Abgeordnetenhaus von Berlin

12. Wahlperiode

Drucksache 12/4372

66 Seiten

Bericht

des Berliner Datenschutzbeauftragten

zum 31. Dezember 1993

Der Berliner Datenschutzbeauftragte hat dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen (§ 29 Berliner Datenschutzgesetz - BlnDSG -). Der vorliegende Bericht schließt an den am 22. März 1993 vorgelegten Jahresbericht 1992 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 1993 ab.

Wir kommen damit zugleich den Pflichten nach § 6 Abs. 3 Gesetz zu dem Staatsvertrag über den Rundfunk im vereinten Deutschland vom 31. August 1991 und zu Art. 36 des Einigungsvertrages[1] nach[2].

1 GVBl. 1991, S. 309 f.
2 vgl. 5.1

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.

Inhaltsverzeichnis

Einleitung

1. **Rechtliche Rahmenbedingungen**
1.1 Deutschland und Europa
1.2 Datenschutz in Berlin

2. **Technische Rahmenbedingungen**
2.1 Zentral, dezentral, überall - Berliner IuK-Politik im Spiegel der technischen Entwicklung
2.2 Automation der Berliner Verwaltung
2.3 Chipkarten - nur Trümpfe für den Datenschutz?

3. **Grundsatzprobleme**
3.1 Magna Charta des Datenschutzes - Auskunfts- und Einsichtsrechte
3.2 Privatisierung öffentlicher Aufgaben zu Lasten des Datenschutzes

4. **Ausgewählte Geschäftsbereiche**
4.1 Arbeit und Frauen
4.2 Bau- und Wohnungswesen
4.3 Finanzen
4.4 Gesundheit
4.5 Inneres
4.5.1 Polizei
4.5.2 Verfassungsschutz
4.5.3 Einwohnerwesen
4.5.4 Statistik
4.5.5 Personalwesen
4.6 Jugend und Familie
4.7 Justiz
4.8 Schule, Berufsbildung und Sport
4.9 Soziales
4.10 Stadtentwicklung und Umweltschutz
4.11 Verkehr und Betriebe
4.12 Wissenschaft und Forschung

5. **Telekommunikation und Medien**
5.1 Berlin
5.2 Deutschland und Europa

6. **Durchsetzung des Datenschutzes**
6.1 Datenschutz im Verwaltungsverfahren
6.2 Falsch verstandener Datenschutz
6.3 Dateienregister
6.4 Der Berliner Datenschutzbeauftragte
6.5 Öffentlichkeitsarbeit

Anlagen zum Jahresbericht 1993

1. **Rede des Berliner Datenschutzbeauftragten vor dem Berliner Abgeordnetenhaus am 16. September 1993**

2. **Stellungnahmen und Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder**
2.1 Stellungnahme der Konferenz vom 15. April 1993 zum Entwurf eines Gesetzes zur Umsetzung des Föderalen Konsolidierungsprogramms - FKPG - (BR-Drs. 121/93 vom 5. März 1993)
2.2 Entschließung der 45. Konferenz am 16./17. Februar 1993 zur Richtlinie des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt (30/313/EWG)
2.3 Entschließung der 46. Konferenz am 26./27. Oktober 1993 zu regelmäßigen Datenübermittlungen an die öffentlich-rechtlichen Rundfunkanstalten und die Gebühreneinzugszentrale (GEZ)
2.4 Entschließung der 46. Konferenz am 26./27. Oktober 1993 zum Datenschutz bei der Privatisierung der Deutschen Bundespost TELEKOM und bei der europaweiten Liberalisierung des Telefonnetzes und anderer Telekommunikationsdienste
2.5 Entschließung der 46. Konferenz am 26./27. Oktober 1993 zur Gewährleistung des Datenschutzes bei der Mobilkommunikation
2.6 Entschließung der 46. Konferenz am 26./27. Oktober 1993 zur Gefährdung der Vertraulichkeit der Funkkommunikation von Sicherheitsbehörden und Rettungsdiensten
2.7 Entschließung der 46. Konferenz am 26./27. Oktober 1993 zum Integrierten Verwaltungs- und Kontrollsystem (InVeKoS) (Verordnungen der EWG Nrn. 3508/92 und 3887/92)
2.8 Entschließung der 46. Konferenz am 26./27. Oktober 1993 zu kartengestützten Zahlungssystemen im Öffentlichen Nahverkehr

3. **Bericht der Arbeitsgruppe Telekommunikation und Medien an die 15. Internationale Konferenz der Datenschutzbeauftragten in Manchester (27. bis 30. September 1993)**

