über die Bonität von Kunden informiert, tatsächlich ein berechtigtes Interesse (Vorleistung) an den von der Spedition veröffentlichten Daten hat. Jeder Internet-Nutzer hatte vielmehr die Möglichkeit, die betreffenden Internet-Seiten einzusehen, auch ohne Grund oder etwa, um Konkurrenten zu erforschen oder als Kredithai mögliche neue Opfer zu akquirieren. Das Speditionsunternehmen hat inzwischen die Website vom Netz genommen und die Schuldnerdaten gelöscht. Die Rechtswidrigkeit von Schuldnerspiegeln im Internet wurde vom Oberlandesgericht Rostock[111] bestätigt.

Wertmarkenverkauf für die „Berlin-Karte S“

Ein Bürger hat sich darüber beschwert, dass er für den Erwerb einer Wertmarke für die „Berlin-Karte S“ an einem privaten Verkaufskiosk dem dortigen Verkäufer als Nachweis der Berechtigung die Trägerkarte, die Angaben über den Bezug von Sozialhilfe enthält, vorlegen sollte. Auf Nachfrage sei ihm vom Verkäufer mitgeteilt worden, dass die BVG diese Forderung zur Voraussetzung für den Verkauf der Wertmarken gemacht habe.

Bei der „Berlin-Karte S“ handelt es sich um einen nicht übertragbaren Fahrausweis (Trägerkarte), der die Empfänger von Sozialhilfe zur Benutzung der BVG und der S-Bahn innerhalb des Stadtgebietes berechtigt, wenn die Trägerkarte mit einer für den laufenden Monat gültigen Wertmarke versehen ist.

[111] Urteil vom 21. März 2001, Az.: 2 U 55/00

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Die Wertmarke ist auf der Vorderseite der Trägerkarte neben dem Lichtbild des Berechtigten aufzukleben. Die Rückseite der Trägerkarte enthält einen Ausweis mit Angaben über das ausstellende Bezirksamt, Geschäftszeichen, Namen, Vornamen, Geburtsdatum und Anschrift des Sozialhilfeberechtigten. Die Ausstellung und Verlängerung der Trägerkarte wird in den zuständigen Berliner Sozialämtern vorgenommen. Die Wertmarken für die „Berlin-Karte S“ sind an allen Verkaufsstellen der BVG, der S-Bahn Berlin GmbH und an zahlreichen, durch besonderen Aushang kenntlich gemachten privaten Verkaufsstellen erhältlich.

Wird der Kunde an den Verkaufsstellen aufgefordert, die „Berlin-Karte S“ als Berechtigungsnachweis für den Erwerb der Wertmarken vorzulegen, erhält der Verkäufer der Wertmarken davon Kenntnis, dass der Kunde Sozialhilfeempfänger bzw. Leistungsbezieher nach dem Asylbewerberleistungsgesetz ist. Zudem werden ihm dessen Personalien offenbart.

Eine derartige Verarbeitung von sensiblen Sozialdaten ist nur zulässig, wenn dies für den jeweils damit verbundenen Zweck erforderlich ist. Als Zweck der Datenverarbeitung wird hier auf die Vermeidung einer missbräuchlichen Nutzung der „Berlin-Karte S“ verwiesen. Die Vorlage der Trägerkarte ist jedoch in keinem Fall geeignet und erforderlich, um den Missbrauch der Wertmarken als Fahrkarte zu verhindern.

Der Vertrag zwischen dem Land Berlin, der BVG und der S-Bahn Berlin GmbH zur Einführung der „Berlin-Karte S“ bestimmt ausdrücklich, dass das Recht zur Beförderung nicht übertragbar ist und ausschließlich dem Karteninhaber zusteht. Weiter ist festgelegt, dass die Bestimmungen zur Fahrscheinkontrolle in den Beförderungsbedingungen von BVG und S-Bahn Berlin GmbH auch auf den Inhaber der „Berlin-Karte S“ Anwendung finden und die „Berlin-Karte S“ nur in Verbindung mit einer für den laufenden Monat gültigen Wertmarke einen gültigen Fahrausweis darstellt. Danach ist eine Benutzung der Wertmarken als Fahrausweis ohne Verbindung mit der Trägerkarte praktisch ausgeschlossen.

Im Interesse der Kunden und des Datenschutzes haben wir daher empfohlen, dass beim Erwerb von Wertmarken für die „Berlin-Karte S“ zukünftig – unabhängig davon, ob dieser Erwerb an Verkaufsschaltern der BVG, der S-Bahn Berlin GmbH oder an privaten Verkaufsstellen erfolgt – auf die Vorlage der Trägerkarte bzw. eines anderen Nachweises verzichtet wird. Während sich die BVG unserer Auffassung angeschlossen hat, will die S-Bahn Berlin GmbH auch zukünftig beim Erwerb der Wertmarken nicht auf den Legitimationsnachweis des Kunden durch Vorlage der Trägerkarte verzichten.

Die Praxis zum Erwerb von Wertabschnitten für die persönliche, nicht übertragbare Karte S ist in der Verhinderung einer missbräuchlichen Nutzung begründet.

Die rabattierte Berlin-Karte S wird bezuschusst. Es ist daher durchaus auch im Sinne der Nutzer, dass dieses Angebot nur von den Berechtigten in Anspruch genommen wird, da andernfalls eine Aussetzung denkbar wäre.

Gleichzeitig ist mit der derzeitigen Verfahrensweise sichergestellt, dass die Nutzungsberechtigten nicht versehentlich als "Schwarzfahrer" unterwegs sind: Zur Sicherstellung der berechtigten Nutzung ist beim Erwerb des Wertabschnitts (wie auch beim Berlin-Ticket A) die Nummer der Trägerkarte auf den Wertabschnitt zu übertragen. Wird diese Nummer nicht übertragen, würde dies im Falle einer Fahrausweiskontrolle als "Schwarzfahren" -bestenfalls als "Graufahren"- gewertet werden. Damit ist die Aussage des Jahresberichts zu relativieren, nach der die beschriebene Praxis *"in keinem Fall geeignet und erforderlich* (ist), *um den Missbrauch ... zu verhindern."*

Vielmehr wird im VBB-Tarif (Teil C, Kapitel 2.5 Berlin-Karte S) ausgeführt: „*Wertabschnitte können nur von Inhabern der Berlin-Karte S ... erworben werden."* Dieser Bestimmung kann nur genüge getan werden, wenn die Form des derzeitigen Erwerbs beibehalten wird.

Der Klage führende Bürger bezieht sich auf private Verkaufsstellen, denen er seine auf der Berlin-Karte S enthaltenen Daten nicht vorlegen möchte. Als Lösung böte sich daher an, die Wertabschnitte an den Verkaufsstellen der Verkehrsunternehmen (BVG, S-Bahn Berlin GmbH) zu erwerben. Im übrigen sei darauf verwiesen, dass die Berlin-Karte S auch bei jeder Fahrausweisprüfung vorgezeigt werden muss. Hierüber wurde jedoch keine Klage geführt.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

4.7 Europäischer und internationaler Datenschutz

Mit der Umsetzung der Europäischen Datenschutzrichtlinie in das BDSG wurden im deutschen Recht erstmals Aussagen darüber getroffen, welches Recht bei grenzüberschreitenden Datenübermittlungen gelten soll (§ 1 Abs. 5 BDSG) und unter welchen Voraussetzungen Datenübermittlungen ins Ausland zulässig sind (§§ 4 b, c BDSG). Dem Grundgedanken des Europäischen Binnenmarktes folgend wird die Übermittlung von Daten an Empfänger innerhalb des europäischen Wirtschaftsraums unter den gleichen Voraussetzungen behandelt wie die Datenübermittlung innerhalb Deutschlands (§ 4 b Abs. 1 BDSG).

Anwendbares Recht

Die Frage, welches Recht bei grenzüberschreitendem Datenverkehr anzuwenden ist, hängt zunächst davon ab, ob auf deutscher Seite ein juristisch selbständiges Unternehmen beteiligt ist. Ist dies der Fall, gilt auf jeden Fall das BDSG für alle Verarbeitungen, die in Deutschland stattfinden (§ 1 Abs. 2 Ziff. 3 BDSG), also auch für die Datenübermittlungen in andere Länder.

Handelt es sich in Deutschland nicht um ein selbständiges Unternehmen, kommt es bei Unternehmen, die ihren Sitz in der Europäischen Union oder sonst im Europäischen Wirtschaftsraum (also in Norwegen, Island oder Liechtenstein) außerhalb Deutschlands haben, darauf an, ob sie eine Niederlassung in Deutschland haben. Dann gilt ebenfalls deutsches Recht. Ist dies nicht der Fall und werden gleichwohl Daten in Deutschland erhoben oder verarbeitet, gilt das Recht des Sitzlandes mit der Folge, dass in der Tat hier das Datenschutzrecht des anderen EU-Landes anzuwenden ist. Deutsche Aufsichtsbehörden haben damit das Recht der anderen Mitgliedstaaten der Europäischen Union zu berücksichtigen (§ 38 Abs. 1 Satz 1 BDSG).

Wird für eine in Deutschland befindliche verantwortliche Stelle ein Auftragnehmer mit Sitz in einem anderen Mitgliedstaat tätig, so findet für diejenige Datenverarbeitung, die im Auftrag getätigt wird, deutsches Recht Anwendung. Der Auftragnehmer muss das Recht der verantwortlichen Stelle beachten, deren Teil er ist (§ 3 Abs. 8 Satz 3 BDSG).

Hat das Unternehmen, das die Daten in Deutschland erhebt, verarbeitet oder nutzt, seinen Sitz in einem Drittland, gilt in jedem Fall das deutsche Datenschutzrecht, wenn die Daten nicht nur durchgeleitet werden (§ 1 Abs. 5 S. 2 BDSG). Besondere Schwierigkeiten bereitet dies bei der Inanspruchnahme von Websites.

Ein in einem Drittland ansässiger Internet Service Provider bietet in Deutschland Dienste an und erhebt über seine von Deutschland aus abrufbare Website personenbezogene Kundendaten.

Im Gegensatz zur Europäischen Datenschutzrichtlinie (Art. 4 Abs. 1 c)) ist nach deutschem Recht für dessen Anwendbarkeit nicht entscheidend, dass auf in

Deutschland belegene (automatisierte) Mittel zurückgegriffen wird, die sich in der Verfügungsgewalt des (im Drittland befindlichen) Anbieters befinden. Gleichwohl wird ein Mindestmaß an Einwirkungsmöglichkeit des Providers auf die in Deutschland stattfindende Verarbeitung vorliegen müssen. Würde nicht eine gewisse Verfügungsgewalt des Verarbeiters im Drittland über das in Deutschland befindliche Gerät gefordert, hieße dies, dass der Anbieter mit sämtlichen Rechtsordnungen konfrontiert ist allein dadurch, dass seine Website europaweit aufgerufen wird. Darüber hinaus wäre der Verarbeiter im Drittland verpflichtet, in jedem EU-Land einen Vertreter zu bestellen (§ 1 Abs. 5 Satz 3 BDSG). Dieses Ergebnis ist nicht sachgerecht. Unabhängig davon bleibt die Frage offen, wie das deutsche Recht im Drittland durchzusetzen ist.

Datenübermittlungen ins Ausland

Ein selbständiges deutsches Tochterunternehmen eines kanadischen Mutterkonzerns möchte Kunden- und Arbeitnehmerdaten einem französischen und einem in den USA befindlichen Schwesterunternehmen übermitteln. Angesichts der Vielzahl der Betroffenen soll davon abgesehen werden, die individuelle Einwilligung einzuholen.

Selbstverständlich gilt das BDSG. Die Zulässigkeit der Datenübermittlung nach Frankreich als einem EU-Land richtet sich ohne weitere Voraussetzungen nach deutschem Recht (insbesondere nach § 28 BDSG).

Die Datenübermittlung in Drittländer wie die USA und Kanada ist ebenfalls nur unter diesen Voraussetzungen zulässig, jedoch mit einer erheblichen Einschränkung: Die Übermittlung darf nicht stattfinden, wenn der Betroffene ein „schutzwürdiges Interesse“ an der Nichtübermittlung hat. Dies ist insbesondere der Fall, wenn beim Datenempfänger ein angemessenes Datenschutzniveau nicht gewährleistet ist (§ 4 b Abs. 2 Satz 1, 2 BDSG). Das macht beim Datenexport in Drittländer zusätzliche Maßnahmen erforderlich. Obwohl das Gesetz bestimmte Kriterien zur Beurteilung des Datenschutzniveaus benennt (§ 4 b Abs. 3 BDSG), ist dies ein schwieriges Unterfangen.

Der einfachste Fall ist der, dass die Europäische Kommission eine Entscheidung zur Angemessenheit des Datenschutzniveaus im Drittland getroffen hat (Art. 25 Abs. 6 Europäische Datenschutzrichtlinie); in diesem Fall kann der Datenexporteur ohne weiteres von der Angemessenheit ausgehen, er hat nur die Rechtmäßigkeit nach dem BDSG im Übrigen zu überprüfen. Eine derartige Entscheidung ist bis zum Ende des Berichtsjahrs allerdings nur für die Schweiz, Ungarn und (mit Einschränkungen) für Kanada ergangen[112].

Eine Sonderrolle spielen die USA: Die Europäische Kommission hat nach Verhandlungen mit dem US-Handelsministerium ebenfalls eine Entscheidung nach Art. 25 Abs. 6 getroffen, nach der für alle Unternehmen, die sich dem „Safe Harbor“-Verfahren unterwer-

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

fen, ebenfalls die Angemessenheit des Datenschutzniveaus anerkannt ist[113].

Wer einen Vertrag für eine Reise nach Kenia abschließt, muss damit rechnen, dass der Reiseveranstalter die Unterbringung in Kenia arrangieren und hierfür personenbezogene Daten übermitteln muss. Die dafür erforderlichen Daten des Betroffenen dürfen ohne Einwilligung an das gebuchte Hotel in Kenia übermittelt werden (§ 4 c Abs. 1 Satz 1 Nr. 2 oder 3 BDSG). Sollen die Daten in Kenia über den ursprünglichen Vertragszweck hinaus noch weiterverarbeitet, etwa an Ausflugsunternehmen vor Ort gegeben werden, damit diese den Reisenden gezielt mit Angeboten umwerben können, so ist hierfür aber die Einwilligung des Betroffenen erforderlich.

Sollen personenbezogene Daten in andere Drittstaaten übermittelt werden, ist zunächst zu prüfen, ob eine der Voraussetzungen des § 4 c Abs. 1 BDSG vorliegt. Insbesondere wenn die Datenübermittlung zur Vertragserfüllung erforderlich ist oder die Einwilligung der Betroffenen in die Datenübermittlung ins Drittland vorliegt, kommt es auf die Angemessenheit des Datenschutzniveaus nicht an. Diese Regelung, die bereits von der Europäischen Datenschutzrichtlinie vorgegeben ist, ist unbefriedigend: Erleichtert sie doch die Datenübermittlung gerade bei Daten, denen hohe Vertraulichkeit zukommt (z. B. Kundendaten), ohne dass der Datenimporteur im Drittland besondere datenschutzrechtliche Verpflichtungen auferlegt bekommt. Zur Wahrung der schutzwürdigen Interessen der Betroffenen ist auch in diesen Fällen der Datenexporteur verpflichtet, dafür Sorge zu tragen, dass der Vertragspartner datenschutzgerecht mit den übermittelten Daten umgeht.

Liegen die Voraussetzungen des § 4 c Abs. 1 BDSG nicht vor, ist die Angemessenheit des Datenschutzniveaus im Einzelfall zu prüfen. Zuständig für die Überprüfung ist die übermittelnde Stelle. Dies folgt daraus, dass sie die Verantwortung für die Zulässigkeit der Übermittlung trägt (§ 4 b Abs. 5 BDSG). Sie kann dabei selbst eine Beurteilung der datenschutzrechtlichen Lage vornehmen, kann insbesondere auch branchenspezifische Regelungen im Drittland (wie etwa im Bereich medizinischer Daten) berücksichtigen.

Hilft auch dies, wie in der Mehrzahl der Fälle zu erwarten, nicht weiter, müssen hinreichende Garantien für die Einhaltung des Datenschutzes im Drittland geschaffen werden. Das BDSG sieht hierfür Vertragsklauseln oder verbindliche Unternehmensregelungen vor. Allerdings müssen in diesem Fall die Datenübermittlungen von den Aufsichtsbehörden genehmigt und an die Europäische Kommission gemeldet werden.

Die Garantien können sich aus einem Vertrag zwischen dem Datenexporteur und dem -importeur ergeben (§ 4 c Abs. 2 Satz 1 BSDG). Damit wird der (wenn überhaupt vorhandene) Datenschutz beim im Drittland befindlichen Datenimporteur auf ein angemessenes

[113] ABl. EG vom 25. August 2000, L 215/7

Niveau „gehoben“. Welche inhaltlichen Anforderungen zu erfüllen sind, hat die Europäische Kommission bereits entschieden (Art. 26 Abs. 4 Europäische Datenschutzrichtlinie). Zugleich hat sie *Mustervertragsklauseln* entworfen[114]. Ihre Verwendung ist nicht zwingend, hat aber den Vorteil, dass die nach § 4 c Abs. 2 BDSG erforderliche Genehmigung der Aufsichtsbehörde entbehrlich ist. Die Behörde kann dann jedoch im Rahmen ihrer Aufsichtsbefugnisse von den exportierenden Unternehmen die Vorlage des Vertrages fordern, damit sie die behauptete vollständige Verwendung der Mustervertragsklauseln überprüfen kann.

Daneben kann natürlich auch der Weg individueller Vereinbarungen gewählt werden. Die darauf beruhenden Übermittlungen müssen dann von der Aufsichtsbehörde genehmigt werden. Im Düsseldorfer Kreis hat man sich darauf verständigt, bei der Bewertung das Arbeitspapier 12 (WP 12) der Art. 29-Gruppe[115] zugrunde zu legen. Es ist somit hilfreich, von Anfang an die dort enthaltenen Kriterien zu berücksichtigen.

Bei Datenübermittlungen innerhalb weltweit tätiger Konzerne kann die Angemessenheit des Schutzniveaus für in Drittländern tätige Unternehmensteile auch über verbindliche *Unternehmensregelungen* hergestellt werden (§ 4 c Abs. 2 Satz 1 a. E. BDSG). Ziel ist, konzernweit ein einheitliches, im Sinne der Europäischen Datenschutzrichtlinie adäquates Datenschutzniveau herzustellen. Der Vorteil besteht darin, dass eventuell erforderliche Einzelverträge des in Deutschland ansässigen Datenexporteurs mit allen in Drittländern befindlichen Datenimporteuren entbehrlich sind. Die Unternehmensregelungen sind der zuständigen Aufsichtsbehörde zur Genehmigung der konkreten Datenübermittlung vorzulegen.

Bei verschiedenen Gesellschaften eines Konzerns innerhalb Deutschlands liegt die Federführung für die Überprüfung der Regelungen nach einer Absprache im Düsseldorfer Kreis bei der Aufsichtsbehörde am Hauptsitz des Konzerns. Sie nimmt die Beurteilung im Einvernehmen mit den anderen zuständigen Aufsichtsbehörden vor. Ungeklärt ist bislang das Genehmigungsverfahren bei verschiedenen in Europa befindlichen Gesellschaften ein und desselben Konzerns. Aus Vereinfachungsgründen sollte eine bereits von einer europäischen Aufsichtsbehörde überprüfte Unternehmensregelung von der anderen nur noch auf Vereinbarkeit mit dem eigenen nationalen Recht überprüft werden.

Bei Verwendung von Unternehmensregelungen und Vertragsklauseln ist eine zweistufige Betrachtung vorzunehmen. In der 1. Stufe ist die Rechtmäßigkeit der konkreten Datenübermittlung zu prüfen (§§ 4 Abs. 1, 4a, 28 ff. BDSG). Das Ergebnis dieser Überprüfung ist nicht Gegenstand der Genehmigung, allerdings Voraussetzung für die Genehmigungsfähigkeit. Sodann

[114] ABl. EG vom 4. Juli 2001, L 181/19, vgl: Anlagenband, a.a.O. II.1; vgl. auch JB 2000, 4.7; vgl. auch Mustervertragsklauseln für die Auftragsdatenverarbeitung, ABl. EG vom 10. Januar 2002, L 6/52, vgl: Anlagenband, a.a.O., II.2
[115] Anlagenband „Dokumente zum Datenschutz 1998“, S. 29

wird festgestellt, ob eine der Voraussetzungen des § 4c Abs. 1 BDSG vorliegt oder ein angemessenes Schutzniveau beim Empfänger vorhanden ist (2. Stufe, z. B. Feststellung der Europäischen Kommission nach Art. 25 Abs. 6 Europäische Datenschutzrichtlinie, Vertragsklauseln oder verbindliche Unternehmensregelungen).

Auch die Unternehmensregelungen sollten inhaltlich an den Vorgaben des Arbeitspapiers WP 12 der Art. 29-Gruppe sowie an den Mustervertragsklauseln der Europäischen Kommission ausgerichtet sein („horizontale Gleichwertigkeit"). Dabei ist insbesondere darauf zu achten, dass festgelegt wird, wie und bei welcher Stelle die Rechte des Betroffenen durchgesetzt werden können (z. B. durch „Drittbegünstigtenklausel", gesamtschuldnerische Haftung). Ein Verstoß gegen (aufgrund von Verträgen oder Unternehmensregelungen) genehmigte Datenübermittlungen führt – mangels Befugnisregelung im BDSG – zwar nicht zur Aussetzung der Vollziehung des Datentransfers durch die Aufsichtsbehörde. Er kann aber die Rücknahme der Genehmigung oder die Verhängung eines Bußgeldes gegen den Datenexporteur nach sich ziehen (§ 43 Abs. 2 Nr. 1 BDSG).

Safe Harbor

Bislang liegen europaweit keine Beschwerden über US-Unternehmen vor, die sich zwar den Safe-Harbor-Prinzipien[116] unterworfen haben, diese jedoch nicht einhalten. In die vom US-Handelsministerium eingerichtete und öffentlich zugängliche Liste waren zum Jahresende nach zögerlichem Start ca. 130 US-Unternehmen als „Harborites" eingetragen. Das informelle Gremium („Panel"), das eigens für die Kooperation zwischen den beigetretenen US-Organisationen und den europäischen Datenschutzbehörden in Streitfällen eingerichtet worden ist, musste bislang nicht tätig werden[117]. Die Art. 29-Gruppe hat zwischenzeitlich ein Formular für Beschwerden im Zusammenhang mit „Safe Harbor" entworfen, dessen Verwendung zwar nicht zwingend ist, aber im Hinblick auf das Sprachproblem in Europa eine einheitliche Behandlung der Beschwerdefälle gewährleistet.

Immer wieder zu betonen ist gerade gegenüber US-Unternehmen, dass die Verpflichtung auf die Safe-Harbor-Prinzipien allein nicht ausreicht, um die Übermittlung von Daten in das US-Unternehmen für zulässig zu erachten. Zunächst müssen die nationalen materiellen Voraussetzungen für die Datenübermittlung vorliegen. Der deutsche Gesetzgeber hat dem Erfordernis dieser Zwei-Stufen-Prüfung für Datenübermittlungen in Drittländer durch § 4 b Abs. 2 Satz 1, 2 BDSG Rechnung getragen.

Übermittlung in Drittländer mit Einwilligung

Ein deutscher Hersteller von aktiven Herzimplantaten führt eine klinische Studie zur Zulassung gleicher Produkte in Japan durch. Die für die Studie erforderlichen

[116] JB 1999, JB 2000, jeweils 4.7
[117] JB 2000, 4.7; vgl. auch Anlagenband „Dokumente zum Datenschutz 2000", S. 51

personenbezogenen Daten umfassen neben den Standarddaten des Patienten im Wesentlichen Messdaten des Implantates. Der zum japanischen Kooperationspartner geschickte Bericht enthält zunächst nur die Ergebnisse der Datenanalyse mit gemittelten Werten. Die japanische Zulassungsbehörde hat jedoch das Recht, bei Bedarf zur Überprüfung der Studie, der Vollständigkeit und Korrektheit der Daten Einsicht in die jeweiligen Patientenakten zu nehmen. Ein Datenschutzvertrag zwischen dem Datenexporteur und dem japanischen Importeur soll aus verwaltungstechnischen Gründen vermieden werden.

Bislang ist Japan ein Drittland ohne angemessenes Datenschutzniveau. Sofern es überhaupt notwendig ist, personenbezogene Daten zu übermitteln, ist dies nur zulässig, wenn die informierte Einwilligung des Patienten vorliegt (§ 4 c Abs. 1 Satz 1 Nr.1, § 4 a Abs. 3 BDSG). Auch dieses Beispiel belegt den Wertungswiderspruch, der entstehen kann, wenn die Einwilligung als einziges Zulässigkeitskriterium für eine Datenübermittlung in Drittländer angesehen wird. „Sensible“ (z. B. medizinische) Daten könnten unter einfacheren Voraussetzungen übermittelt werden als „normale“ Daten, für deren Übermittlung neben den materiellrechtlichen Zulässigkeitsvoraussetzungen auch noch ein angemessenes Datenschutzniveau beim Empfänger erforderlich ist. Deshalb wäre es auch bei der Einwilligung sachgerecht, zusätzlich beim Empfänger die ordnungsgemäße Datenverarbeitung sicherzustellen.

An den japanischen Mutterkonzern eines deutschen Tochterunternehmens sollen aus Deutschland Daten derjenigen Mitarbeiter gegeben werden, die an einem Gewinnbeteiligungsprogramm des Konzerns teilnehmen wollen.

Da sich die Erforderlichkeit der Datenübermittlung nicht aus dem Arbeitsverhältnis ergibt, ist bereits materiell eine Einwilligung notwendig (1. Stufe). Diese muss auch das Einverständnis für die Übermittlung nach Japan umfassen (2. Stufe). Allerdings ist im Verhältnis Arbeitgeber - Arbeitnehmer die Einwilligung als Rechtsgrundlage für die Übermittlung von Arbeitnehmerdaten problematisch, weil nicht sichergestellt ist, dass sie auf der freien Entscheidung des Arbeitnehmers beruht (§ 4 a Abs. 1 Satz 1 BDSG). Frei ist die Entscheidung jedenfalls dann, wenn der Arbeitnehmer bei Verweigerung der Einwilligung keine Nachteile durch den Arbeitgeber befürchten muss. Im Beispiel entzieht sich der Mitarbeiter bei Verweigerung der Einwilligung lediglich dem Bonussystem. Seine Rechtsposition wird dadurch nicht verschlechtert.

4.8 Organisation und Technik

4.8.1 Behördliche und betriebliche Datenschutzbeauftragte

Es war von Anfang an klar, dass die Umsetzung der Europäischen Datenschutzrichtlinie in deutsches Datenschutzrecht die Prioritäten auf die verstärkte dezentrale Kontrolle des Datenschutzes in Unternehmen und

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Behörden legen würde. An Stelle des in einigen anderen europäischen Ländern bevorzugten zentralistischen Kontrollmodells mit starker zentraler Kontrollstelle und ausgeprägtem Meldewesen an die Kontrollstelle wurde in Deutschland auf die Eigenverantwortung der für die Datenverarbeitung verantwortlichen Stellen gesetzt. Dem Bundes- und den Landesdatenschutzbeauftragten wurde eine koordinierende und beratende und auf Stichproben bzw. Anlässe bezogene kontrollierende Rolle zugewiesen. Das Meldewesen wurde bis auf wenige Ausnahmen abgeschafft.

Das novellierte Bundesdatenschutzgesetz beschränkt die Meldepflicht von privaten Unternehmen an die Aufsichtsbehörde auf wenige Branchen (im Wesentlichen Detekteien, Auskunfteien, Markt- und Meinungsforscher) und in wenigen Sonderfällen auf sehr kleine Unternehmen, die keinen betrieblichen Datenschutzbeauftragten bestellen müssen. Dafür werden den betrieblichen Datenschutzbeauftragten zusätzliche Aufgaben zugewiesen: Führung der Übersichten der automatisierten Verarbeitungen, Einsichtnahme durch jedermann in diese Übersichten auf Antrag, Vorabkontrolle.

Für Bundesbehörden sieht das neue Bundesdatenschutzgesetz erstmals die Bestellung behördlicher Datenschutzbeauftragter vor.

Das neue Berliner Datenschutzgesetz ist diesen Vorgaben ebenfalls gefolgt, hat die Position der behördlichen Datenschutzbeauftragten der öffentlichen Stellen Berlins verstärkt und ihren Aufgabenbereich erweitert.

Der Aufgabenkreis des behördlichen Datenschutzbeauftragten ist nicht nur auf neue Aufgaben erweitert, sondern teilweise auch reduziert worden. So ist das Recht des behördlichen Datenschutzbeauftragten entfallen, bei der Auswahl von bei der Verarbeitung personenbezogener Daten tätigen Personen beratend mitzuwirken.

Vorabkontrolle

Eine völlig neue Aufgabe des behördlichen Datenschutzbeauftragten ist die Durchführung von Vorabkontrollen, die vor der Entscheidung über den Einsatz oder eine wesentliche Änderung der Datenverarbeitung durchzuführen sind, wenn die Verarbeitung Daten betrifft, die Berufs- oder besonderen Amtsgeheimnissen unterliegen oder zur Verfolgung von Straftaten und Ordnungswidrigkeiten erhoben werden. Dabei betreffen die Vorabkontrollen die Wirksamkeit der technischen und organisatorischen Maßnahmen. Da diese jetzt auf einem Sicherheitskonzept basieren müssen, welches auf den Ergebnissen einer Risikoanalyse aufbauen muss, gehört es also zu den Aufgaben der behördlichen Datenschutzbeauftragten, die Plausibilität der Risikoanalyse, die Wirkung der im Konzept vorgesehenen Maßnahmen auf die erkannten Risiken und die strikte Umsetzung des Konzepts zu kontrollieren. Auch wenn es im Gesetz nicht explizit genannt wird, so gehört es dennoch zu den Aufgaben der behördlichen Datenschutzbeauftragten, im Vorfeld der Inbetriebnahme eines personenbezogenen IT-Verfahrens auch auf die Zulässigkeit der Datenverarbeitung, der vorgesehenen Datenübermittlungen sowie auf die Maßnahmen zur Wahrung der Rechte der Betroffenen zu achten.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Die Vorabkontrolle wird Bestandteil des nunmehr stets gesetzlich für alle öffentlichen Stellen vorgeschriebenen Sicherheitskonzepts. Solche – in der Regel verfahrensspezifischen – Sicherheitskonzepte sind bereits seit 1999 im Geltungsbereich der IT-Sicherheitsrichtlinie des Landes Berlin für jedes neue Verfahren zu erstellen.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit beteiligt sich an den Vorabkontrollen nur, wenn der behördliche Datenschutzbeauftragte auf Zweifelsfälle gestoßen ist und fachliche Hilfe benötigt und wenn die Vorabkontrolle verwaltungsübergreifende Verfahren betrifft.

Auch die betrieblichen Beauftragten für den Datenschutz haben Vorabkontrollen durchzuführen, soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen (§ 4 d Abs. 5 BDSG). Als Regelbeispiel wird die Verarbeitung besonderer Arten personenbezogener Daten wie Gesundheitsdaten oder Daten über Religion und Weltanschauung sowie Daten zur Bewertung der Persönlichkeit der Betroffenen genannt; die Vorabkontrollen dürfen sich allerdings nicht auf diese Fälle beschränken. Vielmehr haben sie sich auch auf andere besonders eingreifende Verarbeitungen zu erstrecken wie z. B. Videoüberwachung oder Chipkarteneinsatz.

Dateibeschreibungen

Der behördliche Datenschutzbeauftragte hat nach dem neuen Berliner Datenschutzgesetz Dateibeschreibungen zu führen. Dieser Begriff ist missverständlich und bringt die Dateibeschreibungen unrichtigerweise in einen Zusammenhang mit den früher zu führenden und an den Landesdatenschutzbeauftragten weiterzuleitenden Dateienregistern. Tatsächlich handelt es sich um schriftliche Festlegungen für automatisierte Verarbeitungen. Dies ist eine abstraktere Darstellung der Datenverarbeitung, die einen geringeren Aktualisierungsbedarf aufweisen wird. Neu ist auch, dass jede Person unentgeltlich in den öffentlichen Teil dieser Dateibeschreibungen einsehen kann. Die bisherige Praxis der meisten Berliner Behörden, die internen Transparenzpflichten nur unzureichend zu erfüllen, könnte öffentliches Missfallen auslösen.

Der Begriff „Dateibeschreibung“ sollte bei der nächsten Änderung des Berliner Datenschutzgesetzes durch einen treffenderen Begriff ersetzt werden.

Wegen des Wegfalls des Dateien- und Geräteregisters beim Berliner Beauftragten für Datenschutz und Informationsfreiheit werden auch wir verstärkt auf die korrekte und aktuelle Führung der Dateibeschreibungen achten, weil wir uns anders nicht mehr über den Ist-Zustand der Datenverarbeitung unterrichten lassen können. Lücken in den Dateibeschreibungen führen damit zu Kontrolllücken, die nur durch aufwendige Vorortерhebungen geschlossen werden können.

Bestellung von behördlichen Datenschutzbeauftragten und ihrer Vertreter

Wie auch die betrieblichen Datenschutzbeauftragten müssen behördliche Datenschutzbeauftragte und neuerdings auch ihre Vertreter formell und damit schriftlich

Eine kommissarische Aufgabenwahrnehmung kann – beispielsweise im Fall einer längerfristigen Erkrankung des bestellten behördlichen Datenschutzbeauf-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

bestellt werden. Die häufig vorzufindende Praxis, der Bestellung von Personen in dieses Amt das Attribut „kommissarisch“ oder „vorläufig“ anzuheften, ist nicht akzeptabel, wenn mit diesen Einschränkungen auch Einschränkungen der Rechte und des Status der Datenschutzbeauftragten verbunden sein sollen. Der Gesetzgeber hat die betrieblichen und behördlichen Datenschutzbeauftragten so ausgestattet, dass sie innerhalb ihres Unternehmens oder der Behörde unabhängig tätig sein können. Sie genießen Weisungsfreiheit, weitgehenden Schutz vor Abberufung gegen ihren Willen und direkten Zugang an die Organisationsspitze, soweit sie ihre Fachkunde als Datenschutzbeauftragte wahrnehmen. Sie dürfen nur bestellt werden, wenn sie über die notwendige Fachkunde verfügen und zuverlässig sind. Letzteres konkretisiert das neue Berliner Datenschutzgesetz dahingehend, dass sie durch die Bestellung keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt sein dürfen.

tragten – als durchaus geboten erscheinen, zumal eine einmal erfolgte Bestellung aufgrund der Regelung des § 19 a Abs. 2 Satz 3 BlnDSG nicht ohne weiteres widerrufen werden kann. Allerdings stimmt der Senat mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit darin überein, dass solche Fälle, unabhängig von der personal- und dienstrechtlichen Problematik, nicht zu einer Entwertung der Rechtsstellung des behördlichen Datenschutzbeauftragten und einer Umgehung der Normen des BlnDSG führen dürfen.

Bei den von uns seit Jahren begleiteten Koordinierungstreffen der bezirklichen Datenschutzbeauftragten, die im Wesentlichen dem Erfahrungsaustausch dienen, standen die im direkten Bezug zu den Datenschutzbeauftragten stehenden Neuerungen des Berliner Datenschutzgesetzes im Vordergrund.

Die Koordinierungsgruppe, an der bedauerlicherweise nur ein Teil der bezirklichen Datenschutzbeauftragten teilnimmt, hat sich auch konstruktiv an der Schaffung von Grundlagen für die Umsetzung des Berliner Datenschutzgesetzes beteiligt. So ist ein Formular zur Führung der Dateibeschreibungen entwickelt worden, das noch mit der Senatsverwaltung für Inneres abgestimmt wird. Ziel ist es, ein möglichst einheitliches Muster einer Dateibeschreibung für die gesamte Berliner Verwaltung zu erstellen, das bei Bedarf auch aus unserem Internetangebot.abgerufen werden kann.

Die Abstimmung zwischen der Senatsverwaltung für Inneres und dem Berliner Beauftragten für Datenschutz und Informationsfreiheit ist mittlerweile abgeschlossen. Die Senatsverwaltung für Inneres hat ihr Formular zur Führung der Dateibeschreibung an die betroffenen öffentlichen Stellen als Vordruckangebot übersandt. Die Verwendung des Formulars ist für die datenverarbeitenden Stellen nicht verbindlich, erscheint aber aus Gründen der Einheitlichkeit bei der Führung von Dateibeschreibungen im Land Berlin wünschenswert. Entscheidend ist, dass die datenverarbeitenden Stellen den Anforderungen des § 19 Abs. 2 BlnDSG hinsichtlich der dort genannten schriftlichen Festlegungen Rechnung tragen.

Außerdem haben wir einen Leitfaden für die Durchführung der Vorabkontrolle erarbeitet, der die behördlichen Datenschutzbeauftragten auch bei der Durchführung dieser neuen Aufgabe unterstützen soll.