4. **Auszug aus dem Geschäftsverteilungsplan**

5. **Abkürzungsverzeichnis**

6. **Stichwortverzeichnis**

Einleitung

Der Berliner Datenschutzbeauftragte legt zum fünfzehnten Mal dem Abgeordnetenhaus, der Berliner Verwaltung, aber auch der Berliner Öffentlichkeit einen Tätigkeitsbericht vor. Wir haben die im Datenschutzgesetz niedergelegte Verpflichtung, jährlich einen derartigen Bericht zu verfassen, immer so verstanden, daß nicht nur eine Liste der festgestellten Datenschutzmängel vorgelegt wird, sondern dem Leser ein Überblick über die aktuellen Probleme des Datenschutzes gegeben werden soll. Obwohl sich der Senat in seiner Stellungnahme zum Jahresbericht 1992 hierüber kritisch geäußert hat, bedeutet dies, daß nicht nur über das Landesrecht, sondern auch über Bundesgesetzgebung und -rechtsprechung berichtet werden muß: Die Berliner Verwaltung wird in entscheidenem Maße durch die bundesrechtlichen und künftig mehr und mehr auch die europarechtlichen Vorgaben bestimmt.

So standen im Jahr 1993 in der öffentlichen Debatte über den Datenschutz in Bund und Land zwei Themenbereich im Vordergrund, die das Bundesrecht betreffen: Die Frage, ob durch eine Zurücknahme der grundrechtlichen Garantie der Unverletzlichkeit der Wohnung und eine erneute Verschärfung der Strafprozeßordnung der „Große Lauschangriff" auch bei der Strafverfolgung zugelassen werden sollte. Komplizierter und verwirrender, für die Betroffenen aber auch in datenschutzrechtlicher Hinsicht folgenreicher sind die Änderungen des Sozialrechts, die den angeblich in erheblichem Umfang vorhandenen Mißbrauch von Sozialleistungen mit Hilfe bisher kaum vorstellbarer Möglichkeiten regelmäßiger Datenübermittlungen und -abrufe bekämpfen sollen.

Zu beiden Problemen hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, deren Vorsitz unser Land in diesem Jahr hatte, klar geäußert: Zum Großen Lauschangriff bekräftigte die Konferenz ihren Beschluß vom Vorjahr, nach dem jedem ein privates Refugium, ein persönlicher Bereich bleiben muß, der obrigkeitlicher Ausforschung - insbesondere heimlicher - entzogen ist. Der Lauschangriff auf Privatwohnungen für Zwecke der Strafverfolgung dürfe auch in Zukunft nicht erlaubt werden. Zu den Änderungen in der Sozialgesetzgebung wiesen die Datenschutzbeauftragten auf die Gefahren hin, die damit verbunden sind, daß Einzelfallüberprüfungen durch pauschale Datenabgleiche ersetzt werden und damit die Daten all derjenigen, bei denen keine Anhaltspunkte für falsche Angaben oder Verletzungen von Mitteilungspflichten bestehen, in einem kaum beschränkten Abgleich der Datenbestände nicht nur der Sozialleistungsträger untereinander, sondern auch mit Beständen anderer Verwaltungen genutzt werden sollen.

Die öffentlichen Debatten um diese Gesetzgebungsprojekte haben gezeigt, daß der Datenschutz mehr als zuvor Widerständen ausgesetzt ist. Diese werden häufig in überzogener Weise dargestellt: Schlagwörter wie „Datenschutz ist Täterschutz" oder „Wer schützt uns vor dem Datenschutz?" nutzen auf unsachgemäße Weise Ängste in der Bevölkerung, um eine Stimmung zu erzeugen, in denen Gesetzgebungsvorhaben lanciert werden können, die in früheren Jahren als nicht akzeptabler Verstoß gegen die Prinzipien der informationellen Selbstbestimmung angesehen worden wären.

Diese Grundstimmung hat sich, von den stets vorhandenen Ausnahmen abgesehen, auf die Berliner Verwaltung noch nicht übertragen. In der Regel wird der Datenschutz richtigerweise als notwendiges Korrektiv für die zunehmende Informatisierung der Gesellschaft angesehen. Die Berliner Rechtslage, die von einem bürgerfreundlichen Datenschutzgesetz geprägt ist, trägt hierzu entscheidend bei: Neue Gesetzesbestimmungen und Verordnungen schaffen für Verwaltung und Bürger zunehmend Transparenz. Die Bürger und Bürgerinnen unseres Landes sind aufgerufen, durch Skepsis gegenüber unsachlichen Parolen und durch Wahrnehmung ihrer Rechte ihre informationelle Selbstbestimmung durchzusetzen.

1. Rechtliche Rahmenbedingungen

1.1 Deutschland und Europa

Das Grundrecht auf informationelle Selbstbestimmung

Am 15. Dezember 1983 hat das Bundesverfassungsgericht in seinem „Volkszählungsurteil" erstmals das Recht auf informationelle Selbstbestimmung formuliert[3]. In einer späteren Entscheidung sprach das Gericht ausdrücklich von einem Grundrecht auf Datenschutz[4]. Dennoch gibt die Verfassungswirklichkeit im vereinten Deutschland 10 Jahre nach dem Volkszählungsurteil den Datenschutzbeauftragten wenig Anlaß zur Zufriedenheit.

Es ist unbestreitbar, daß die konsequente Rechtsprechung des Bundesverfassungsgerichts dazu beigetragen hat, dem Datenschutz einen Stellenwert einzuräumen, den er auch nach der Verabschiedung der ersten Datenschutzgesetze in Bund und Ländern noch nicht hatte. Andererseits hat der Bundesgesetzgeber in den vergangenen Jahren (gerade auch im Berichtszeitraum) ständig neue Gesetze beschlossen, die zwar der Bekämpfung der organisierten Kriminalität, der mißbräuchlichen Inanspruchnahme von Sozialleistungen oder der Steuerhinterziehung dienen sollen, gleichzeitig aber zu einer massenhaften Verarbeitung der Daten von unverdächtigen und rechtstreuen Bürgern führen. Selbst wenn einzelne dieser Gesetze für sich betrachtet noch hinnehmbar sein mögen, stellt sich doch die Frage, ob die gesetzlich legitimierte Verarbeitung von Bürgerdaten durch die verschiedensten staatlichen Stellen (von der mindestens ebenso datenhungrigen Privatwirtschaft einmal abgesehen) nicht insgesamt ein Ausmaß erreicht, das in der Summe dem Grundrecht auf informationelle Selbstbestimmung nicht mehr gerecht wird.

Vor diesem Hintergrund erscheint es dringend geboten, das Grundrecht auf informationelle Selbstbestimmung ausdrücklich in den Text der geschriebenen Verfassung aufzunehmen. Diese Forderung hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder schon im April 1992 erhoben[5] und im Berichtszeitraum mehrfach bekräftigt. Dennoch haben entsprechende Vorschläge in der Gemeinsamen Verfassungskommission von Bundestag und Bundesrat nicht die erforderliche 2/3-Mehrheit gefunden[6], wobei auch Berlin - entgegen unserer Empfehlung - die Vorschläge nicht unterstützt, sondern sich der Stimme enthalten hat.

Stattdessen wird - unabhängig von den Beratungen in der Gemeinsamen Verfassungskommission - in der politischen Diskussion zunehmend befürwortet, das Grundrecht auf Unverletzlichkeit der Wohnung, das ebenfalls zentrale Bedeutung für die informationelle Selbstbestimmung der Bürger hat, für Zwecke des „Großen Lauschangriffs" einzuschränken.

Immerhin haben mehrere Fraktionen für die jetzt begonnenen Beratungen in den gesetzgebenden Körperschaften eigene Gesetzentwürfe eingebracht, in denen die Aufnahme eines Menschenrechts auf informationelle Selbstbestimmung und auf Zugang zu den Daten der vollziehenden Gewalt in den Grundrechtskatalog des Grundgesetzes vorgeschlagen wird[7].

Bundesgesetzgebung

Mit dem Gesetz über Maßnahmen zur Bewältigung der finanziellen Erblasten im Zusammenhang mit der Herstellung der Einheit Deutschlands, zur langfristigen Sicherung des Aufbaus in den neuen Ländern, zur Neuordnung des bundesstaatlichen Finanzausgleichs und zur Entlastung der öffentlichen Haushalte *(Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms - FKPG -)* vom 23. Juni 1993[8] wurden Vorschriften in das Bundessozialhilfegesetz und in das Arbeitsförderungsgesetz aufgenommen, die die informationelle Selbstbestimmung deutlich beeinträchtigen. Danach sind die Träger der Sozialhilfe befugt, alle Sozialhilfeempfänger ohne konkreten Anlaß regelmäßig im Wege

3 BVerfGE 65, 1, 43
4 BVerfG NJW 1991, S. 2129, 2132
5 Jahresbericht 1992, Anlage 2.2
6 BR-Drs. 800/93, S. 60 ff.
7 BT-Drs. 12/6323, 12/6686, 12/6570
8 BGBl. 1993 I, S. 944 ff.

des *automatisierten Datenabgleichs* daraufhin zu überprüfen, ob und in welcher Höhe und für welche Zeiträume sie Leistungen der Bundesanstalt für Arbeit oder der gesetzlichen Unfall- oder Rentenversicherung beziehen (§ 117 Abs. 1 BSHG). Damit wird jedem Sozialhilfeempfänger ohne konkrete Anhaltspunkte unterstellt, daß er möglicherweise Sozialhilfe unrechtmäßig und in betrügerischer Absicht in Anspruch nimmt, während er gleichzeitig Arbeitslosenunterstützung oder Leistungen der gesetzlichen Unfall- oder Rentenversicherung erhält oder andere Nebeneinkünfte hat. Die Datenschutzbeauftragten des Bundes und der Länder hatten während des Gesetzgebungsverfahrens in einer Stellungnahme vom 15. April 1993 Kritik an diesem pauschalen Datenabgleich geübt[9]. Die Ausschüsse des Bundesrates hatten ebenfalls empfohlen, von dem pauschalen Datenabgleich abzusehen. Das in Kraft getretene Gesetz berücksichtigt diese grundsätzlichen Einwände nicht, auch wenn im einzelnen Verbesserungen erreicht werden konnten.