Probleme mit der Bestellung von Datenschutzbeauftragten

Schon immer haben wir bei Kontrollen beobachtet, dass dann, wenn ein ordnungsgemäß bestellter und von der Unternehmens- oder Behördenleitung gut unterstützter Datenschutzbeauftragter wirkte, die Ergebnisse der Kontrollen signifikant besser ausfielen, als wenn dies nicht der Fall war. Die bessere Unterrichtung der Mitarbeiter über datenschutzgerechtes Verhalten, die rechtzeitige Einflussnahme auf die Gestaltung organisatorischer und informationstechnischer Prozesse, die Aufmerksamkeit für alltägliche Nachlässigkeiten beim Umgang mit personenbezogenem Material und viele andere Eigenschaften und Aktivitäten des Datenschutzbeauftragten führen zu einer Akzeptanz des Datenschutzes, die gleichzeitig konstruktiv ist. Die mit den neuen Datenschutzgesetzen bedeutender gewordene Rolle des betrieblichen oder behördlichen Daten-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

schutzbeauftragten macht es noch erforderlicher, auf die ordnungsgemäße Bestellung und die ausreichende Ausstattung der Datenschutzbeauftragten zu achten. Sie können nämlich den Datenschutz in ihren Häusern sicherstellen, nicht der Landesdatenschutzbeauftragte oder die Aufsichtsbehörde.

Trotzdem müssen wir auch in diesem Jahr über grobe Mängel bei der organisatorischen Sicherstellung des Datenschutzes berichten.

Da eine bei der geplanten Einführung modifizierter informationstechnischer Verfahren vorgesehene Beteiligung des behördlichen Datenschutzbeauftragten des *Universitätsklinikums Benjamin Franklin* daran scheiterte, dass die Verwaltungsleitung keinen Datenschutzbeauftragten nennen konnte, wurden wir gebeten, die gewünschte Stellungnahme zu den Verfahren abzugeben. Dies war Anlass genug, das Klinikum offiziell nach der Bestellung eines behördlichen Datenschutzbeauftragten zu fragen. Zwar wurde ein Name genannt und eine Bestellung aus dem Jahre 1993 vorgelegt, bei der näheren Kontrolle stellte sich jedoch heraus, dass dieser Datenschutzbeauftragte bereits 1995 mit seinem Einverständnis, weil er sich angesichts der technischen Entwicklung nicht mehr als sachkundig einschätzte, durch einen externen Datenschutzbeauftragten abgelöst worden war. Dessen Vertrag wurde im Frühjahr 2000 aus Ersparnisgründen nicht mehr verlängert, ein neuer Datenschutzbeauftragter wurde nicht bestellt. Da die Aufgabenentbindung des früheren Datenschutzbeauftragten nicht schriftlich vollzogen wurde, ging die Verwaltungsleitung stillschweigend davon aus, er sei wieder im Amt. So war klar, dass zur Bestellung Missverständnisse auftraten. Auf jeden Fall wurde bis zum Ende des Berichtszeitraums kein Datenschutzbeauftragter aktiv.

Um eine formelle Beanstandung abzuwenden, gab der Ärztliche Direktor des Klinikums die Zusage, dass bis zum Ablauf einer gemeinsam vereinbarten Frist ein Datenschutzbeauftragter ordnungsgemäß bestellt würde, der mindestes bis zur Aufarbeitung der über Jahre versäumten datenschutzrechtlichen Pflichten vollzeitig tätig werden müsste, und bis zum Ablauf einer weiteren Frist die gesetzlich geforderten Dateibeschreibungen erstellt werden würden.

Nach Ablauf der Frist erreichte uns eine Absichtserklärung, eine benannte Person zum Datenschutzbeauftragten sowie einen Vertreter zu bestellen. Da der Kandidat über keine Sachkenntnis als Datenschutzbeauftragter verfügte, haben wir ihm Hinweise für die Erlangung der erforderlichen Sachkenntnisse gegeben und unsere Unterstützung zugesagt. Allerdings lag auch einen Monat nach Ablauf der Frist keine Bestellung vor, so dass wir von einer Beanstandung nicht mehr absehen konnten.

In einem *Krankenhaus der Vivantes-Gruppe*, das wir einer Kontrolle unterzogen hatten[118], war zwar ein

Die Funktion des Behördlichen Datenschutzbeauftragten für den Fachbereich Humanmedizin war durch den zwischen 1993 und 2001 bestellten Behördlichen Datenschutzbeauftragten permanent besetzt. Er wurde nicht, wie im Bericht erwähnt, von einem externen Datenschutzbeauftragten abgelöst und damit entpflichtet, sondern lediglich bei der Wahrnehmung seiner Aufgaben unterstützt. Auf Grund der in diesem Zusammenhang aufgetretenen Problematik wurde jedoch eine personelle Veränderung angestrebt und durch die Bestellung eines neuen Behördlichen Datenschutzbeauftragten gelöst.

Der mit Wirkung von 13.2.2002 bestellte Behördliche Datenschutzbeauftragte für den Fachbereich Humanmedizin hat im Hinblick auf die vom Berliner Beauftragten für Datenschutz und Informationsfreiheit vorgetragenen Beanstandungen unverzüglich reagiert und mit den erforderlichen Maßnahmen zur Einrichtung dieses Aufgabengebiets begonnen.

Zum Erwerb der für die Durchführung des Datenschutzes erforderlichen Fachkunde besuchte der bestellte Behördliche Datenschutzbeauftragte Fortbildungsveranstaltungen an der Verwaltungsakademie bzw. ist eine weitere Teilnahme an Fortbildungsveranstaltungen beabsichtigt. Weiterhin wurden Ansprechpartner in den wissenschaftlichen Einrichtungen, Dezernaten und Sonderbereichen des Fachbereichs Humanmedizin benannt.

Im Rahmen eines ersten persönlichen Kontaktgesprächs erfolgen nunmehr Vororterhebungen, die zur Abklärung des Vorhandenseins von personenbezogenen Daten dienen. Diese aufwändige Datensammlung soll gleichzeitig die zu erstellenden Datenbeschreibungen vorbereiten. In diesem Zusammenhang werden auch Einschätzungen vorgenommen, in welchen Bereichen die vorgeschriebenen Vorabkontrollen erfolgen müssen.

In der weiteren Perspektive sind - als ergänzende Ausführung zum Datenschutz – auch entsprechende Unterweisungen gegenüber den Mitarbeitern des Fachbereichs Humanmedizin geplant.

Das Universitätsklinikum Benjamin Franklin geht davon aus, dass die intensiven Bemühungen und die gesamte Vorgehensweise des neuen Behördlichen Datenschutzbeauftragten den vom BlnBDI aufgezeichneten Nachholbedarf im angemessenen Zeitrahmen

[118] vgl. 4.4.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Datenschutzbeauftragter bestellt worden, der als Arzt und Systemverwalter über die notwendige Fachkunde verfügte, dem aber praktisch kein Zeitbudget für diese Aufgabe zugestanden wurde. Auch die sächliche Unterstützung seitens der Krankenhausleitung unterblieb weitgehend, denn der Datenschutzbeauftragte verfügte nicht einmal über ein Einzelzimmer, in dem er vertrauliche Gespräche, z. B. mit Patienten oder Kollegen, die sich in ihren Datenschutzrechten verletzt fühlten, führen konnte. Der Datenschutzbeauftragte verfügte weder über die erforderliche Zeit noch über den erforderlichen Rückhalt seitens der Krankenhausleitung, um den notwendigen Überblick über die Datenverarbeitung im Hause, geschweige denn die gesetzlich geforderten Übersichten bzw. Verzeichnisse zu erhalten. So konnte nicht verwundern, dass die Kontrollmaßnahme zu sehr schlechten Ergebnissen führte.

befriedigen und das Klinikum den gesetzlichen Vorgaben entsprechen wird.

4.8.2 Organisation des Datenschutzes in privaten Unternehmen

Registerführung

Im Zuge der Novellierung des Bundesdatenschutzgesetzes wurde auch für private Unternehmen das Meldewesen zum Register der Aufsichtsbehörde grundlegend geändert.

§§ 4 d und 4 e BDSG stellen nunmehr die neue – leider kompliziert geratene - Rechtsgrundlage für die Meldepflicht dar. Nach § 4 d Abs. 1 müssen Verfahren automatisierter Verarbeitungen vor der Inbetriebnahme bei der zuständigen Aufsichtsbehörde gemeldet werden. Tatsächlich ergeben sich durch die Regelungen in § 4 d Abs. 2-4 jedoch so viele Ausnahmen, dass die Meldepflicht gegenüber der früheren Regelung weiter reduziert worden ist. Im Gegensatz zu früher müssen sich Unternehmen, die geschäftsmäßig im Auftrag für andere Datenverarbeitung betreiben, grundsätzlich nicht mehr bei der Aufsichtsbehörde melden.

In erster Linie unterfallen nunmehr der Meldepflicht die Verfahren automatisierter Verarbeitungen, in denen personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung (§ 29 BDSG, z. B. Detekteien, Auskunfteien, Adresshandel) oder zum Zweck der anonymisierten Übermittlung (§ 30 BDSG, z. B. Markt- und Meinungsforschung) gespeichert werden.

Für Verfahren automatisierter Verarbeitungen mit personenbezogener Daten, die anderen Zwecken dienen, entfällt die Meldepflicht, wenn die verantwortliche Stelle einen betrieblichen Datenschutzbeauftragten bestellt hat. Eine Pflicht zur Bestellung besteht, wenn die verantwortliche Stelle

- mit mehr als vier Arbeitnehmern personenbezogene Daten automatisiert erhebt, verarbeitet oder nutzt oder
- automatisierte Verarbeitungen vornimmt, die einer Vorabkontrolle nach § 4 d Abs. 5 BDSG unterliegen, oder

- personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung oder der anonymisierten Übermittlung erhebt, verarbeitet oder nutzt.

Sofern ein Unternehmen wegen der geringen Anzahl der mit der Datenverarbeitung beschäftigten Mitarbeiter keinen betrieblichen Datenschutzbeauftragten bestellen muss, ist es dennoch von der Meldepflicht befreit, sofern es Daten nur im Rahmen seiner vertraglichen Verpflichtungen verarbeitet. Um auch in anderen Fällen keine Meldepflicht auszulösen, empfehlen wir auch bei kleinen Unternehmen die freiwillige Bestellung eines Datenschutzbeauftragten.

Sind Meldungen abzugeben, müssen sie durch die Stelle erfolgen, die für die Verarbeitung verantwortlich ist. Die Stelle muss aber auch dann melden, wenn sie Dienstleistungsunternehmen mit der Verarbeitung im Auftrag betraut. Die Meldungen haben bereits vor Inbetriebnahme des meldepflichtigen Verfahrens zu erfolgen. Auch Änderungen und Auflösungen des Verfahrens sind rechtzeitig schriftlich zu melden.

Neu ist, dass das Register der Aufsichtsbehörde kein Firmenregister mehr ist, zu dem sich Unternehmen mit bestimmten Angaben über Struktur, Leitung und Unternehmenszweck melden müssen, sondern ein Register der Verfahren automatisierter Verarbeitungen. Demzufolge werden die Unternehmen in der Regel mehrere Meldungen abgeben müssen.

Auch der Zweck des Registers hat sich geändert. Nach dem alten BDSG enthielt das Register der Aufsichtsbehörde alle Unternehmen, die die Aufsichtsbehörde ohne bestehenden Anlass von Amts wegen kontrollieren durfte. Dieser Zweck entfiel mit dem neuen BDSG, denn der Vorbehalt, dass bei den meisten privaten Unternehmen nur bei Vorliegen eines Anlasses kontrolliert werden durfte, wurde gestrichen. Nunmehr unterliegen alle privaten Unternehmen der anlassfreien Kontrolle durch die Aufsichtsbehörde. Im Register bleiben nur noch solche Unternehmen, die aufgrund ihrer Geschäftstätigkeit der besonderen datenschutzrechtlichen Aufmerksamkeit bedürfen, und Kleinstunternehmen, die keinen betrieblichen Datenschutzbeauftragten bestellt haben, obwohl sie personenbezogene Daten zu anderen Zwecken als zur Erfüllung vertraglicher Verpflichtungen verarbeiten.

Der Inhalt der Meldung ergibt sich aus § 4 e BDSG, wobei im Gegensatz zu den bisherigen meldepflichtigen Einzelangaben nun neuerdings aus Vereinfachungsgründen auch Kategorien von Daten und Empfängern gemeldet werden können. Völlig neu ist die Angabe von geplanten Datenübermittlungen in Drittstaaten außerhalb der Europäischen Gemeinschaft bzw. des Europäischen Wirtschaftsraums.

Die Änderungen des datenschutzrechtlichen Meldewesens bei der Aufsichtsbehörde bedeuten, dass das noch bestehende Register alten Rechts bereinigt werden muss und dass auch die Unternehmen, die bereits zum alten Register gemeldet haben und weiterhin meldepflichtig bleiben, neue Meldungen abzugeben haben.

Es besteht für Verarbeitungen, die vor dem In-Kraft-Treten des neuen Bundesdatenschutzgesetzes schon bestanden haben, eine Übergangsfrist von drei Jahren.

Eine Arbeitsgruppe des Düsseldorfer Kreises hat sich mit den Neuerungen der Meldepflicht befasst und auch ein Merkblatt, eine Ausfüllanleitung und das entsprechende Meldeformular entwickelt, das möglichst von allen meldepflichtigen Stellen verwendet werden sollte. Die Aufsichtsbehörden halten diese Dokumente in ihren Internetangeboten zum Downloaden bereit.

Erfahrungen aus Routinekontrollen in privaten Unternehmen

Bei unseren regelmäßigen technisch-organisatorischen Kontrollen der Firmen und Unternehmen im privaten Bereich haben wir auch im letzten Jahr wieder Mängel bei der Einhaltung des Datenschutzes festgestellt, von denen exemplarische Fälle hier kurz dargestellt werden:

Bei einigen Firmen wurde festgestellt, dass sie zwar einen betrieblichen Datenschutzbeauftragten bestellt haben, doch an eine Stellvertreterregelung nicht gedacht haben. Gerade auch bei Abwesenheit des bestellten Datenschutzbeauftragten - sei es durch Urlaub, Krankheit oder aus sonstigen Gründen - ist es erforderlich, dass der Datenschutz im Hause weiterhin sichergestellt wird. Wir empfehlen den Firmen, rechtzeitig einen Stellvertreter zu benennen, der auch insbesondere in Bezug auf die Fachkunde geschult sein sollte. Bei sehr kleinen Firmen empfehlen wir, dass zumindest ein weiterer Mitarbeiter vor Beginn einer vorhersehbaren Abwesenheit von dem betrieblichen Datenschutzbeauftragten in die Datenschutzproblematik des Hauses eingewiesen werden sollte.

Zu einer ordnungsgemäßen Dokumentation gehört auch eine Übersicht der Dateien und Geräte, die in einer Firma und ganz besonders in einem größeren Unternehmen vorliegen sollte. Bei unseren Kontrollen haben wir leider feststellen müssen, dass das nicht immer oder nur rudimentär der Fall war.

Diese Übersichten sind nicht nur für die Firmen selbst wichtige technisch-organisatorische Grundlagen für ihre Datenverarbeitung, sondern für Kontrollinstanzen wie die Datenschutzaufsichtsbehörde stellen sie ein hilfreiches Instrument dar, um einen schnellen Überblick über wesentliche Teile der Datenverarbeitungsinfrastruktur im Hause zu bekommen. Eine vollständige und aktuell geführte Übersicht aller Dateien und Geräte bzw. der Netzinfrastruktur kann einen Kontrollvorgang außerdem wesentlich verkürzen.

Unsere Kontrollen betrafen auch den Umgang der Mitarbeiter mit personenbezogenen Daten und insbesondere die gesetzlich vorgeschriebene Verpflichtung auf das Datengeheimnis. Bei festen Mitarbeitern wird in der Regel die Einholung dieser Verpflichtung korrekt und vor allem in schriftlicher Form durchgeführt. Bei Firmen aber, die bestimmte Mitarbeiter nur zeitweise beschäftigen oder sich sonstiger Hilfskräfte be-

dienen, wird diese Maßnahme oft vergessen oder aber nicht für erforderlich erachtet. So war ein Transportunternehmen, das des Öfteren Transporte mit datenschutzrechtlich relevantem Material durchführte, der Auffassung, dass eine mündliche Aufklärung über den Schutz personenbezogener Daten ausreichend sei.

Insbesondere bei neuen Mitarbeitern sollte bei Beschäftigungsbeginn auch durch die Unterschrift auf dem Verpflichtungsformular bewusst gemacht werden, dass der Umgang mit personenbezogenen Daten einer besonderen Aufmerksamkeit bedarf. Das Original der Verpflichtung sollte zu den Personalunterlagen genommen und eine Kopie den betreffenden Mitarbeitern ausgehändigt werden.

4.8.3 Datenschutzprobleme bei drahtlosen Netzen

Der Wegfall der Abhängigkeit von fest verlegten Kabeln macht drahtlose lokale Netze, so genannte Wireless- beziehungsweise Funk-LANs für viele Anwendungsbereiche attraktiv. Schnell kann z. B. bei einer Konferenz ein mitgebrachtes Notebook in ein Funknetz integriert werden. Auch entfallen kostenintensive Baumaßnahmen, wenn in Altbauten oder gar denkmalgeschützten Gebäuden Kabelnetze verlegt werden müssten.

Mit dem Einsatz dieser Technik ist es Anwendern, die über einen Rechner mit einer entsprechenden Funknetzwerkkarte verfügen und sich im Empfangsbereich des Netzes aufhalten, möglich, sich automatisch in das Netzwerk zu integrieren. Dieser Vorgang funktioniert voll automatisiert und lässt sich mit dem Anschluss eines Rechners an ein bestehendes kabelgebundenes Rechnernetz vergleichen.

Allerdings sind erhebliche Sicherheitsfragen zu lösen, wenn man diese Technologie für sensible Datenverarbeitungsverfahren anwenden will. Die Funkwellen kennen beispielsweise keine räumlichen Barrieren, außerhalb dieser nicht gesendet bzw. empfangen werden darf. So kann der Parkplatz vor der Firma einen sehr guten Angriffspunkt darstellen. Früher war noch ein physischer Zugang zum LAN-Kabel notwendig, heute reicht bei unzureichenden Sicherheitseinstellungen eine Funknetzwerkkarte für das Notebook aus.