Die Träger der Sozialhilfe sind auch befugt, einen regelmäßigen Datenabgleich untereinander zur Feststellung der mißbräuchlichen Inanspruchnahme von Sozialhilfe durchzuführen (§ 117 Abs. 2 BSHG). In beiden Fällen bedarf es noch einer Rechtsverordnung des Bundesministeriums für Familie und Senioren, bevor der automatisierte Abgleich stattfinden darf.

Wer in Zukunft Sozialleistungen beantragt, muß damit rechnen, daß seine Daten jederzeit ohne konkreten Anlaß von anderen Sozialleistungsträgern für Überprüfungszwecke „on line" abgerufen werden können. Damit ist der Zweckbindungsgrundsatz im Verhältnis zwischen den Sozialleistungsträgern ohne Not entwertet worden. Die *Rasterfahndung* als Instrument der Verdachtsschöpfung hat damit auch Eingang in das Sozialrecht gefunden, ohne daß im Gesetzgebungsverfahren mit Zahlen belegt worden wäre, daß die schon bisher gegebenen Kontroll- und Übermittlungsbefugnisse im Einzelfall nicht ausreichen.

Bereits aufgrund des Gesetzes, also ohne zusätzliche Rechtsverordnung, dürfen die Träger der Sozialhilfe zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe Daten von Sozialhilfeempfängern bei anderen Stellen ihrer Verwaltung überprüfen. Dazu zählen neben Daten über Geburt und Wohnsitz auch Daten über Mietzahlungen, Dauer und Kosten von bezogenen Leistungen (Elektrizität, Gas, Wasser, Telefon oder Abfallentsorgung) sowie über die Eigenschaft als Kraftfahrzeughalter. Diese Überprüfung darf allerdings nicht im Wege des automatisierten Datenabgleichs stattfinden und sie muß im Einzelfall erforderlich sein[10].

Am 29. November 1993 trat das Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten *(Geldwäschegesetz - GwG)*[11] in Kraft. Das Gesetz verpflichtet Kreditinstitute, die Kunden bei Annahme oder Abgabe von Bargeld, Wertpapieren oder Edelmetallen im Wert von 20 000,– DM oder mehr zu identifizieren. Das gilt auch, wenn mehrere kleinere Bargeldbeträge eingezahlt oder abgehoben werden, die zusammen den Schwellenwert von 20 000,– DM erreichen oder übersteigen, sofern tatsächlich Anhaltspunkte dafür vorliegen, daß zwischen ihnen eine Verbindung besteht. Die Angaben, die der Kunde zu seiner Identifizierung macht, muß das Kreditinstitut aufzeichnen (in der Regel durch Anfertigung einer Kopie des vorgelegten Dokuments, wie z. B. eines Personalausweises) und sechs Jahre lang aufbewahren. In den Fällen der Identifizierungspflicht muß der Kunde auch angeben, ob er für eigene Rechnung handelt. Ist dies nicht der Fall, so hat das Kreditinstitut nach Angaben des Kunden Namen und Anschrift desjenigen festzustellen, für dessen Rechnung der Kunde handelt.

Stellt ein Kreditinstitut Tatsachen fest, die darauf schließen lassen, daß eine Finanztransaktion einer strafbaren Geldwäsche dient, so hat es dies unverzüglich den Strafverfolgungsbehörden anzuzeigen. Die beabsichtigte Finanztransaktion darf erst durchgeführt werden, wenn die Staatsanwaltschaft dem zugestimmt hat oder wenn seit der Anzeige zwei Werktage verstrichen sind, ohne daß die Durchführung der Transaktion untersagt wurde.

Ähnliche Pflichten zur Identifizierung und Anzeige treffen Lebensversicherungsunternehmen, Versteigerer, Kreditkartengesellschaften, Vermögensverwaltungen, Edelmetallhändler, Spielbanken und die Deutsche Bundespost.

Durch das am 30. Dezember 1993 in Kraft getretene *Gesetz zur Bekämpfung des Mißbrauchs und zur Bereinigung des Steuerrechts* (Mißbrauchsbekämpfungs- und Steuerbereinigungsgesetz - StMBG -)[12] wurde die Abgabenordnung um eine Vorschrift ergänzt, wonach die Finanzbehörden berechtigt sind, Sozialleistungsträgern und Subventionsgebern Tatsachen mitzuteilen, die zur Erstattung von Sozialleistungen führen können oder im Zusammenhang mit einem strafbaren Subventionsbetrug stehen.

Rechtsprechung

Das zweite Urteil des Bundesverfassungsgerichts zur *Neuregelung des Schwangerschaftsabbruchs* vom 28. Mai 1993[13] enthält detaillierte datenschutzrechtliche Festlegungen. Nach der Entscheidung ist die Straffreiheit eines Schwangerschaftsabbruchs dann verfassungsgemäß, wenn die Schwangere zuvor an einer Beratung teilgenommen hat, in der der Versuch unternommen worden ist, sie für das Austragen des Kindes zu gewinnen. Dabei betont das Gericht die Verpflichtung des Gesetzgebers, die Rechtslage insgesamt so zu gestalten, daß es für die Frau nicht naheliegt, die Beratung gar nicht erst anzunehmen und in die Illegalität auszuweichen[14]. Bis zur Neuregelung der Bestimmungen über den Schwangerschaftsabbruch durch den Gesetzgeber hat das Bundesverfassungsgericht deshalb mit Gesetzeskraft angeordnet, daß die schwangere Frau auf ihren Wunsch gegenüber der sie beratenden Person anonym bleiben kann[15]. Die Anordnung enthält außerdem genaue Vorgaben für die Protokollierung des Beratungsgesprächs, bei der keine Daten über die Identität der beratenen Schwangeren zu erheben sind. Auch betont das Bundesverfassungsgericht die Notwendigkeit, die Schwangere davor zu schützen, den Abbruch und ihre Gründe hierfür unter Beeinträchtigung ihres Persönlichkeitsrechts weiteren Personen offenbaren zu müssen. Dies hat Bedeutung sowohl für die Ausgestaltung des Sozialhilfeanspruchs, der auch die Kosten eines Schwangerschaftsabbruchs umfassen kann, als auch für die Frage der Lohnfortzahlung durch den Arbeitgeber[16]. Das Bundesverfassungsgericht empfiehlt dem Gesetzgeber ausdrücklich, alle Verfahren zur staatlichen Gewährung von Schutz und Hilfe für Schwangere möglichst bei einer Behörde, etwa bei der gesetzlichen Krankenversicherung, zusammenzufassen, damit sichergestellt ist, daß die Frau nur einmal ihre Situation darlegen muß. Dies kann allerdings - im Gegensatz zur Beratung - nicht anonym geschehen[17].

In seinem Beschluß vom 24. Juni 1993[18] hat sich das Gericht zu der Frage geäußert, unter welchen Voraussetzungen eine Straßenverkehrsbehörde vom Führerscheininhaber die *Vorlage eines medizinisch-psychologischen Gutachtens* verlangen darf. Im konkreten Fall hatte die Behörde einen Bürger, der in seinem abgestellten Kraftwagen mit einem Bekannten zum ersten Mal Haschisch geraucht hatte und bei dem die Polizei etwa 0,5 Gramm Haschisch sichergestellt hatte, zur Vorlage eines medizinisch-psychologischen Gutachtens aufgefordert, weil Zweifel an seiner Eignung zum Führen von Kraftfahrzeugen bestünden. Der Betroffene ließ die Untersuchung zwar durchführen, weigerte sich jedoch, das Gutachten der Behörde vorzulegen. Daraufhin wurde ihm die Fahrerlaubnis entzogen. Seine Verfassungsbeschwerde hatte Erfolg. Das Bundesverfassungsgericht betont, daß die Behörde in diesem Fall durch ihr Vorgehen in unverhältnismäßiger Weise in das allgemeine Persönlichkeitsrecht des Bürgers eingegriffen habe. Dieses Recht schütze grundsätzlich vor der Erhebung und Weitergabe von Befunden über den Gesundheitszustand, die seelische Verfassung und den Charakter, und zwar um so intensiver, je näher die Daten der Intimsphäre des Betroffenen stehen, die als unantastbarer Bereich pri-

9 vgl. Anlage 2.1
10 BGBl. 1993 I S. 2353 ff., in Kraft im wesentlichen am 1. Januar 1994
11 BGBl. 1993 I, S. 1770 ff.
12 BGBl. 1993 I, S. 2310 ff.
13 BvF 2/90, 4/92, 5/92, NJW 1993, S. 1751 ff.
14 NJW 1993, S. 1760
15 BGBl. 1993 I, S. 821, Ziff. 3 (4)
16 NJW 1993, S. 1770
17 zur gegenwärtigen Praxis in Berlin siehe unten 4.10
18 1 BvR 689/92, NJW 1993, S. 2365 ff.