Im zweiten Quartal diesen Jahres informierte uns ein prominenter Hacker-Club darüber, dass in den öffentlich zugänglichen Gebäuden, im Freigelände, ja sogar auf öffentlichem Straßenland in der Umgebung verschiedener Berliner Krankenhäuser Funknetze in Betrieb waren, die das Testsystem der Clubmitglieder aktiv in das Netz integrierten. In einem der Vivantes GmbH zugehörenden Krankenhaus war die Anwendung von Funknetzen offenkundig sehr verbreitet, so dass die Hacker eine Vielzahl von Verbindungsdaten gewinnen konnten, die den aktiven Zugang auf sensible Daten ermöglicht hätten. Da der Hacker-Club dafür bekannt ist, dass es sein Ziel ist, Schwachstellen aufzudecken, aber nicht zu nutzen, waren seine Beteuerungen glaubwürdig, dass er nicht versucht hat, in strafba-

rer Weise auf personenbezogene Patientendaten zuzugreifen.

In drei anderen Krankenhäusern, einem weiteren Vivantes-Haus, einer anderen Privatklinik und bestimmten Stationen eines Universitätsklinikums, wurden Wireless-LANs festgestellt, die externe Systeme ebenfalls automatisch einbanden, die jedoch offenbar nur zu Versuchszwecken installiert waren und keinen Zugang zu personenbezogenen Patientendaten ermöglicht hätten.

In allen Fällen lagen gravierende Administrationsmängel vor, denn die Option, in den Empfangsbereich des Wireless-LAN hineingeratene Rechner automatisch einzubinden, lässt sich abschalten. Geschieht dies, können nur solche Rechner im Netz kommunizieren, deren MAC-Adressen (Adresse der Funknetzkarte) dem Netz bekannt sind. Aus diesem Grunde konnten die Mängel bei den vier Krankenhäusern schnell beseitigt werden, nachdem wir die betrieblichen oder behördlichen Datenschutzbeauftragten dieser Häuser über die Ergebnisse der Hacker-Club-Recherchen unterrichtet hatten. Ein Haus gab die Netztechnik an den Hersteller zurück, weil dieser keine hinreichende informationstechnische Sicherheit gewährleisten konnte. Vielleicht veranlasste die schnelle Reaktion der Krankenhäuser die Redaktion des SPIEGELs dazu, in einem Artikel zu dieser Berliner Aktion des Hacker-Clubs davon abzusehen, die Namen der Krankenhäuser öffentlich zu machen[119].

Abgesehen von diesen groben Administrationsmängeln ergibt sich aus der Fachliteratur und aus den Erfahrungen, die den Datenschutzbeauftragten des Bundes und der Länder aus universitären Großeinsätzen solcher Techniken vorliegen, dass Wireless-LANs keine hinreichende informationstechnische Sicherheit bieten, wenn die vorhandenen sicherheitsspezifischen Leistungsmerkmale nicht durch zusätzliche Sicherheitsmaßnahmen ergänzt werden:

Die netzseitige Schnittstelle zur Anbindung von Rechnern an das Funknetz, der so genannte Access Point, kann so konfiguriert werden, dass sie nur die Rechner als dem Netz zugehörig anerkennt, deren MAC-Adresse bei ihr eingetragen ist. Dann erfolgt vor der Herstellung der Netzverbindung eine Filterung der MAC-Adresse. Da jedoch die MAC-Adressen von Netzkarten ohne besonderen Aufwand geändert werden können, ist es für jemanden, der eine vom Access Point zugelassene MAC-Adresse kennt, ohne weiteres möglich, sich unbefugt in das Wireless LAN einzubinden. Daher ist die MAC-Adressen-Filterung nur eine Maßnahme mit relativ geringer Wirksamkeit, insbesondere dann, wenn man mit vorsätzlichen oder gar kriminell motivierten Angriffen auf die Sicherheit solcher Netze rechnen muss. In diesen Fällen ist es notwendig, dass zusätzliche Authentifizierungsmechanismen zwischen dem Access Point und den Zugriff begehrenden Systemen eingesetzt werden, z. B. Challenge-Response-

[119] Leichtes Spiel für Datendiebe. In: DER SPIEGEL 18/2001 vom 30. April 2001, S. 208 ff.

Verfahren, bei denen die gemeinsame Verfügbarkeit geheimer Schlüssel mit kryptographischen Verfahren abgeprüft wird.

Da die Daten, die über Funkstrecken übertragen werden, abgehört werden können, ist es notwendig, dass die Daten verschlüsselt werden. Funknetze des Standards IEEE 802.11b verwenden ein symmetrisches Verschlüsselungsverfahren mit der Bezeichnung WEP (Wired-Equivalent-Privacy), standardmäßig mit 40 Bit oder 104 Bit Verschlüsselungstiefe. Eine 40-Bit-Verschlüsselung kann unter keinen Umständen als hinreichend sicher angesehen, gleichgültig, welche Algorithmen mit solchen Schlüsseln arbeiten. Eine 104-Bit-Verschlüsselung wäre hinreichend sicher, wenn beim WEP-Verfahren nicht mathematische Schwächen aufgedeckt worden wären, die von amerikanischen Forschern bereits zu erfolgreichen Kryptoanalysen genutzt werden konnten.

Daher muss es den im Einzelfall zu erstellenden Risikoanalysen überlassen bleiben, ob man mit dem Restrisiko leben und sich daher mit dem WEP-Verfahren begnügen kann oder ob zusätzliche oder alternative Verschlüsselungsverfahren, die auf den bekannt sicheren Verfahren aufbauen, eingesetzt werden müssen.

4.9 Informationsfreiheit: Auf dem Weg zur Normalität

Langsam aber stetig setzt sich in Deutschland die Informationsfreiheit durch. Im Jahr 2001 hat ein weiteres Bundesland die gesetzlichen Grundlagen dafür gelegt. Am 15. November 2001 verabschiedete der Landtag in Wiesbaden das Informationsfreiheitsgesetz Nordrhein-Westfalens, welches am 1. Januar 2002 in Kraft trat[120]. Auch hier ist die Datenschutzbeauftragte die für die Sicherstellung des Rechts auf Information zuständige Dienststelle (§ 13 Abs. 2 IFG NRW). Damit verfügen nunmehr vier Bundesländer – neben Nordrhein-Westfalen und Berlin sind dies auch Brandenburg und Schleswig-Holstein – über ein solches Gesetz.

Der Entwurf eines Bundesgesetzes zur Informationsfreiheit war Gegenstand eines sechswöchigen Diskussionsforums im Internet, das das Bundesministerium des Innern im Frühsommer anbot, um auch auf diesem Wege Anregungen zur Gesetzgebung zu sammeln. Diese Form einer frühzeitigen Einbeziehung interessierter Bürgerinnen und Bürger in den Gesetzgebungsprozess ist begrüßenswert und sollte auch in anderen Gesetzgebungsverfahren genutzt werden. Dass allerdings die Bemühungen für ein Informationsfreiheitsgesetz des Bundes – welches Gegenstand des Koalitionsvertrages von Bündnis 90/Die Grünen und SPD war – noch in der 14. Wahlperiode des Bundestages von Erfolg gekrönt sein werden, ist unwahrscheinlich, da bisher ein endgültiger Referentenentwurf nicht vorliegt.

[120] Gesetz über die Freiheit des Zugangs zu Informationen für das Land Nordrhein-Westfalen (Informationsfreiheitsgesetz Nordrhein-Westfalen, IFG NRW), GVBl. S. 806

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Auch im europäischen Rahmen hat sich die Informationsfreiheit weiterentwickelt. Mit der 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[121] haben die Unionsbürger und natürliche wie auch juristische Personen, die ihren Wohnsitz oder Sitz in einem Mitgliedstaat haben, ein gesetzlich verankertes Recht auf Zugang zu Dokumenten der Organe. Im internationalen Rahmen gibt es – initiiert durch den neuseeländischen Beauftragten – Bemühungen, die Informationsfreiheitsbeauftragten in einer ständigen Konferenz zu vernetzen.

Umfrage zum Berliner Informationsfreiheitsgesetz (IFG)

Eine erste umfangreichere Evaluation der Anwendung des IFG in Berlin hat die Senatsverwaltung für Inneres erstellt. Grundlage war eine landesweite Umfrage, in die alle öffentlichen Stellen einbezogen wurden. Sie bezog sich auf alle Anträge auf Akteneinsicht bzw. Aktenauskunft der ersten dreizehn Monate nach In-Kraft-Treten des IFG im Zeitraum vom 30. Oktober 1999 bis zum 30. November 2000. Neben der statistischen Erfassung der Anträge, der Art ihrer Bearbeitung und Bescheidung zielte die Umfrage auch auf eine Sammlung von Erfahrungen und Problemen beim Umgang mit dem IFG.

In dem der Umfrage zugrunde liegenden Zeitraum sind insgesamt 164 Anträge auf Akteneinsicht oder Aktenauskunft gestellt worden. Die Befürchtungen, ein allgemeines Informationszugangsrecht würde die Berliner Verwaltung lahm legen, sind demnach unberechtigt gewesen. Gleichwohl ist der Ansatz des IFG, das das herkömmliche Verhältnis zwischen Offenheit und Amtsverschwiegenheit umkehrt, für die Bürgerinnen und Bürger wie auch für die Verwaltungen bis heute gewöhnungsbedürftig. Die Informationsfreiheit als alltäglicher Bestandteil des Kontaktes zwischen mündigen Bürgern und der Verwaltung ist noch auf dem Wege zur Normalität. Umso mehr begrüßen wir Initiativen von öffentlichen Stellen, die Informationsrechte bekannt zu machen. Hervorzuheben ist das Bezirksamt Marzahn-Hellersdorf, das auf seiner Homepage Erläuterungen zum IFG und einen Antragsvordruck zur Akteneinsicht anbietet.

Die landesweite Umfrage zum Berliner IFG war ein wichtiger Schritt zur Kenntlichmachung der Probleme, die im Umgang mit dem neuen Gesetz zu Tage getreten sind. In der Tat ist die teilweise befürchtete „Antragsflut“ ausgeblieben. Dafür ist andererseits deutlich geworden, dass die Auslegung einzelner Paragraphen des IFG erhebliche Schwierigkeiten bereitet, die zum Teil in Formulierungen und Regelungstechnik des Gesetzes selbst begründet sind.

Problemfelder

Der Anteil der Anträge auf Akteneinsicht oder Aktenauskunft gegenüber öffentlichen Stellen, bei denen der Berliner Beauftragte für Akteneinsicht und Informationsfreiheit durch Beschwerden oder mit der Bitte um Beratung beteiligt wird, ist erwartungsgemäß hoch. Dies ist nicht so sehr der rigiden Bescheidung der Anträge geschuldet, sondern Unsicherheiten und Anwendungsschwierigkeiten des Gesetzes sowie der Tatsache, dass die bisherige Aktenführung in den Verwaltungen nicht dem Gedanken der Informationsfreiheit Rech-

Die Aktenführung in der Berliner Verwaltung kann sich nicht primär an dem Gedanken der Informationsfreiheit ausrichten. Vielmehr sind Zusammengehörigkeit, Vollständigkeit und Chronologie die entscheidenden Leitlinien der Aktenführung, wie sie auch in der Gemeinsamen Geschäftsordnung für die Berliner Verwaltung – Allgemeiner Teil (GGO I) ihren Niederschlag gefunden haben. Eine etwaige Trennung der Akten in solche, die zur Einsicht freigegeben sind und solche, die Einschränkungen der Informationsfreiheit

[121] ABl. EG Nr. L 145 vom 31. Mai 2001, S. 43

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

nung trägt. Die immer wiederkehrenden Probleme spiegeln sich auch in den Anmerkungen zur Umfrage der Senatsverwaltung für Inneres wider. Teilweise entsprechen sie den im letzten Tätigkeitsbericht angesprochenen. Insbesondere sind die nachfolgenden zu nennen, die zum Teil durch eine erweiterte Kommentierung des Gesetzes, aufbauend auf den Erfahrungen bei der Bearbeitung der Anträge, zu lösen sind, teilweise aber auch Anlass geben, über eine behutsame Novellierung einiger Gesetzesformulierungen durch das Abgeordnetenhaus nachzudenken. Ausdrücklich ist aber festzustellen, dass sich das IFG in seiner jetzigen Form alles in allem bewährt hat.

Bereits der Bericht zum Vorjahreszeitraum ging auf die Schwierigkeiten der Verwaltungen mit § 6 Abs. 1 IFG ein, wonach ein Recht auf Akteneinsicht oder –auskunft, von der personenbezogene Daten betroffen sind, nicht besteht, wenn tatsächliche Anhaltspunkte auf ein *überwiegendes Privatinteresse* des Antragstellers gegeben sind. Diese Formulierung, die als Missbrauchsklausel erst im Endstadium des Gesetzgebungsprozesses eingefügt wurde, verleitet nicht selten dazu, nach Motiven der Antragstellung zu forschen, obwohl das Gesetz eine Begründung des Antrags nicht verlangt. Übersehen wird dabei bisweilen, dass sie sich lediglich auf die Herausgabe personenbezogener Daten bezieht und nur dann zum Tragen kommen kann, wenn tatsächliche Anhaltspunkte auf ein überwiegendes Privatinteresse wie Neid, Rachegelüste oder pures Querulantentum vorliegen.

Das in § 1 IFG geregelte Informationsinteresse ist gegeben, wenn die gewonnenen Erkenntnisse unmittelbar der Allgemeinheit zugänglich gemacht werden, um über die bestehenden Informationsmöglichkeiten hinaus die demokratische Meinungs- und Willensbildung zu fördern und eine Kontrolle staatlichen Handelns zu ermöglichen. Jeder Mensch (bzw. jede juristische Person, § 3 Abs. 1 IFG), der einen Antrag auf Auskunft oder Einsicht in staatliche Unterlagen beantragt, ist Teil dieser Allgemeinheit, der die Informationen zugänglich gemacht werden. Er handelt als „Sachwalter der Allgemeinheit“. Seine individuellen (auch Rechtsschutz-) Interessen an der Auskunft müssen gegenüber denen der Allgemeinheit nicht zurückstehen bzw. sich nicht mit diesen decken. Lebensnah ist vielmehr davon auszugehen, dass viele Anträge auf Akteneinsicht oder -auskunft nach dem IFG auch von der subjektiven Interessen- und Motivationslage des Antragstellers geprägt sind. Insofern können durchaus mehrere Interessenlagen parallel nebeneinander bestehen, ohne dass das Informationsinteresse der Allgemeinheit nach § 1 IFG ausgeschlossen wäre. Das Ziel des IFG, der Öffentlichkeit Zugang zu Informationen über die Hintergründe und Intentionen von Entscheidungen zu gewähren, bezieht sich nicht nur auf übergreifende Sachverhalte, die eine größere Öffentlichkeit betreffen, sondern eben auch auf begrenzte Entscheidungen der Verwaltung, von denen nur wenige betroffen sind. Die Kontrolle staatlichen Handelns als Zweck des IFG umfasst auch diese Vorgänge.

unterliegen, ist weder praktikabel noch rechtlich möglich, da die Gewährung von Akteneinsicht regelmäßig auf einer Einzelfallentscheidung beruht, zum Teil vom Antragsteller abhängig sein kann und darüber hinaus das IFG selbst in einzelnen Paragraphen Abwägungen vorsieht und der Verwaltung einen Ermessensspielraum eröffnet. Vor diesem Hintergrund erscheinen lediglich in begründeten Einzelfällen Änderungen der bisherigen Aktenführung mit Blick auf das IFG sinnvoll.
Nach den ersten Erfahrungen im Umgang mit dem IFG teilt der Senat die Einschätzung, dass das Gesetz in Teilbereichen aus Gründen der Klarstellung und zur besseren Handhabung unter Berücksichtigung der Ergebnisse der landesweiten Umfrage zum IFG novelliert werden sollte. Dabei sind auch die Entscheidungen des Berliner Verwaltungsgerichts bzw. Oberverwaltungsgerichts zum IFG zu berücksichtigen.

Der Senat teilt die Ausführungen des Berliner Beauftragten für Datenschutz und Informationsfreiheit zu dem in § 1 IFG geregelten Informationsinteresse. Dass viele Anträge im Ansatz eher der Verfolgung privater Interessen dienten, hat auch die landesweite Umfrage zum Berliner IFG ergeben.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Der Umfrage der Senatsverwaltung für Inneres ist auch zu entnehmen, dass die Ermittlung der zu erhebenden *Gebühren* den öffentlichen Stellen weiterhin erhebliche Probleme bereitet. Wie die Ausfüllung der Rahmengebührentatbeständen im Einzelfall geschehen soll, ist angesichts der geringen Erfahrungen der einzelnen Verwaltungen unklar. Unserer - bereits im vorigen Jahresbericht erwähnten - Anregung, den Behörden eine Staffel der Gebühren nach Umfang der Akten und Zeitaufwand an die Hand zu geben, ist die Senatsverwaltung für Inneres auch im Berichtszeitraum nicht gefolgt. Wir halten sie aber weiterhin sowohl im Interesse der öffentlichen Stellen als auch der antragstellenden Bürgerinnen und Bürger für sinnvoll. Dabei muss berücksichtigt werden, dass:

- die Obergrenze der Gebühren, die sich auf eine sehr umfangreiche Akteneinsicht (viele Ordner) bezieht, bei 511,29 € liegt. Dementsprechend dürfen die Gebühren für eine Akteneinsicht auch bei einem gewissen Aufwand nicht bereits im oberen Bereich der Rahmengebühren liegen,
- der Europäische Gerichtshof in seinem Urteil vom 9. September 1999[122] festgestellt hat, dass Gebühren für eine Akteneinsicht eine angemessene Höhe nicht überschreiten und nicht prohibitiv sein dürfen,
- das IFG die Teilhabe der Bürger an der demokratischen Meinungs- und Willensbildung unterstützen soll,
- das IFG eine transparente Verwaltung und nachvollziehbare Entscheidungen der Verwaltung fördern soll und
- die Informationserteilung keine klassische Dienstleistung der Verwaltung für den Bürger allein in dessen Interesse ist, sondern Bestandteil einer modernen, transparenten Verwaltung und auch in ihrem Interesse, einer größeren Legitimation durch den Souverän, erfolgt.