vater Lebensgestaltung gegenüber aller staatlicher Gewalt Achtung und Schutz beansprucht[19]. Das Gericht hebt hervor, daß gerade die bei einem psychologischen (im Gegensatz zum medizinischen) Gutachten ermittelten Befunde zum Charakter des Betroffenen seine Selbstachtung ebenso wie sein gesellschaftliches Ansehen berühren. Er müsse die Einzelheiten in einer „verhörähnlichen Situation" offenlegen[20]. Es sei ein unverhältnismäßiger Eingriff in das Persönlichkeitsrecht, bereits bei erstmaligem Haschischkonsum eine derart einschneidende Untersuchung zu verlangen, zumal bereits durch Harn-, Blut- oder Haaruntersuchungen hätte geklärt werden können, ob der Untersuchte in Wirklichkeit gewohnheitsmäßiger Haschischkonsument ist. Diese medizinischen Untersuchungsmethoden greifen nach Auffassung des Gerichts wesentlich schonender in das allgemeine Persönlichkeitsrecht ein und sind daher vorrangig anzuwenden.

Bemerkenswert ist eine Entscheidung des Bundesgerichtshofs in Strafsachen vom 15. Dezember 1992[21], in der es um die Verwertbarkeit von Auskünften der TELEKOM über die mit einem *Mobiltelefon* (Autotelefon) geführten Gespräche für Zwecke eines *Strafverfahrens* ging. Im Mobilfunkverkehr speichert die TELEKOM Verbindungsdatensätze, die neben Datum, Uhrzeit, Zielrufnummer und Anzahl der Gebühreneinheiten auch Daten über die örtlichen Funkvermittlungsstellen enthalten, in deren Bereich ein Telefongespräch begonnen und beendet worden ist. Im konkreten Fall waren insbesondere die Ortsangaben für das Strafverfahren, in dem der Betroffene wegen Betruges und räuberischer Erpressung angeklagt war, von Bedeutung, weil sie zu den Tatorten in Beziehung gesetzt werden konnten. Der Bundesgerichtshof hielt eine Verwertung der Auskünfte der TELEKOM nach § 12 Fernmeldeanlagengesetz im Strafverfahren für zulässig, ohne darauf einzugehen, daß gegen die Verfassungsmäßigkeit dieser Vorschrift unter den geänderten Bedingungen der digitalen Vermittlungstechnik erhebliche Bedenken bestehen.

Aus diesem Grund hatten sowohl die Konferenz der Datenschutzbeauftragten des Bundes und der Länder schon 1991[22] als auch der Bundesrat in seinem Beschluß vom 27. September 1991[23] den Gesetzgeber aufgefordert, die Reichweite dieser Befugnis zu Eingriffen in das Fernmeldegeheimnis zu beschränken. Nach seinem gegenwärtigen Wortlaut läßt das Fernmeldeanlagengesetz nämlich Auskünfte über den Fernmeldeverkehr bereits bei Bagatellstraftaten zu. Der Bundesgerichtshof scheint zudem im Gegensatz zum Fangschaltungsbeschluß des Bundesverfassungsgerichts vom 25. März 1992[24] die Speicherung von Gesprächsdaten zum Zwecke der Gebührenberechnung und des Gebührennachweises durch „betriebsbedingte immanente Schranken" des Fernmeldegeheimnisses als gerechtfertigt anzusehen.

Datenschutz in Europa weiter auf der Kriechspur

Ein Jahr nach dem Inkrafttreten des *Europäischen Binnenmarktes* am 1. Januar 1993 und trotz des Inkrafttretens des *Maastrichter Vertrages über die Europäische Union*[25] am 1. November 1993 tritt die Harmonisierung des Europäischen Datenschutzrechts nach wie vor auf der Stelle. Die Beratungen in der Arbeitsgruppe des Europäischen Rates über den von der Kommission gemachten *„Geänderten Vorschlag für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*[26]" sind noch immer nicht abgeschlossen und gestalten sich sehr langwierig.

Der Grund dafür liegt zum einen in der unterschiedlichen Ausgangslage in den Mitgliedstaaten der Europäischen Union, die - soweit sie innerstaatlich überhaupt ein allgemeines Datenschutzrecht kennen - sehr unterschiedliche Strukturen des materiellen Datenschutzes und der Datenschutzkontrolle aufweisen; zum anderen versuchen die Vertreter der Mitgliedstaaten offenbar zunehmend, ihr jeweiliges nationales Datenschutzrecht auch auf der europäischen Ebene festschreiben zu lassen. Schließlich üben international tätige private Datenverarbeiter (z. B. Kreditkartengesellschaften und Direktwerbeunternehmen) starken Druck auf die Unionsorgane aus, um die im Richtlinienentwurf enthaltenen moderaten Beschränkungen der privaten Datenverarbeitung noch weiter zu verwässern. Dadurch droht der Richtlinienvorschlag sein Ziel zu verfehlen, einen datenschutzrechtlichen Mindeststandard für die Europäische Union festzulegen, der von den Mitgliedstaaten durchaus innerstaatlich zu Gunsten der Bürger überschritten werden kann, soweit dadurch der zwischenstaatliche Datenaustausch nicht beschränkt wird.