Der Senat hat zum Problem der Gebührenberechnung bereits im Rahmen seiner Stellungnahme zum Jahresbericht 2000 des BlnBDI eingehend Stellung genommen und verweist auf die dort gemachten Ausführungen, an denen festgehalten wird. Dabei lautet der zentrale Einwand gegen eine Staffelung, dass der für die Berechnung der Gebühr maßgebliche Verwaltungsaufwand eine Frage des Einzelfalls ist und sich mit Blick auf das IFG nur schwerlich sinnvoll kategorisieren lässt. Wenn überhaupt, so ließe sich der Verwaltungsaufwand wohl am ehesten nach dem erforderlichen Zeitaufwand staffeln, nicht aber nach der vorgeschlagenen Kombination aus Aktenumfang und Zeitaufwand. Denn zum einen ist der Umfang einer Akte als Kriterium kaum aussagekräftig, da Akten mit vergleichsweise geringer Seitenzahl einer Vielzahl begründungspflichtiger Einschränkungen des Informationsrechts nach den §§ 6 ff. IFG unterliegen und eingehende Prüfungen nach sich ziehen können, während andere umfangreichere Akten problemlos offengelegt werden können. Zum anderen schlägt sich die Notwendigkeit der Durchsicht umfangreicher Akten ja gerade im Zeitaufwand nieder, so dass nicht ersichtlich ist, wie die beiden Kategorien sinnvoll kombiniert werden könnten. Schon an diesen Beispielen wird deutlich, welche Probleme eine Kategorisierung mit sich bringt.

Das Kriterium des Zeitaufwandes kann zudem – einzelfallgerechter als jede Staffelung – bereits auf der Grundlage des geltenden Gebührenrechts der Berechnung der Gebühr zu Grunde gelegt werden. Der Senat weist darauf hin, dass sich der Gesetzgeber mit der Regelung des § 16 Satz 2 IFG bewusst für eine Anwendung der gebührenrechtlichen Regelungen entschieden hat. Das aufgeworfene Problem ist daher schwerpunktmäßig gebührenrechtlicher Art. Denn für Rahmengebühren gilt insbesondere § 5 der Verwaltungsgebührenordnung (VGebO) und das der Vorschrift des § 5 Nr. 2 VGebO zugrundeliegende Kostendeckungsprinzip. Auch § 8 Abs. 2 des Gesetzes über Gebühren und Beiträge (GebG) gebietet bei der Festsetzung von Verwaltungsgebühren die Berücksichtigung der Kosten des Verwaltungszweiges. Freilich ist im Einzelfall das gebührenrechtliche Äquivalenzprinzip zu beachten, welches besagt, dass die Gebühren in keinem Missverhältnis zu der von der öffentlichen Verwaltung gebotenen Leistung stehen dürfen. Die Intention des IFG, die Teilhabe der Bürger an der demokratischen Meinungs- und Willensbildung zu unterstützen, entbindet jedoch nicht von der Beachtung der bestehenden gebührenrechtlichen Regelungen, zumal der Gesetzgeber – wie bereits betont – bewusst auf das Gebührenrecht verwiesen hat.

Schwierigkeiten bereitet das Verhältnis der Informationsansprüche nach dem IFG zu in anderen Gesetzen geregelten Auskunfts- und Einsichtsansprüchen. Insbesondere sehen sich die Anwender mit der Frage konfrontiert, wie sich die weitergehenden Rechte auf die

Auch nach Auffassung des Senats kann das Verhältnis von Informationsansprüchen nach dem IFG zu sonstigen gesetzlich geregelten Auskunfts- und Einsichtsansprüchen im Einzelfall erhebliche Probleme bereiten. Diese Probleme sind bei der beabsichtigten Novellie-

[122] Az.: C 217/97

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

begrenzten Ansprüche anderer Gesetze, die in der Regel an die Betroffenheit des Antragstellers oder seine Beteiligung an einem Verwaltungsverfahren anknüpfen, auswirken. Derartige Konkurrenzfragen führen allerdings nicht nur im Informationsfreiheitsrecht zu Problemen, sondern sind auch in vielen anderen Rechtsgebieten – nicht zuletzt im Datenschutzrecht – Anlass zu juristischen Auseinandersetzungen. Die naheliegendsten Gesetzeskonkurrenzen können aber wie folgt gelöst werden:

Informationsansprüche des IFG treten hinter denen aus Spezialgesetzen für Betroffene, Beteiligte oder Dritte, soweit diese speziellen Vorschriften weitergehen (§ 3 Abs. 3 IFG) oder dem Anspruch aus dem IFG entsprechen, zurück. Hier greift der Spezialitätsgrundsatz. Dieser Vorrang ist für den Antragsteller auch unschädlich, da es sich regelmäßig um die günstigere Anspruchsgrundlage handelt, bei der meist keine Gebührenpflicht besteht.

Ausdrücklich festgestellt ist in § 2 Abs. 2 IFG der ausschließliche Vorrang des UIG bei Umweltinformationen. Für diese ist die Anwendung des IFG ausgeschlossen.

rung des IFG soweit als möglich durch gesetzliche Klarstellungen zu beseitigen.

§ 3 Abs. 3 ist nicht so zu verstehen, dass das IFG generell einen Mindeststandard für alle Informationsansprüche auch aus anderen Gesetzen setzt. Gleichwohl ist der Wille des Berliner Gesetzgebers, den Bürgerinnen und Bürgern einen umfassenden Informationszugang zu ermöglichen, bei der Ermittlung des Anspruchs auf Information und seiner Grenzen nach anderen Rechtsnormen zu berücksichtigen. Sehen andere Gesetze Aktenauskunfts- oder Akteneinsichtsrechte vor, die hinter denen des IFG zurückbleiben, so ist zu unterscheiden:

Die angeführten Beispiele zeigen eindringlich, wie schwierig im Einzelfall die auftretenden Konkurrenzfragen sein können. Richtig dürfte der Ansatz sein, dass das IFG nicht für Akten gilt, für die Einsichts- oder Auskunftsregelungen unabhängig vom Beteiligtenstatus bestehen. Hingegen ist in jenen Fällen, in denen ein Spezialgesetz lediglich die Einsichtnahme durch Verfahrensbeteiligte regelt, im Einzelfall zu prüfen, ob die getroffene Regelung abschließend ist und die subsidiäre Anwendbarkeit des IFG ausschließt oder nicht.

Informationsansprüche aus *Bundesgesetzen* sind in der Regel abschließend und können durch weitergehende Ansprüche aus dem IFG nicht verdrängt, wohl auch nicht ohne weiteres ergänzt werden, da der Bundesgesetzgeber in der jeweiligen Materie von seiner Gesetzgebungskompetenz Gebrauch gemacht hat. Gleichwohl ist zu prüfen, ob sie weitergehende Ansprüche nach dem IFG oder eine Sperrwirkung für landesgesetzliche Regelungen in der konkreten Materie darstellt. So ist in den Fällen, in denen Landesbehörden Bundesrecht ausführen, jedenfalls dann von der Geltung des IFG auszugehen, wenn es nicht um den materiellen Inhalt von Verwaltungsentscheidungen, sondern um die Ausgestaltung des Verwaltungsverfahrens geht, für die das Land zuständig ist.

§ 34 FGG regelt die Einsicht in Gerichtsakten für jeden, wenn er ein berechtigtes Interesse glaubhaft macht. Diese Vorschrift ist – unabhängig von § 2 Abs. 1 Satz 2 IFG – abschließend.

Das SGB X regelt die öffentlich-rechtliche Verwaltungstätigkeit der Behörden nach dem SGB (§ 1 SGB X). In § 25 trifft es Aussagen zur Akteneinsicht durch Beteiligte, welche an die Geltendmachung oder Verteidigung ihrer rechtlichen Interessen gebunden ist. Über

eine Akteneinsicht von Unbeteiligten (ggf. in anonymisierter Form) macht es keine Aussage. Dies schließt zwar eine Einsicht in die Sozialakten selbst aus. Unterlagen zur Organisation der Berliner Sozialverwaltung sind dagegen sehr wohl zugänglich zu machen.

Informationsansprüche aus dem IFG bestehen in der Regel auch für die Materien, in denen andere *Gesetze des Landes Berlin* bereits begrenzt Akteneinsichts- und -auskunftsrechte vorsehen – zumeist Rechte der Betroffenen oder Beteiligten eines Verfahrens oder einer Datenverarbeitung. Für das Verwaltungsverfahren stellt dies § 4 a Abs. 4 Berliner Verwaltungsverfahrensgesetz (VwVfGBln) bereits ausdrücklich fest, ebenso § 4 Abs. 5 Pressegesetz für die Medien. Die Informationsansprüche spezieller Gesetze begrenzen die nach dem IFG nicht, soweit nicht tatsächlich der Spezialitätsgrundsatz betroffen ist. Da sich Spezialgesetze hinsichtlich der Akteneinsichts- und Aktenauskunftsrechte auf bestimmte Personengruppen, nämlich Beteiligte, Betroffene, Berufs- und Amtsgruppen, beziehen, bleibt hier Raum für das jedermann zustehende Informationsrecht des IFG, freilich mit den Einschränkungen der §§ 6–12 IFG. Der begrenzte Informationsanspruch von Angehörigen dieser Personengruppen kann nach Maßgabe des IFG durch die jedermann zustehenden Rechte des IFG ergänzt werden, dann allerdings auch nach den Maßstäben des IFG.

Sehen spezialgesetzliche Regelungen für bestimmte Personengruppen (Beteiligte, Betroffene etc.) einen begrenzten Informationsanspruch vor, so muss im Einzelfall geprüft werden, ob diese Grenzen auch für einen Anspruch aus dem IFG bindend sind, weil ein umfassender Informationsanspruch dem Schutzzweck des Spezialgesetzes zuwiderlaufen würde.

Nicht jeder Antragsteller kann sich auf § 13 Abs. 5 Satz 1 IFG berufen. So hat ein Nicht-Verfahrensbeteiligter keinen Anspruch auf Herausgabe von Kopien von Prüfungsfragen einer Prüfungseinrichtung. Sein Anspruch kann hier nicht weiter gehen als der des Prüflings. Die Vorschrift schützt nämlich die Wiederverwertbarkeit der Prüfungsfragen.

Akteneinsicht zur Prozessführung

Die Komplexität und Vielschichtigkeit des IFG und die Konsequenzen für die Verwaltung seien an einem Beispiel dargestellt, bei welchem wir um eine rechtliche Bewertung gebeten wurden.

In einer vor dem Kammergericht anhängigen Schadensersatzklage einer GmbH, die als treuhänderischer Entwicklungsträger des Landes Berlin fungiert, gegen eine von ihr mit der Erstellung eines Wertgutachtens beauftragte Firma haben die Anwälte der Beklagten und Berufungsklägerin Akteneinsicht bei der Senatsverwaltung für Stadtentwicklung beantragt. Eine Abteilung der Senatsverwaltung hatte die Plausibilitätsprüfung des von der Beklagten erstellten Gutachtens durchgeführt. Durch die Akteneinsicht erhofft sich die Beklagte eine Verbesserung ihrer Position im Berufungsverfahren.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Die in diesem Zusammenhang auftretenden Probleme betrafen die Anwendung des IFG im laufenden Gerichtsverfahren, warfen aber auch wiederum die Frage auf, ob die hier offensichtlich gegebenen Privatinteressen an der begehrten Information einem Einsichts- oder Auskunftsanspruch nach dem IFG entgegenstehen. Unsere Prüfung kam zu dem Schluss, dass das IFG auch in Fällen wie diesem einen Einsichts- oder Auskunftsanspruch gewährt. § 2 Abs. 1 Satz 1 IFG regelt die Informationsrechte gegenüber den Behörden und sonstigen öffentlichen Stellen des Landes Berlin und unterscheidet dabei nicht zwischen privatrechtlicher und öffentlich-rechtlicher Tätigkeit der öffentlichen Stelle. Es trifft auch keine Aussage darüber, dass das Gesetz etwa im Fall einer anhängigen Klage nicht anwendbar sein soll. Danach musste das IFG auch hier umfassend gelten, so dass die bei der Behörde vorhandenen Unterlagen dem Informationszugang unterlagen. Dies betraf jedenfalls diejenigen Unterlagen, die auch vor Klageerhebung vorhanden waren und für einen Informationszugang in Betracht gekommen wären.

Hätte es sich dagegen um Unterlagen gehandelt, die erst nach Klageerhebung im Hinblick auf den Prozess entstanden sind – etwa um solche, aus denen sich eine bestimmte Prozessstrategie für das Land Berlin ergibt und die deshalb nicht in den Prozess eingebracht werden -, so wäre ein Informationsanspruch nicht auf das IFG zu gründen gewesen. Der Ausschluss des Informationszuganges bei derartigem Aktenmaterial ergibt sich aus § 9 Abs. 1 Satz 1 l. Fall IFG. Danach besteht das Recht auf Akteneinsicht oder Aktenauskunft nicht, soweit und solange ein vorzeitiges Bekanntwerden des Akteninhaltes nach der besonderen Art der Verwaltungstätigkeit mit einer ordnungsgemäßen Aufgabenerfüllung unvereinbar ist. Die Vorbereitung und Begleitung eines Zivilprozesses durch Bedienstete oder Vertreter des Landes Berlin stellen eine Verwaltungstätigkeit dar, auch wenn das Land Berlin im Zivilprozess selbst die Rechtsstellung eines Privaten hat. Die Offenbarung dieser Tätigkeit durch Offenlegung des nach Klageerhebung angelegten Aktenmaterials, aus dem auch prozesstaktische Erwägungen hervorgehen können, ist unvereinbar mit der ordnungsgemäßen Aufgabenerfüllung, nämlich mit der möglichst erfolgreichen Führung des Zivilprozesses.

Zu diesem Ergebnis, das auf den Zeitpunkt und den Zweck der Entstehung der Unterlagen abstellt, muss man auch deshalb kommen, da dem Bürger nach Klageerhebung die auch vorher nach IFG bestehenden Rechte erhalten bleiben müssen. Würde man demgegenüber die Auffassung vertreten, dass nach Klageerhebung sämtliche zu der streitigen Angelegenheit existierenden Unterlagen unzugänglich sind, hieße dies, dass sich der Antragsteller - wenn er selbst Klage einreicht – in eine schlechtere Rechtsposition versetzt, als er sie vor Klageerhebung innehatte. Dann aber wäre ihm zu raten, jedes Mal vor Beschreiten des (Zivil-)Rechtsweges gegen das Land Berlin zunächst die Rechte nach dem IFG auszuschöpfen.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

5. Telekommunikation und Medien

Die Terroranschläge des 11. September 2001 haben im Bereich der Telekommunikation zu einer Vielzahl von gesetzgeberischen Initiativen auf nationaler und internationaler Ebene geführt, mit denen die Überwachungsbefugnisse der Strafverfolgungsbehörden und der Geheimdienste erweitert werden sollen.

So enthält das Terrorismusbekämpfungsgesetz eine Verpflichtung der Anbieter von Telekommunikationsdienstleistungen, Auskünfte über Verbindungsdaten zukünftig auch an das Bundesamt für Verfassungsschutz und die anderen Nachrichtendienste des Bundes zu erteilen (§ 8 Abs. 8 BVerfschG, § 10 Abs. 3 MAD-G, § 8 Abs. 3a BND-G).

Einzelne Bundesländer haben im Bundesrat darüber hinaus die Forderung erhoben, die Anbieter von Telekommunikationsdienstleistungen dazu zu verpflichten, Verbindungsdaten über Telekommunikationsvorgänge – unabhängig davon, ob dies für die Abrechnung mit dem Nutzer erforderlich ist, für einen Zeitraum von mindestens sechs Monaten für Zwecke der Strafverfolgung zu speichern.

Solche Mindestspeicherungsfristen existieren bereits jetzt in Großbritannien und Frankreich. Auch auf der Ebene der Europäischen Union gibt es Bestrebungen, den nach wie vor nicht verabschiedeten Vorschlag für eine Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, der die Telekommunikations-Datenschutzrichtlinie 97/66/EG ersetzen soll[123], um eine entsprechende Öffnungsklausel zu ergänzen, die den Mitgliedstaaten die Schaffung solcher Speicherungsverpflichtungen ermöglicht.

Sollten sich diese Vorschläge durchsetzen, wäre damit ein Paradigmenwechsel verbunden: Bisher erlauben die einschlägigen Rechtsvorschriften lediglich den Zugriff auf solche Verbindungsdaten, die bei Anbietern von Telekommunikationsdienstleistungen ohnehin für die Abrechnung von Dienstleistungen mit ihren Kunden gespeichert sind. Zukünftig würden hingegen die Telekommunikationsnetze und – soweit die dort angebotenen Dienste in die Überwachungsmaßnahmen mit einbezogen werden – auch das Internet implizit zu einem Fahndungsnetz umgestaltet werden, bei dem sich der Umfang der Speicherung von Verbindungsdaten ausschließlich an den Bedürfnissen der Strafverfolgungsbehörden und der Geheimdienste orientiert. Solchen Bestrebungen waren die Datenschutzbeauftragten in der Vergangenheit entschieden entgegengetreten[124].

[123] JB 2000, 5.1

[124] Pressemitteilung des Hamburgischen Datenschutzbeauftragten vom 30. November 2000: Das Internet ist kein datenschutzfreies Fahndungsnetz. Datenschutzbeauftragte lehnen Forderungen der Innenministerkonferenz ab; Entschließung der Europäischen Datenschutzkonferenz vom 10./11. Mai 2001 in Athen zu „Retention of Traffic Data by Internet Service Providers (ISPs)

Diese Entwicklung ist umso bedauerlicher, als es bisher in der Bundesrepublik kaum empirische Untersuchungen darüber gibt, inwieweit diese erheblichen Eingriffe in das Fernmeldegeheimnis aller Nutzer von Telekommunikationsdiensten durch entsprechende Fahndungserfolge bei der Bekämpfung von Straftaten zu rechtfertigen sind. Das bereits im letzten Jahr durch das Bundesministerium der Justiz in Auftrag gegebene Gutachten zu „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO“ war zum Ende des Berichtzeitraums noch nicht abgeschlossen. Ergebnisse dieses Gutachtens sollen nach Angaben des Max-Planck-Instituts für ausländisches und internationales Strafrecht in Freiburg im Breisgau Mitte des Jahres 2002 vorliegen.