Erstaunlicherweise hat sich auch die Bundesregierung gemeinsam mit den Vertretern Dänemarks, Großbritanniens und Irlands inzwischen an dem Versuch beteiligt, in der Ministerratsarbeitsgruppe den Richtlinienvorschlag der Kommission zu Lasten des Bürgers zu verändern. So soll nach einem gemeinsamen Vorschlag dieser vier Regierungen die wichtige Erhebungsphase aus dem Anwendungsbereich der Richtlinie ebenso herausfallen wie der gesamte Sicherheits-, Finanz- und Justizbereich. Dabei gehört die Entwicklung einer engen Zusammenarbeit in den Bereichen Justiz und Inneres gerade zu den ausdrücklichen Zielen der Europäischen Union nach dem Vertrag von Maastricht.

Zudem hat die Kommission inzwischen ihrerseits in einem der Bereiche, die nach dem Willen der Bundesregierung aus der allgemeinen Datenschutzrichtlinie ausgeklammert werden sollen, einen Vorschlag gemacht, der zu einer gemeinschaftsweiten Speicherung von personenbezogenen Daten führen soll. Auf der Grundlage einer unmittelbar als innerstaatliches Recht geltenden Verordnung des Rates der Europäischen Union soll ein *Zollinformationssystem (ZIS)* errichtet werden[27]. Das ZIS soll aus einer zentralen Datenbank bestehen, die über Terminals von allen Mitgliedstaaten und der Kommission aus zugänglich ist. Es soll die Verhinderung, Ermittlung und Bekämpfung von Handlungen, die den europäischen Zoll- und Agrarregelungen zuwiderlaufen „bzw. zuwiderzulaufen scheinen", unterstützen und die Effizienz der Zusammenarbeit zwischen den zuständigen Behörden steigern. Dieser Verordnungsvorschlag verdeutlicht, daß die allgemeine Datenschutzrichtlinie in dem Maße an Bedeutung verliert, wie vordringliche speziellere Probleme des Datenaustauschs zwischen den Mitgliedstaaten und den Organen der Europäischen Union bereichsspezifisch geregelt werden.

Gemäß einem Auftrag, den der Europäische Rat von Maastricht bei der Unterzeichnung des Vertrages über die Europäische Union am 15. Dezember 1991 erteilt hatte, hat die Kommission einen *Bericht über den Zugang der Öffentlichkeit zu Dokumenten, die sich im Besitz der Gemeinschaftsorgane befinden,* vorgelegt[28]. Hintergrund dieses Berichtes ist die in der Erklärung von Maastricht zum Ausdruck kommende politische Absicht, die Entscheidungsfindung in den europäischen Gremien für den Bürger transparenter und das Handeln der Gemeinschaft bürgernäher zu gestalten. Der Bericht der Kommission macht deutlich, daß sie selbst durch eine Reihe von Maßnahmen ihre Arbeit durchschaubarer gestalten will und die übrigen Organe der Union ebenso wie die Mitgliedstaaten auffordert, gemeinsam ein Konzept für den freien Zugang der Bürger zu Informationen zu entwickeln, das zumindest einen gewissen Mindeststandard für die Europäische Union enthält[29]. Diese Initiative für einen verbesserten allgemeinen Zugang zu den Informationen bei den Unionsorganen und in den Mitgliedstaaten ist zu begrüßen. „Bürgernähe" bleibt ein leeres Schlagwort, wenn die Verwaltung weiter vom Grundsatz der Geheimhaltungsbedürftigkeit ihres Handelns ausgeht und dem Bürger den Zugang zu allgemeinen Informationen, die keine Daten zu seiner Person enthalten, verweigert.

Das Beispiel der *Richtlinie über den freien Zugang zu Informationen über die Umwelt*[30], die noch immer ihrer Umsetzung in innerstaatliches deutsches Recht harrt, verdeutlicht die Wichtigkeit des

19 BVerfG NJW 1993, S. 2365
20 NJW 1993, S. 2366
21 5 StR 394/92, CuR 1993, S. 709 f.
22 Jahresbericht 1991, Anlage 2.2
23 BR-Drs. 416/91
24 vgl. dazu Jahresbericht 1992, 1.1
25 BGBl. 1992 II, S. 1251 ff.
26 KOM (92) 422 endg.-SYN 287
27 Geänderter Vorschlag für eine Verordnung des Rates über die gegenseitige Amtshilfe der Verwaltungsbehörden der Mitgliedstaaten und die Zusammenarbeit dieser Behörden mit der Kommission im Hinblick auf die ordnungsgemäße Anwendung der Zoll- und Agrarregelungen KOM (93) 350 endg. - SYN 450 - vom 1. September 1993, BT-Drs. 12/6173
28 Mitteilung an den Rat, das Parlament und den Wirtschafts- und Sozialausschuß (93/C 156/05), abgedruckt in: Datenschutz und Datensicherung 1993, S. 572 ff.
29 DuD 1993, S. 573
30 vgl. Jahresbericht 1992, 1.1