5.1 Telekommunikationsnetze und -dienste

Übereinkommen über Datennetzkriminalität des Europarates

Über den Entwurf für ein Übereinkommen über Datennetzkriminalität des Europarates hatten wir bereits in unserem Jahresbericht 2000 berichtet. Auch im zurückliegenden Berichtszeitraum hatten sich die Datenschutzbeauftragten wiederum mit dem Übereinkommen zu beschäftigen. Im Rahmen des Übereinkommens, das am 23. November 2001 in Budapest von 26 Mitgliedern des Europarates und 4 weiteren Ländern unterzeichnet worden ist, ist die Einführung verschiedener neuer Straftatbestände geplant, die bisher in den Strafgesetzen vieler Mitgliedstaaten des Europarates nicht enthalten sind. Gleichzeitig werden Verfahren zur Verfolgung dieser Straftaten festgelegt, darunter ebenfalls Maßnahmen zur Verpflichtung von Telekommunikationsanbietern, personenbezogene Daten über Kommunikationsvorgänge in Telekommunikationsnetzen (sowohl Inhalts- als auch Verkehrsdaten) zu speichern und diese Daten nationalen und ausländischen Behörden zur Verfügung zu stellen, die entsprechende Ermittlungen in dem betreffenden Strafverfahren durchführen. Das Übereinkommen wird in Kraft treten, sobald seine Ratifikation durch fünf Staaten – darunter wenigstens drei Mitgliedsländer des Europarates – erfolgt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte in einer Entschließung im März 2001[125] unter anderem die Bundesregierung aufgefordert, sich bei der Schaffung von nationalen und internationalen Regelungen zur Bekämpfung von Datennetzkriminalität dafür einzusetzen, dass Maßnahmen zur Identifikation von Internet-Nutzern, zur Registrierung des Nutzungsverhaltens und Übermittlung der dabei gewonnen Daten für Zwecke der Strafverfolgung erst dann erfolgen dürfen, wenn ein konkreter Verdacht besteht. Datenschutz und Fernmeldegeheimnis müssen gewährleistet und Grundrechtseingriffe auf das unabdingbare Maß begrenzt, der Zugriff und die Nutzung personenbezogener Daten einer strikten und eindeuti-

[125] vgl. Anlagenband, a.a.O., I.1

gen Zweckbindung unterworfen werden. Schließlich sollen Daten von Internet-Nutzern nur in Länder übermittelt werden dürfen, in denen ein angemessenes Niveau des Datenschutzes, des Fernmeldegeheimnisses und der Informationsfreiheit gewährleistet ist und wo verfahrensmäßige Garantien bei entsprechenden Eingriffen bestehen.

Auch die Art. 29-Datenschutzgruppe hat im März 2001 eine umfangreiche Stellungnahme zum Entwurf des Übereinkommens zur Datennetzkriminalität angenommen[126].

Auch wenn die jetzt verabschiedete Fassung gegenüber den vorher veröffentlichten Vorentwürfen einige marginale datenschutzrechtliche Verbesserungen aufweist, berücksichtigt die Konvention nach wie vor einseitig die Interessen der Strafverfolgungsbehörden. Zu kritisieren ist insbesondere, dass bei den Maßnahmen zur Gewährleistung der Netzsicherheit nach wie vor repressiven Maßnahmen gegenüber den Nutzern der Vorzug gegeben wird, anstatt den Betreibern der entsprechenden Infrastruktur-Einrichtungen aufzugeben, für einen besseren Schutz ihrer Anlagen und Übertragungsnetze zu sorgen.

Auch die Kommission der Europäischen Gemeinschaften beschäftigt sich mit dem Problem der Computerkriminalität[127]. Anders als in der Europaratskonvention ist in dem Papier der Kommission ein Interesse erkennbar, für einen angemessenen Ausgleich zwischen den Bedürfnissen der Strafverfolgungsbehörden einerseits und dem Recht auf informationelle Selbstbestimmung der Nutzer von elektronischen Medien andererseits zu sorgen: So betont die Kommission, dass zur Schaffung einer sicheren Informationsgesellschaft in erster Linie die Sicherheit der Informationsinfrastruktur verbessert werden muss, wobei gleichzeitig anonyme und pseudonyme Nutzungsmöglichkeiten für die angebotenen Dienste erhalten bleiben müssen. Gleichzeitig wird angeregt, über Fragen der Bekämpfung der Datennetzkriminalität einen offenen Diskussionsprozess unter Einbeziehung von Diensteanbietern, Bürgerrechtsorganisationen, Verbraucherverbänden und Datenschutzbeauftragten zu führen[128].

Telekommunikations-Überwachungsverordnung

Die langjährigen Bemühungen nunmehr zweier Bundesregierungen, eine Nachfolgevorschrift für die Fernmeldeüberwachungsverordnung zu erstellen, haben im zurückliegenden Jahr ihren Abschluss gefunden: Am 29. Januar 2002 ist die Telekommunikations-Überwachungsverordnung (TKÜV) in Kraft getreten[129]. Die verschiedenen öffentlich bekannt geworde-

[126] Stellungnahme 4/2001 zum Entwurf einer Konvention des Europarates über Cyberkriminalität; WP 41; 5001/01/DE/endg
[127] Mitteilung der Kommission zur Schaffung einer sicheren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität vom 26. Januar 2001, KOM (2000) 890 endg.
[128] vgl. hierzu auch die Stellungnahme der Art. 29-Datenschutzgruppe zur Mitteilung der Kommission über die „Schaffung einer sicheren Informationsgesellschaft durch Verbesserung der Sicherheit der Informationsinfrastrukturen und Bekämpfung der Computerkriminalität“ vom 5. November 2001; WP 51; 5074/01DE/endg
[129] BGBl. I, S. 458

nen Entwurfsfassungen[130] waren bis zum Schluss Gegenstand einer ebenso engagiert wie kontrovers geführten Debatte zwischen dem Bundeswirtschaftsministerium, den Datenschutzbeauftragten, den Anbietern von Telekommunikations- und Internetdienstleistungen und anderen gesellschaftlichen Gruppen. Heiß umstritten war insbesondere bis zuletzt, welche Anbieter von Telekommunikations- und Internetdienstleistungen vom Anwendungsbereich der Verordnung umfasst bzw. ausgenommen werden sollen.

Die Verordnung enthält selbst keine materiellen Befugnisse für die Sicherheitsbehörden für die Telekommunikationsüberwachung; diese Befugnisse sind vielmehr abschließend in der Strafprozessordnung (§§ 100 a, 100 b), dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Art. 10-Gesetz – G10 –) und dem Außenwirtschaftsgesetz (§§ 39–43) geregelt. Dort ist abschließend festgelegt, bei welchen Straftaten eine Überwachung der Telekommunikation überhaupt angeordnet werden kann. Die Rechtsvorschriften verpflichten Anbieter, die geschäftsmäßig Telekommunikationsdienstleistungen erbringen oder daran mitwirken.

Die TKÜV legt dagegen fest, welche Arten von technischen und organisatorischen Vorkehrungen bestimmte Betreiber von Telekommunikationsnetzen und Anbieter von Telekommunikations- und Internetdienstleistungen treffen müssen, um die technische Umsetzung von Überwachungsmaßnahmen zu ermöglichen.

Die der TKÜV zugrunde liegende Verordnungsermächtigung aus § 88 des Telekommunikationsgesetzes (TKG) fasst den Kreis der Verpflichteten sehr weit: Nach § 88 Abs. 4 TKG ist jeder Betreiber einer Telekommunikationsanlage, der anderen den Netzzugang zu seiner Telekommunikationsanlage geschäftsmäßig überlässt, verpflichtet, den gesetzlich zur Überwachung der Telekommunikation berechtigten Stellen auf Anforderung einen Netzzugang für die Übertragung der im Rahmen einer Überwachungsmaßnahme anfallenden Informationen bereitzustellen.

Die TKÜV selbst schränkt den Kreis der Anbieter, die zur ständigen Vorhaltung technischer Einrichtungen zur Umsetzung der gesetzlich vorgesehenen Maßnahmen zur Überwachung der Telekommunikation und zu vorbereitenden organisatorischen Vorkehrungen für die Umsetzung solcher Maßnahmen verpflichtet sind, auf Betreiber von Telekommunikationsanlagen ein, die Telekommunikationsdienstleistungen für die Öffentlichkeit anbieten. Damit werden die Betreiber von „nicht-öffentlichen“ Telekommunikationsanlagen – insbesondere von Telefonnebenstellenanlagen, unternehmensinternen Telekommunikationsanlagen und „corporate networks“ – von der Verpflichtung zur Vorhaltung technischer Einrichtungen und zu organisatorischen Vorkehrungen freigestellt. Dies gilt auch für Betreiber von Verbindungsnetzen, zu denen der Teilnehmer keinen direkten Zugang hat, Internet-

[130] vgl. zuletzt JB 1999, 5.1

Access-Provider und Betreiber von Telekommunikationsanlagen, die aus Übertragungswegen gebildet werden, die nicht dem unmittelbaren teilnehmerbezogenen Zugang zum Internet dienen. Einbezogen in den Kreis der Verpflichteten sind dagegen Übertragungswege im Internet, mit denen einem Teilnehmer unter Umgehung der Vermittlungsfunktion eines Zugangsnetzes der unmittelbare Zugang zum Internet eröffnet wird. Die Begründung führt hierzu insbesondere Anbieter von DSL-Anschlüssen auf[131]. Ausgenommen sind auch Betreiber von Telekommunikationsanlagen, die der Verteilung von Rundfunk oder anderen für die Öffentlichkeit bestimmten Informationen oder dem Abruf von allgemein zugänglichen Informationen dienen (dies betrifft z. B. Telekommunikationsanlagen von Content-Providern), sowie von Telekommunikationsanlagen, die der Übermittlung von Messwerten oder nicht individualisierten Daten, wie z. B. Verkehrsmessanlagen oder von Notrufen oder „Informationen für die Sicherheit und Leichtigkeit des See- oder Luftverkehrs“, dienen (§ 2 Abs. 2 Nr. 4 TKÜV); ferner kleine Telekommunikationsanlagen, an die nicht mehr als 1.000 Teilnehmer angeschlossen sind.

Erleichterungen in Bezug auf Zeiträume, innerhalb derer die Daten den Behörden zur Verfügung gestellt werden müssen, sowie hinsichtlich der Ausgestaltung des technischen Verfahrens sind darüber hinaus auf Antrag für Betreiber kleiner Telekommunikationsanlagen, an die nicht mehr als 10.000 Teilnehmer angeschlossen sind, möglich (vgl. § 21 TKÜV).

Im Vorfeld der Verabschiedung der TKÜV war insbesondere umstritten, inwieweit Anbieter von Internetdienstleistungen in den Anwendungsbereich der TKÜV mit einbezogen werden sollen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in einer Entschließung unter anderem entschieden dagegen gewandt, mit der TKÜV eine technische Infrastruktur zu schaffen, die jederzeit eine umfassende Überwachung des Internet-Verkehrs möglich macht[132]. Es ist daher zu begrüßen, dass zumindest Internet-Access-Provider (allerdings mit Ausnahme der DSL-Anschlüsse) und Inhalteanbieter ausdrücklich vom Geltungsbereich der Verordnung ausgenommen worden sind. Dagegen sind Anbieter von E-Mail-Diensten für ihre Mail-Server in den Anwendungsbereich der Verordnung einbezogen. Dies betrifft allerdings nur Einrichtungen, die den Endteilnehmern einen direkten Zugriff ermöglichen (also die SMTP- und POP3-Server eines Anbieters, bei dem ein bestimmter Nutzer eine E-Mail-Adresse registriert hat), nicht aber Server, die nur als Vermittlungsknoten bei der Zustellung solcher Nachrichten dienen.

Angesichts der vielfältigen im Internet bestehenden Umgehungsmöglichkeiten (als Beispiel sei hier nur die Registrierung einer E-Mail-Adresse bei einem ausländischen Anbieter genannt) sind jedoch Zweifel ange-

[131] vgl. die Begründung zu § 2 Abs. 2 Satz 2 unter Nr. 3

[132] Entschließung zu „Entwurf der Telekommunikations-Überwachungsverordnung“. In: Anlagenband, a.a.O., I.1

bracht, ob die Verpflichtung dieser Anbieter durch die TKÜV auch im Hinblick auf die damit für die Anbieter solcher Dienste entstehenden, erheblichen Kosten dem Grundsatz der Verhältnismäßigkeit genügt.

Anzuerkennen ist der Versuch des Verordnungsgebers, die in der Verordnungsermächtigung des § 88 TKG wesentlich zu weit gefasste Ermächtigung in der Verordnung selbst – wenngleich durch ein sehr komplexes System verschiedener Rückausnahmen und einzelner Erleichterungen – auf ein einigermaßen vernünftiges Maß zu begrenzen. Gleichwohl sollte die vom Bundeswirtschaftsministerium angekündigte Novellierung des TKG in der nächsten Legislaturperiode dazu genutzt werden, die überschießende Verordnungsermächtigung bereits im Gesetz selbst entsprechend einzuschränken. Aber auch die jetzt in der TKÜV festgelegten Verpflichtungen sollten in absehbarer Zeit im Lichte der Ergebnisse der Untersuchung über die Effektivität von Telekommunikations-Überwachungsmaßnahmen[133] im Rahmen einer Evaluation auf den Prüfstand gestellt werden.

Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten

Mit einem Gesetz zur Änderung der Strafprozessordnung[134] wurden die Bestimmungen des § 12 Fernmeldeanlagengesetz (FAG), der bisher den Zugriff der Strafverfolgungsbehörden auf bei Anbietern von Telekommunikationsdienstleistungen gespeicherte Verbindungsdaten regelt, ersetzt. § 12 FAG trat zum 31. Dezember 2001 außer Kraft, so dass die Schaffung einer neuen Rechtsvorschrift erforderlich war, wenn die bisher im Fernmeldeanlagengesetz enthaltenen Befugnisse für die Strafverfolgungsbehörden nicht ersatzlos entfallen sollten.

Die Datenschutzbeauftragten hatten in der Vergangenheit mehrfach die bisher in § 12 FAG enthaltenen Eingriffsbefugnisse für die Strafverfolgungsbehörden als zu weitgehend kritisiert und die Ersetzung der Vorschrift durch eine verfassungskonforme Bestimmung im Rahmen der Strafprozessordnung gefordert[135]. Das neue Gesetz enthält datenschutzrechtlich positive Ansätze: So wird die Anordnungsbefugnis zukünftig auf Straftaten von erheblicher Bedeutung, insbesondere auf die in § 100 a Satz 1 StPO genannten Straftaten beschränkt.

Gleichzeitig ist jedoch eine Anordnungsbefugnis für beliebige weitere Straftaten vorgesehen, die mittels einer Endeinrichtung begangen werden (§ 100 g Abs. 1 Satz 1 StPO). Abweichend von der bisherigen Rechtslage kann die Auskunft jetzt in beiden Fällen auch über zukünftige Telekommunikationsverbindungen angeordnet werden.

Wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten auf

[133] vgl. Einleitung zu 5.
[134] BGBl. I, S. 3879
[135] JB 1999, 5.1

andere Weise aussichtslos oder wesentlich erschwert wäre, darf zusätzlich auch die Erteilung einer Auskunft darüber angeordnet werden, ob von einem Telekommunikationsanschluss Telekommunikationsverbindungen zu den Beschuldigten hergestellt worden sind (§ 100 g Abs. 2 StPO).

Eine Verpflichtung zur Speicherung von Verbindungsdaten nur für Zwecke der Strafverfolgung, wie sie § 100 a StPO ermöglicht, ist mit der Regelung ausdrücklich nicht verbunden. Auch Auskünfte über Aktivmeldungen von Mobiltelefonen im „stand by"-Betrieb werden durch die Vorschrift (noch) nicht ermöglicht.

In der Gesetzesbegründung wird darauf abgestellt, dass sowohl die IMEI (International Mobile Equipment Identification)-Nummer von Mobiltelefonen als auch die im Internet verwendeten IP-Adressen durch den Begriff „Kennung" in § 100 g Abs. 3 StPO erfasst werden sollen. Dies ist jedoch nicht der Fall, da die IMEI-Nummer von den Betreibern weder zu Nutzungsnoch zu Abrechnungszwecken benötigt wird und ihre Speicherung als Verbindungsdatum daher gemäß § 89 Abs. 2 TKG unzulässig wäre. Wenn die IMEI-Nummer tatsächlich unter den Begriff der „Kennung" in § 100 g Abs. 3 Nr. 1 des Entwurfs fallen soll, wäre dies eine Verarbeitung allein für Zwecke der Strafverfolgung, die jedoch ausdrücklich nicht beabsichtigt ist. Bei IP-Adressen, die von Internet-Nutzern verwendet werden, handelt es sich überdies im Regelfall nicht um Bestandsdaten der Telekommunikation. Vielmehr sind feste „statische" IP-Adressen, die von Teledienstean-bietern vergeben und gespeichert werden, als Bestandsdaten des jeweiligen Teledienstes anzusehen. Bei den vielfach üblichen „dynamisch" zugewiesenen IP-Adressen handelt es sich weder um Bestandsdaten der Telekommunikation noch um solche der Teledienste, sondern um Verbindungs- beziehungsweise Nutzungsdaten des Teledienstes. Soweit IP-Adressen durch Telekommunikationsdienste (z. B. im ISDN) übertragen werden, handelt es sich dabei um Inhalte der Telekommunikation, die nur unter den Voraussetzungen der §§ 100 a, 100 b StPO überwacht werden dürfen.

Aufenthaltsinformationen in mobilen Kommunikationsdiensten (Location based services)

Aufenthaltsinformationen werden in den Mobilfunknetzen bereits seit deren Bestehen verarbeitet. In der Vergangenheit wurden diese Informationen nur zum Aufbau einer Verbindung zu dem mobilen Endgerät generiert und genutzt; daher verfügten nur die Anbieter von Telekommunikationsnetzen über solche Aufenthaltsinformationen, die in den meisten Ländern umfassend zur Wahrung des Fernmeldegeheimnisses verpflichtet sind.

Während sich bisher die Genauigkeit der Ortung nach der Größe der betreffenden Funkzelle in dem zellularen Netzwerk richtete, haben die Betreiber von Netzwerken jetzt damit begonnen, die technische Infrastruktur ihrer Netzwerke so zu verändern, dass in naher Zukunft

wesentlich genauere Informationen über den Aufenthaltsort eines jeden mobilen Endgerätes verfügbar sein werden. Die Entwicklung des mobilen elektronischen Geschäftsverkehrs wird gleichzeitig zur Einführung einer Vielzahl von neuen Diensten führen, die auf der Kenntnis des präzisen Aufenthaltsortes der Nutzer basieren. Damit werden Aufenthaltsinformationen auch für solche Anbieter verfügbar, die nicht an die gesetzlichen Beschränkungen des Fernmeldegeheimnisses unmittelbar gebunden sind.

Die verbesserte Genauigkeit von Aufenthaltsinformationen und ihre Verfügbarkeit nicht nur für die Betreiber mobiler Telekommunikationsnetze kann zu neuen Risiken für die Privatsphäre von Nutzern mobiler Endgeräte führen.

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation hat auf ihrer 29. Sitzung am 15./16. Februar 2001 einen gemeinsamen Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten gefasst, in dem Forderungen hinsichtlich der datenschutzgerechten Gestaltung solcher Dienstleistungen erhoben werden[136]. Darin hat die Arbeitsgruppe u. a. gefordert, den Entwurf und die Auswahl technischer Einrichtungen solcher Dienste an dem Ziel zu orientieren, entweder überhaupt keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen. Grundsätzlich sollten präzise Aufenthaltsinformationen nicht als ein Standard-Leistungsmerkmal eines Dienstes generiert werden, sondern nur „nach Bedarf“, soweit es für einen bestimmten Dienst erforderlich ist, der an den Aufenthaltsort des Nutzers geknüpft ist. Der Nutzer muss gleichzeitig die volle Kontrolle darüber behalten, ob präzise Aufenthaltsinformationen im Netz entstehen. Nutzer sollten die Möglichkeit haben, die präzise Aufenthaltsbestimmung jederzeit abschalten zu können.

Aufzeichnung von Verbindungsdaten in der Berliner Verwaltung

Bereits in unserem letzten Jahresbericht hatten wir darauf hingewiesen, dass bei der Verarbeitung personenbezogener Daten auf Telekommunikationsanlagen im Land Berlin die Regelungen des § 5 Informationsverarbeitungsgesetz (IVG) einzuhalten sind[137]. Insbesondere müssen Dienst- und Privatgespräche getrennt werden; darüber hinaus dürfen Dienstgespräche im Regelfall nicht apparate- bzw. mitarbeiterbezogen gespeichert, sondern müssen Gruppen von in der Regel nicht weniger als zehn Beschäftigten zugeordnet werden.

In den vom Landesbetrieb für Informationstechnik (LIT) betreuten TK-Anlagen sind keine Gebührenerfassungssysteme für mitarbeiterbezogene Gesprächsdaten im Einsatz.

Die technische Umsetzung dieser Regelung bereitet in der Berliner Verwaltung offensichtlich nach wie vor Schwierigkeiten.

So hatte die Freie Universität Berlin uns bereits im Januar 2000 darüber informiert, dass dort die Neuin-

[136] vgl. Anlagenband, a.a.O., IV.1
[137] JB 2000, 5.1

stallation von mehreren vernetzten digitalen ISDN-Nebenstellenanlagen geplant war. Dort war ursprünglich die mitarbeiterbezogene Speicherung auch von Verbindungsdaten über Dienstgespräche geplant. Unterdessen konnte in intensiven Gesprächen zwischen unserer Dienststelle, der behördlichen Datenschutzbeauftragten der FU und den anderen dort mit der Umsetzung des Vorhabens befassten Stellen sowie Vertretern des Herstellers der Anlage eine Lösung gefunden werden, die die Bestimmung des § 5 IVG unter Nutzung der vom Hersteller standardmäßig zur Verfügung gestellten Softwarekomponenten in befriedigender Weise umsetzt.

5.2 Tele- und Mediendienste

Novellierung des Teledienstedatenschutzgesetzes

Bereits bei In-Kraft-Treten des Informations- und Kommunikationsdienstegesetzes im August 1997 war der Bundesregierung durch Beschluss des Bundestages die Evaluierung der damals neuen Regelung innerhalb von zwei Jahren nach In-Kraft-Treten des Gesetzes auferlegt worden[138]. In unserem letzten Jahresbericht hatten wir über die Initiative der Bundesregierung berichtet, die Ergebnisse der Evaluierung des IuKDG in einer Novellierung des Gesetzes umzusetzen[139]. Mit dem Elektronischer Geschäftsverkehr-Gesetz (EGG), das am 21. Dezember 2001 in Kraft getreten ist[140], erfolgte dies zusammen mit der Umsetzung der Europäischen E-Commerce Richtlinie[141].

Zu den wesentlichen Änderungen zählt, dass die bereits vorher bestehende Berechtigung der Anbieter von Telediensten, Nutzungsprofile bei Verwendung von Pseudonymen zu erstellen, unter den Vorbehalt eines Widerspruchs des Nutzers gestellt wurde (§ 6 Abs. 3 TDDSG).

Neu eingefügt wurde auch eine Vorschrift, die den Anbietern von Telediensten ermöglicht, personenbezogene Daten ihrer Nutzer über die ansonsten gesetzlich festgelegten Fristen hinaus zu verarbeiten, wenn dem Diensteanbieter tatsächliche Anhaltspunkte vorliegen, dass seine Dienste von diesen Nutzern in der Absicht in Anspruch genommen werden, das Entgelt nicht oder nicht vollständig zu entrichten (§ 6 Abs. 8 TDDSG). Betroffene Nutzer sind in diesen Fällen allerdings über derartige Maßnahmen zu unterrichten, sobald dies ohne Gefährdung des mit der Maßnahme verfolgten Zweckes möglich ist.

Erfreulich ist, dass das TDDSG jetzt um Bußgeldvorschriften ergänzt worden ist, die in der Vorgängerfassung des Gesetzes „vergessen“ worden waren. § 9 TDDSG enthält nunmehr einen Katalog von Bußgeldtatbeständen, nach denen Verstöße von Teledienstean-bietern gegen die Bestimmungen des TDDSG bei der

[138] JB 1998, 5.2
[139] JB 2000, 5.2
[140] BGBl. I, S. 3721
[141] 2000/31/EG vom 8. Juni 2000

Verarbeitung personenbezogener Daten mit einer Geldbuße bis zu 50.000 Euro geahndet werden können.

Auch das Teledienstegesetz (TDG) ist um eine Bußgeldvorschrift ergänzt worden, die sich auf Verstöße gegen die Impressumspflicht bezieht (vgl. §§ 6, 12 des TDG). Gleichzeitig sind die Informationspflichten der Anbieter von Telediensten in § 6 TDG erweitert worden.

Gestrichen wurde die Bestimmung des § 5 Abs. 2 TDDSG, nach der für die Verarbeitung von Bestandsdaten der Nutzer für Zwecke der Werbung, der Markt- und Meinungsforschung oder zur bedarfsgerechten Gestaltung von Telediensten eine ausdrückliche Einwilligung der Nutzer erforderlich war. Trotzdem ist die Einwilligung in diesen Fällen weiterhin erforderlich: Ein Rückgriff auf die Bestimmung des § 28 BDSG, das für werbliche Nutzung eine Widerspruchslösung vorsieht, ist nicht möglich, weil die in § 5 TDDSG festgelegten Erlaubnistatbestände dort abschließend geregelt sind.

Vom Geltungsbereich des TDDSG ausgenommen ist zukünftig die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Dienst- und Arbeitsverhältnis, soweit die Nutzung der Teledienste zu ausschließlich beruflichen oder dienstlichen Zwecken erfolgt (§ 1 Abs. 1 Nr. 1 TDDSG); die Aufsichtsbehörden hatten bereits in der Vergangenheit eine Geltung des TDDSG für diesen Bereich verneint. Dies ist jetzt auch im Gesetzestext selbst ausdrücklich klargestellt. Für den genannten Bereich sind die Regelungen des BDSG anzuwenden.

Ebenfalls ausgenommen ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten innerhalb von oder zwischen Unternehmen oder öffentlichen Stellen, soweit die Nutzung der Teledienste zur ausschließlichen Steuerung von Arbeits- oder Geschäftsprozessen erfolgt („b2b“; § 1 Abs. 1 Nr. 2 TDDSG). Damit soll dem Umstand Rechnung getragen werden, dass das TDDSG eigentlich den privaten Nutzer schützen soll. Unklar ist allerdings bisher, wie dieser Bereich von privaten Nutzungsverhältnissen abgegrenzt werden kann.

Wie üblich wurde im Bundesrat im Gesetzgebungsverfahren der Versuch unternommen, Verpflichtungen der Anbieter von Telediensten zur Speicherung und Übermittlung von Bestands- und Nutzungsdaten für Zwecke der Strafverfolgung einzuführen. So sollten Bestands- und Nutzungsdaten bei Telediensten nicht nur an Strafverfolgungsbehörden, sondern auch an Verwaltungsbehörden zur Verfolgung von Ordnungswidrigkeiten und an Nachrichtendienste übermittelt werden. Anbieter von Telediensten sollten darüber hinaus zur Speicherung von Nutzungsdaten auf Vorrat für eine mögliche spätere Strafverfolgung verpflichtet werden. Gegen diese Bestrebungen hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung zum Datenschutz beim elektronischen Geschäftsverkehr entschieden ausgesprochen[142].

[142] vgl. Anlagenband, a.a.O., I.1

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

Internet–Dienstvereinbarung der Berliner Verwaltung

Die Senatsverwaltung für Inneres plant, mit dem Hauptpersonalrat für die Behörden, Gerichte und nichtrechtsfähigen Anstalten des Landes Berlin eine „Dienstvereinbarung über die Nutzung des Internet und anderer elektronischer Informations- und Kommunikationsdienste in der Berliner Verwaltung“ zu schließen. Die Dienstvereinbarung soll insbesondere die Befugnisse der genannten öffentlichen Stellen des Landes Berlin zur Speicherung personenbezogener Nutzungsdaten für solche Dienste regeln.

Die Speicherung von personenbezogenen Daten über das Nutzungsverhalten einzelner Nutzer soll dabei nur in Ausnahmefällen zugelassen werden: In der Regel sollen zur Abrechnung und Kontrolle der kostenverursachenden dienstlichen Nutzung nur der Zeitpunkt des Abrufs und die Größe des übertragenen Objekts für Gruppen von 15 Mitarbeitern gespeichert werden.

Zur Kontrolle missbräuchlicher Nutzung ist vorgesehen, dass – soweit ein hinreichender Verdacht auf Verletzung entsprechender dienst- oder arbeitsvertraglicher Pflichten durch Nutzung des Internet vorliegt – über längstens drei Monate hinweg nach Ankündigung Nutzungsdaten einschließlich der abgerufenen Zielseiten in Gruppen von mindestens sieben Mitarbeitern gespeichert werden dürfen (§ 5 Abs. 1).

Lediglich beim dringenden Verdacht eines Dienstvergehens oder der Verletzung arbeitsvertraglicher Pflichten kann die zuständige Dienstelle mit Zustimmung der obersten Dienstbehörde zur Aufklärung des Sachverhalts für die Dauer von längstens drei Monaten Nutzungsdaten auch über Einzelpersonen speichern, um von ihnen Erklärung des dienstlichen Bezugs dieser Zugriffe zu verlangen. Über diese Maßnahmen sind die betroffenen Beschäftigten im Nachhinein zu informieren.

Die Bestimmungen des Entwurfs sind im Wesentlichen den Regelungen des § 5 IVG nachgebildet.

Die Senatsverwaltung für Inneres hat uns bei der Erstellung der Dienstvereinbarung beteiligt. Dabei war eine Vielzahl unterschiedlicher Bedürfnisse zu berücksichtigen, die eine Speicherung von Nutzungsdaten und der Internet-Nutzung erfordern. Dazu gehören unter anderem auch Aspekte der Datensicherheit, die die Speicherung von Nutzungsdaten zur Erkennung und Verfolgung von Eindringversuchen in das Berliner Landesnetz von außen erforderlich machen. Die vielen verschiedenen Bedürfnisse haben ein relativ komplexes Regelwerk entstehen lassen, das allerdings aus Sicht des Datenschutzes die personenbezogene Speicherung von Nutzungsdaten nur in wenigen Fällen zulässt und dem Gebot der Datenvermeidung nach § 5 a BlnDSG entspricht.

Die Internet-Dienstvereinbarung ist in der mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit abgestimmten Form mit Datum vom 21. Februar 2002 mit dem Hauptpersonalrat abgeschlossen worden.

In der Praxis werden bisher Nutzungsdaten auf Proxy-Rechnern in der Berliner Verwaltung in größerem Umfang gespeichert, als die Regelungen in der Dienst-

Die Protokolldateien der vom LIT betriebenen Proxy-Server bei anderen Behörden werden unmittelbar nach einer behördenabhängigen anonymisierten Auswertung

vereinbarung dies zulassen. Zum ordnungsgemäßen Betrieb der Firewalls und Proxy-Rechner dürfen personenbezogene Daten wie Rechneradresse oder Nutzerkennung nur so weit und so lange in Verbindung mit Kommunikationsinhaltsdaten wie z. B. den aufgerufenen Seiten im Internet unter Wahrung der gesetzlichen Zweckbindung gemäß § 11 Abs. 5 BlnDSG gespeichert werden, wie dies für die Sicherstellung der Betriebsfähigkeit zwingend erforderlich ist. Dies ist zumindest hinsichtlich der vom LIT betriebenen Firewall nur für sehr wenige Nutzer der Fall. Die dortigen Sicherheitserfordernisse können überwiegend mit – nicht personenbezogenen – Protokolldaten auf Proxy-Ebene sichergestellt werden.

zum Zweck der Abrechnung (Menge des Datenaufkommens) gelöscht. Von den Proxy-Servern der einzelnen Verwaltungen werden ausschließlich deren IP-Adressen an den zentralen Proxy-Server im LIT übermittelt.

UseNet News-Server

Einem Bürger war von einem Berliner Betreiber eines Servers, der der Nutzung des „UseNet News"-Dienstes im Internet dient, die Benutzerkennung gesperrt worden, die dort benötigt wird, um Beiträge in einzelnen Newsgroups veröffentlichen zu können. Als Grund gab der Betreiber an, der Nutzer hätte gegen die Verpflichtung aus den dortigen Nutzungsbedingungen verstoßen, nach der jeder Beitrag in der Betreffzeile mit dem vollen Vor- und Nachnamen des Nutzers gekennzeichnet werden muss. Der Betroffene wandte sich an uns mit der Bitte um datenschutzrechtliche Beratung.

Der UseNet News-Dienst (auch „Netnews" oder „News") gehört zu den ältesten Diensten des Internet. Über die angeschlossenen Server können die Nutzer auf eine Vielzahl verschiedener, thematisch gegliederter „Newsgroups" zugreifen und dort die Beiträge anderer Nutzer lesen beziehungsweise selbst Beiträge in die Gruppen einstellen. Hierzu hat die Netzgemeinde im Laufe der Jahre im Wege der Selbstregulierung ein Regelwerk verfasst („Netiquette"), das den „guten Ton" bei der Nutzung des Dienstes festlegt. Zu den dort getroffenen Festlegungen zählt unter anderem, dass angeregt wird, dass Nutzer, die Beiträge in einzelnen Gruppen veröffentlichen, diese mit ihrem vollen Vor- und Nachnamen kennzeichnen. In einigen Newsgroups, in denen es um sehr sensible Themen geht (beispielsweise sexuelle Gewohnheiten), wird hingegen die Nutzung von Pseudonymen beispielsweise Artikeln, die über so genannte Anonymous Remailer in die Gruppen eingestellt werden, geduldet.

Bei dem Angebot, Beiträge unter Nutzung von technischen Einrichtungen eines Anbieters in die Newsgroups einzustellen, handelt es sich um einen Teledienst. Damit sind die Bestimmungen des TDDSG anzuwenden. Dieses sieht vor, dass Anbieter ihren Nutzern die Möglichkeit zur anonymen bzw. pseudonymen Nutzung ihrer Dienste einräumen müssen (§ 4 Abs. 1), soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren.

Dem Betreiber eines solchen Dienstes steht es natürlich frei, seinen Nutzern die Einhaltung der in der „Neti-

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

quette“ niedergelegten Festlegungen zu empfehlen. Er darf die Einhaltung dieser Regeln jedoch dann nicht erzwingen, wenn dies gegen geltendes Recht verstößt. Vorliegend hatte der Betreiber es versäumt, die Nutzer in angemessener Form darüber zu informieren, dass verfasste Nachrichten auch mit einem Pseudonym gekennzeichnet werden können.

5.3 Datenschutz und Medien

Im zurückliegenden Berichtszeitraum ist der Zweite Staatsvertrag zur Änderung des Staatsvertrags über die Zusammenarbeit zwischen Berlin und Brandenburg im Bereich des Rundfunks in Kraft getreten[143]. Der Staatsvertrag gilt für private Rundfunkveranstalter in den Ländern Berlin und Brandenburg; durch die in Kraft getretenen Änderungen werden unter anderem die geltenden Datenschutzbestimmungen an die Regelungen des Vierten Rundfunkänderungsstaatsvertrages[144] in das Berliner und Brandenburger Landesrecht auch für die privaten Rundfunkveranstalter übernommen.

Letztmals: Negative Auskunftspflicht

Nach wie vor hatten wir uns mit dem Umfang der Auskunftspflicht von Rundfunkteilnehmern zu befassen. Mehrere Berliner Rundfunkteilnehmer hatten sich darüber beschwert, dass die im Auftrag des Senders Freies Berlin tätige GEZ bei ihnen wiederholt Auskunft darüber begehrt hatte, ob neben Hörfunk- nunmehr auch Fernsehgeräte zum Empfang bereitgehalten würden.

Der SFB behauptete eine Auskunftspflicht nach § 4 Abs. 5 Rundfunkgebührenstaatsvertrag auch dann, wenn von dem Betroffenen weiterhin keine Fernsehgeräte zum Empfang bereitgehalten werden, und bestand darauf, dass Rundfunkteilnehmer, die nur ein Hörfunkgerät angemeldet haben, der Rundfunkanstalt beziehungsweise der GEZ in jährlichen Abständen mitteilen, dass sie weiterhin nicht über ein Fernsehgerät verfügen. Unsere Überprüfung hatte demgegenüber ergeben, dass die Vorschrift des Rundfunkgebührenstaatsvertrages nicht zu einer derartigen „Negativ-Auskunft“ verpflichtet[145]. Der SFB hat es jedoch unterlassen, unsere Anregung umzusetzen, die Formulare derart zu gestalten, dass künftig eine Auskunftspflicht nur noch in den Fällen angeführt wird, in denen ein Fernsehgerät zum Empfang bereitgehalten wird[146]. Auf nochmalige Nachfrage hat uns der SFB mitgeteilt, dass man dort an der Auffassung festhalte, dass eine Auskunftspflicht auch in den Fällen besteht, in denen weiterhin kein Fernsehgerät zum Empfang bereitgehalten wird. Wir haben daraufhin unter Ausschöpfung der uns zur Verfügung stehenden Mittel das vom SFB praktizierte Verfahren formell datenschutzrechtlich nach § 26 Abs. 1 BlnDSG beim Intendanten des SFB beanstandet.

Der Senat hält an seinen Stellungnahmen zu den Datenschutzberichten 1999 und 2000 fest. Er begrüßt, dass der SFB das Verfahren rundfunkteilnehmerfreundlicher ausgestaltet hat.

[143] JB 2000, 5.3
[144] JB 1999, 5.3
[145] JB 1999, 5.3
[146] JB 2000, 5.3

Auch diese Maßnahmen konnte jedoch den SFB nicht dazu bewegen, von seiner bisherigen Praxis abzurücken. Der Intendant des SFB hat vielmehr – in Übereinstimmung mit den anderen Landesrundfunkanstalten – die Auffassung des SFB bekräftigt, dass auch solche Personen zur Auskunft verpflichtet sind, die weiterhin kein Fernsehgerät zum Empfang bereithalten. Wir halten dagegen an unserer Rechtsauffassung fest.

Immerhin hat der SFB das dort praktizierte Verfahren insoweit verändert, dass Rundfunkteilnehmer, die gegenüber dem SFB beziehungsweise der GEZ einmal bestätigen, dass sie weiterhin kein Fernsehgerät zum Empfang bereithalten, und gleichzeitig ausdrücklich darum bitten, von weiteren Anfragen gleicher Art ausgenommen zu werden, bei der GEZ für zukünftige gleichartige Versandmaßnahmen – ohne Anerkenntnis einer Rechtspflicht – gesperrt werden. Damit besteht für die „Nur-Hörfunkteilnehmer" zukünftig immerhin die Möglichkeit zu erreichen, dass sie derartige Anschreiben nicht „alle Jahre wieder" mehrfach in ihrem Briefkasten vorfinden.

Neue Medienordnung

Große Ereignisse werfen ihre Schatten voraus: Bund und Länder haben sich grundsätzlich darauf geeinigt, die Gesetzgebungskompetenz im Bereich der Medien neu zu ordnen. Dabei soll der Jugendschutz in die Gesetzgebungskompetenz der Länder überführt werden; im Gegenzug soll der Bund die Gesetzgebungskompetenz für die Mediendienste erhalten, die bisher in einem Staatsvertrag der Länder geregelt sind[147].

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung[148] darauf hingewiesen, dass zu den bei der Neuordnung der Gesetzgebungskompetenzen von Bund und Ländern zu beachtenden Rahmenbedingungen auch die Grundrechte auf Schutz der Privatsphäre und der personenbezogenen Daten sowie der Meinungsfreiheit und der Vertraulichkeit der Kommunikation zählen. Diese Rechte müssen in einer neuen Medienordnung durchgängig gewährleistet bleiben. Die Konferenz hat aus diesem Grund gefordert, das Fernmeldegeheimnis nach Artikel 10 des Grundgesetzes zu einem allgemeinen Kommunikations- und Mediennutzungsgeheimnis weiterzuentwickeln und einfach gesetzlich abzusichern.

Änderungen in Bezug auf die Rechte der Nutzer von Mediendiensten und die Pflichten der Anbieter sind durch die geplante Verlagerung der Gesetzgebungskompetenz kaum zu erwarten, da die Datenschutzregelungen des Mediendienste-Staatsvertrags bereits jetzt weitestgehend den Vorschriften für die Anbieter von Telediensten[149] entsprechen, die bereits jetzt durch Bundesgesetz geregelt sind. Eine Vereinheitlichung der Gesetzesmaterie dürfte die Tätigkeit der Anbieter von Diensten im Internet insofern erleichtern, als die Ein-

[147] Staatsvertrag über Mediendienste (Mediendienste-Staatsvertrag – MDStV) vom 23. Juni 1997 (GVBl. S. 361; JB 1997, 5.3)
[148] Entschließung zu „Neue Medienordnung". In: Anlagenband, a.a.o., I.3
[149] vgl. 5.2

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

ordnung bestimmter Internet-Dienstleistungen als Telebeziehungsweise als Mediendienste in der Vergangenheit in Einzelfällen zu Schwierigkeiten geführt hat.

Unverändert sollte auch die Zuweisung der datenschutzrechtlichen Kontrollkompetenz an die Aufsichtsbehörden der Länder bleiben, die bisher sowohl für Tele- als auch für Mediendienste besteht, um ein Auseinanderfallen der Datenschutzkontrolle im Offline- und Online-Bereich zu verhindern.

Zusammenführung der Landesrundfunkanstalten SFB und ORB

Die Berliner Senatskanzlei und die Staatskanzlei Brandenburg planen den Abschluss eines Staatsvertrages, mit dem der Sender Freies Berlin (SFB) und der Ostdeutsche Rundfunk Brandenburg (ORB) zu einer gemeinsamen Landesrundfunkanstalt für Berlin und Brandenburg zusammengeführt werden sollen. Wir haben gemeinsam mit dem LDA Brandenburg hierzu einen Vorschlag für die Datenschutzbestimmungen, die bei der neugebildeten Rundfunkanstalt Anwendung finden sollen, übersandt. Da bereits jetzt das geltende Recht für den SFB in Berlin und den ORB in Brandenburg sich nur Nuancen unterscheidet, haben wir im Wesentlichen empfohlen, die bisher bestehenden Regelungen in den Staatsvertrag zu übernehmen.

Der Staatsvertragsentwurf berücksichtigt im vollem Umfang die Vorstellungen der Datenschutzbeauftragten der Länder Berlin und Brandenburg.

Insbesondere sollte es bei der bisherigen Aufteilung der datenschutzrechtlichen Kontrollkompetenz auch bei der neuen Rundfunkanstalt bleiben: Bereits jetzt wird sowohl in Berlin als auch in Brandenburg im „journalistisch-redaktionellen“ Bereich, soweit die Rundfunkanstalt personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken verarbeitet, die Kontrolle der Einhaltung des geltenden Datenschutzrechts durch eine(n) Datenschutzbeauftragte(n) der jeweiligen Rundfunkanstalt wahrgenommen. Diese Beschränkung der staatlichen Aufsicht im publizistischen Kernbereich der Tätigkeit der Rundfunkanstalten ist aus verfassungsrechtlichen Gründen (Art. 5 GG) geboten.

Die Kontrolle der Verarbeitung personenbezogener Daten von Mitarbeitern und Rundfunkteilnehmern im „wirtschaftlich-administrativen“ Bereich wird dagegen auch schon bisher vom jeweiligen Landesbeauftragten für den Datenschutz wahrgenommen. Dabei muss es auch zukünftig bleiben, da eine umfassende Kontrollbefugnis der Datenschutzbeauftragten der Rundfunkanstalten auch für die Verarbeitung von Mitarbeiter- und Rundfunkteilnehmerdaten den Bestimmungen der Europäischen Datenschutzrichtlinie (Art. 9) widersprechen würde.

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats

6. Aus der Dienststelle

6.1. Entwicklung

Mit dem neuen BlnDSG wurde die Amtsbezeichnung unserer Dienststelle an den Gesetzestitel des IFG angepasst. Sie lautet seit 5. August 2001 „Berliner Beauftragter für Datenschutz und Informationsfreiheit“.

Die im vergangenen Jahr umstrittene Frage, wer den Berliner Beauftragten für Datenschutz und Informationsfreiheit zur Wahl im Abgeordnetenhaus vorschlagen muss, wurde im Rahmen der Novellierung durch Nichtregelung geklärt: Das bisherige Vorschlagsrecht des Senats wurde aus den Bestimmungen über die Bestellung und Entlassung des Beauftragten gestrichen. Da Beauftragte vom Abgeordnetenhaus gewählt und vom Präsidenten des Abgeordnetenhauses ernannt werden, ergibt sich damit unmittelbar aus der Verfassung, dass nunmehr dem Abgeordnetenhaus das Vorschlagsrecht zukommt.

Der Senat geht davon aus, dass mit der Streichung des konstitutiven Wahlvorschlagsrechts des Senats im Gesetz nicht das Recht des Senats entfallen ist, auch einen Vorschlag zu unterbreiten.

Die Arbeit in der Dienststelle wurde im Berichtsjahr dadurch erschwert, dass die Leitung des Bereichs Recht nicht besetzt werden konnte. Belastend war auch, dass für die Aufgabe nach dem Informationsfreiheitsgesetz im Gegensatz zu anderen Ländern bisher keine Stelle zur Verfügung gestellt wurde. Weitere große Belastungen werden dadurch auf uns zukommen, dass das neue BDSG eine Amtsaufsicht über die Privatunternehmen vorsieht. Soll diese bundesrechtliche Vorgabe im Land Berlin erfüllt werden, kann es auch für diese Aufgabe nicht beim derzeitigen Personalbestand bleiben, der im Wesentlichen auf die Kontrolle des öffentlichen Bereichs ausgerichtet ist.

Die Forderung nach zusätzlichen Stellen aufgrund des Informationsfreiheitsgesetzes sowie für die zu erwartende Amtsaufsicht über die Privatunternehmen im Rahmen der Novellierung des Bundesdatenschutzgesetzes und den damit voraussichtlich eintretenden Aufgabenzuwachs ist nicht nachvollziehbar. Angesichts der Tatsache, dass der Berliner Beauftragte für Datenschutz und Informationsfreiheit regelmäßig von den zur Sanierung des Haushalts unabdingbar notwendigen Sparmaßnahmen im Personalbereich ausgenommen wird – so auch im Doppelhaushalt 2002 und 2003 – und damit gegenüber allen anderen Bereichen – einschließlich der Verwaltung des Abgeordnetenhauses und des Rechnungshofes –, die ihre unverändert wahrzunehmenden Aufgaben mit einem immer geringeren Personalbestand erfüllen müssen, bevorzugt wird, erscheint die Forderung unangemessen. Der Senat geht deshalb davon aus, dass mit dem vorhandenen Personal die Aufgabenwahrnehmung und ggf. auch die Bewältigung zusätzlicher Aufgaben möglich sein muss. Die Einschätzung, dass eine Aufstockung des Personalbestandes unausweichlich sei, wird nicht geteilt.

6.2. Die Aufgaben

Die Verteilung der Vorgänge auf die einzelnen Arbeitsgebiete zeigt einen weiteren Anstieg des Telekommunikations- und Medienbereichs, der nunmehr mit den Arbeitsgebieten Innere Sicherheit und Wirtschaft ungefähr gleich aufliegt. Die meisten Vorgänge kommen nach wie vor aus dem Bereich Gesundheit und Soziales.

6.3 Zusammenarbeit mit dem Parlament

Der Unterausschuss „Datenschutz“ des Ausschusses für Innere Sicherheit und Ordnung hatte unter dem Vorsitz des Abgeordneten Peter Trapp bis zum Ende

der Legislaturperiode in eineinhalb Jahren 21 Sitzungen. Die Beratung der Jahresberichte 1998 und 1999 konnte abgeschlossen werden. Der Unterausschuss machte insgesamt 15 Beschlussempfehlungen, die in der letzten Sitzung des Abgeordnetenhauses am 27. September 2001 angenommen wurden[150]. Wesentlicher Beratungspunkt war die Erörterung des Entwurfs für ein neues Berliner Datenschutzgesetz, bei der weitere Verbesserungen der Senatsvorlage erreicht werden konnten.

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 der Landesbeauftragten für Datenschutz Nordrhein-Westfalen, Bettina Sokol, in Düsseldorf (8./9. März 2001) und Münster (24./25. Oktober 2001) tagte, wurde erneut eine Reihe von Beschlüssen gefasst, die die Fortentwicklung des Datenschutzes fördern sollten[151]. Die Ergebnisse sind bei den Berichten aus den Arbeitsgebieten dargestellt worden. Im laufenden Jahr hat der Landesbeauftragte für den Datenschutz Rheinland-Pfalz, Prof. Dr. Walter Rudolf, den Vorsitz übernommen.

Die Arbeitsgemeinschaft der Informationsbeauftragten Deutschlands, der nach Berlin, Brandenburg und Schleswig-Holstein ab 1. Januar 2002 auch Nordrhein-Westfalen angehört, erörterte Fragen der Fortbildung der Informationsfreiheitsgesetzgebung am 23. Juli 2002 in Berlin.

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. Für die weitere Arbeit war von besonderer Bedeutung die Klärung des Vorsitzes in diesem Gremium. Einzelne Datenschutzbeauftragte hatten in Frage gestellt, ob der Vorsitz dieses Koordinierungsgremiums weiterhin in der Hand eines Ministeriums liegen könne, da dieses nicht über die in der Europäischen Richtlinie vorgeschriebene „völlige Unabhängigkeit“ (Art. 28 Abs. 1) verfüge. Diese Auffassung wurde in einem Schriftwechsel mit dem zuständigen Mitglied der Europäischen Kommission bestätigt. Nach eingehender Debatte wurde ein Kompromiss gefunden: Ab 2002 wechselt der Vorsitz jährlich so, dass abwechselnd ein Innenministerium und ein Landesbeauftragter den Vorsitz führt. Im Jahr 2002 beginnt Baden-Württemberg, gefolgt von Berlin im Jahr 2003.

[150] vgl. Anlage 1
[151] vgl. Anlagenband, a.a.O., I.1.-3.

Im Düsseldorfer Kreis hat der Berliner Beauftragte für Datenschutz und Informationsfreiheit den Vorsitz in den Arbeitsgruppen „Telekommunikation, Tele- und Mediendienste“ sowie „Internationaler Datenverkehr“. Die wichtigsten Themen waren die datenschutzrechtliche Behandlung von IP-Adressen insbesondere bei Bannerwerbung im Internet sowie die Sicherstellung hinreichender Garantien für den Datenschutz bei der Datenübermittlung in Drittländer[152].

Auf europäischer Ebene ist der Berliner Beauftragte für Datenschutz und Informationsfreiheit zusammen mit dem Bundesdatenschutzbeauftragten deutscher Vertreter in der Artikel 29-Datenschutzgruppe, der alle europäischen Datenschutzinstitutionen angehören und die die Europäische Kommission in Datenschutzfragen berät.

Die Internationale Arbeitsgruppe Datenschutz in der Telekommunikation, die im Rahmen der Internationalen Konferenz der Datenschutzbeauftragten unter dem Vorsitz des Berliner Beauftragten für Datenschutz und Informationsfreiheit arbeitet, hatte wie immer zwei Sitzungen. Mittelpunkt der Sitzung am 15./16. Februar 2001 in Bangalore/Indien standen die Datenschutzfragen, die im Zusammenhang mit Lokationsdaten beim Mobilfunk auftreten. In einem gemeinsamen Standpunkt wird vor allem die Bedeutung der Einwilligung der Teilnehmer in die Nutzung dieser Funktion betont[153]. In der Sitzung am 28. August in Berlin wurden Papiere zu elektronischen Wahlen und zur Infrastruktur bei öffentlichen digitalen Schlüsseln beschlossen. Die Arbeitsergebnisse wurden bei der Internationalen Konferenz der Datenschutzbeauftragten am 24.-26. September 2001 in Paris vorgestellt. Mit der Europäischen Datenschutzkonferenz, die vom 9.-11. Mai 2001 in Athen tagte, wurde eine besondere Kooperationsvereinbarung getroffen.

Abgeschlossen wurde das von der Europäischen Kommission geförderte Leonardo-da-Vinci-Projekt DATAPROT, bei dem ein für ganz Europa gültiges Konzept der Fortbildung für Lehrpersonal im Bereich des Datenschutzes entwickelt wurde. Das Projekt wurde von der Datenschutzkommission der spanischen Hauptstadt Madrid koordiniert.

6.5 Öffentlichkeitsarbeit

Bereits in den vergangenen Jahren haben wir darüber berichtet, dass unser Internetprogramm www.datenschutz-berlin.de zunehmend in den Mittelpunkt unserer Öffentlichkeitsarbeit rückt. Diese Tendenz hat sich auch im Berichtszeitraum 2001 fortgesetzt. Dokumentiert wird diese Entwicklung durch die Zahl von insgesamt bis zu 530.000 „Hits“, die monatlich auf unser Programm zugreifen. Unsere verschiedenen Online-Publikationen werden bis zu 6.400-mal im Monat im Download-Verfahren abgerufen. Bestätigung findet unsere Arbeit zudem durch die vie-

[152] vgl. 4.7
[153] vgl. 5.1

len elektronischen Anfragen und Anregungen, die uns – verstärkt auch aus dem nationalen und internationalen Raum – in Bezug auf unser Internetprogramm erreichen. Leider müssen einige der an uns herangetragenen Fragen, Anregungen und Vorschläge zur Erweiterung bzw. Ergänzung des Programms - angesichts der beschränkten personellen und finanziellen Ressourcen, die uns zur Pflege des Programms zur Verfügung stehen – unberücksichtigt bleiben. Wir bitten insofern um Verständnis.

Unabhängig von unseren vielfältigen Aktivitäten im Bereich der Online-Publikationen haben wir auch im vergangenen Jahr einige Broschüren herausgegeben.

Im vergangenen Jahr wurde zwar die Neufassung des Bundesdatenschutzgesetzes verabschiedet. Eine Neuverkündung des Gesetzes ist jedoch bis heute ausgeblieben. Wir haben daher – motiviert durch die vielfachen Anfragen - auf der Grundlage einer vom Bundesministerium des Innern gefertigten Arbeitsfassung eine Textfassung des geänderten Gesetzes erstellt und als Broschüre unter dem Titel „Bundesdatenschutzgesetz 2001“ in unserer Schriftenreihe „Berliner Informationsgesetzbuch“ herausgegeben. Im Materialienband Nr. 30 haben wir ergänzend dazu, in Kooperation mit dem Unabhängigen Landeszentrum für den Datenschutz Schleswig-Holstein, die wichtigsten „Neuregelungen im Bundesdatenschutzgesetz“ zusammengestellt und erläutert.

Auch das Berliner Datenschutzgesetz wurde im vergangenen Jahr in wesentlichen Punkten geändert. Um das bestehende Informationsbedürfnis der Bürger bzw. der Rechtsanwender in den Berliner Verwaltungen zu befriedigen, haben wir auch dieses Gesetz als Textfassung mit dem Titel „ Berliner Datenschutzgesetz“ in unserer Schriftenreihe „Berliner Informationsgesetzbuch“ veröffentlicht.

Die Schriftenreihe „Ratgeber zum Datenschutz“, in der wir den interessierten Bürgern kurze, allgemein verständliche Informationen und Hilfe zur Selbsthilfe zu ausgewählten Datenschutzthemen anbieten, erfreut sich zunehmender Beliebtheit. Dies hat uns veranlasst, ein weiteres Heft in dieser Reihe herauszugeben. Im Band Nr. 6 beschreiben wir unter dem Titel „Handels- und Wirtschafts-Auskunfteien“ deren Praxis der Informationssammlung über die wirtschaftliche Betätigung, Kreditwürdigkeit und Zahlungsfähigkeit von Unternehmen und Privatpersonen. Das Heft gibt Auskunft über die Zulässigkeit dieser Tätigkeiten und informiert den Betroffenen über seine Rechte im Umgang mit derartigen Einrichtungen.

Berlin, 18. März 2002

Prof. Dr. Hansjürgen Garstka

Berliner Beauftragter für Datenschutz und Informationsfreiheit

Berlin, den 18. Juni 2002

Der Senat von Berlin

Klaus Wowereit

Regierender Bürgermeister

Bericht des Beauftragten für Datenschutz und Informationsfreiheit	Stellungnahme des Senats