freien Informationszugangs in einem speziellen Bereich. Ein Recht auf freien Zugang zu Informationen der öffentlichen Verwaltung muß natürlich mit den Regeln über den Schutz der informationellen Selbstbestimmung anderer Bürger verzahnt werden. Allerdings - darauf haben wir wiederholt hingewiesen[31] - schließt informationelle Selbstbestimmung ein allgemeines Informationszugangsrecht nicht von vornherein aus. Auch die Europäische Kommission will dem allgemeinen Informationszugangsrecht nicht generell den Vorrang vor der informationellen Selbstbestimmung des Bürgers einräumen[32].

1.2 Datenschutz in Berlin

Bereichsspezifischer Datenschutz weiter verbessert

Sieht man von dem im wesentlichen bereits 1992 erörterten und Anfang des Jahres in Kraft getretenen Gesetz über die Schaffung bereichsspezifischer Regelungen für die Verarbeitung personenbezogener Daten (Artikelgesetz) ab, ist das wichtigste Landesgesetz mit datenschutzrechtlichen Regelungen, das im Berichtszeitraum verabschiedet wurde, zweifellos das *Gesetz über die Sicherung und Nutzung von Archivgut des Landes Berlin (Archivgesetz des Landes Berlin - ArchGB)*[33], das am 9. Dezember 1993 in Kraft trat. Damit ist in Berlin als einem der letzten Bundesländer eine Rechtsgrundlage für das Archivwesen geschaffen und eine der ältesten Forderungen des Berliner Datenschutzbeauftragten erfüllt worden.

Sowohl für historisch interessierte Bürger und Wissenschaftler als auch für die Verwaltung ist damit Rechtssicherheit in einem zentralen Bereich des Umgangs mit personenbezogenen Unterlagen, die bei öffentlichen Stellen Berlins entstanden sind, geschaffen worden. An der Formulierung des Gesetzestextes war der Berliner Datenschutzbeauftragte bereits in einem frühen Stadium beteiligt. Das Landesarchivgesetz orientiert sich in weiten Teilen am Bundesarchivgesetz, enthält jedoch in einzelnen Punkten abweichende Regelungen. So sind insbesondere die *Schutzfristen,* nach deren Ablauf das Archivgut von jedermann oder speziell für Zwecke der zeitgeschichtlichen Forschung genutzt werden kann, kürzer als im Bundesrecht vorgesehen. Diese Regelungen können im Hinblick auf die Forschungsfreiheit akzeptiert werden, auch wenn sie den Persönlichkeitsschutz Verstorbener verkürzen, zumal der Gesetzgeber gleichzeitig für den Schutz personenbezogener Daten, insbesondere solcher Informationen, die Berufs- oder besonderen Amtsgeheimnissen unterliegen, Sorge getragen hat.

Generell sind alle Behörden, Gerichte und sonstige Stellen des Landes Berlin verpflichtet, sämtliche Unterlagen, die zur Erfüllung ihrer Aufgaben nicht mehr benötigt werden, in der Regel *spätestens* 30 Jahre nach ihrer Entstehung auszusondern und unverändert dem Landesarchiv anzubieten, soweit nicht Rechtsvorschriften andere Fristen bestimmen. Dies gilt auch für Unterlagen mit personenbezogenen Daten. Diese Vorschrift sollte die Verwaltung nicht dahingehend mißverstehen, daß sie personenbezogene Daten stets 30 Jahre lang aufbewahren darf. Vielmehr richtet sich die zulässige Aufbewahrungsdauer nach speziellen Rechtsvorschriften, und soweit solche nicht vorhanden sind, nach der konkreten Erforderlichkeit für die Erfüllung der jeweiligen Verwaltungsaufgabe.

Das neue Archivgesetz ergänzt auch das Berliner Datenschutzgesetz in einem wichtigen Punkt. Personenbezogene Daten, deren Speicherung zur Erfüllung der Verwaltungsaufgabe nicht mehr erforderlich sind, müssen nicht mehr - wie nach altem Datenschutzrecht vorgeschrieben - sofort gelöscht, sondern vielmehr zunächst dem Landesarchiv angeboten werden. Handelt es sich dabei um personenbezogene Daten, deren Speicherung von vornherein unzulässig war oder deren Löschung der Betroffene inzwischen verlangen kann, so dürfen die Unterlagen nur mit Einwilligung des Betroffenen dem Landesarchiv überantwortet werden (§ 17 Abs. 4 Satz 2 BlnDSG). Das Landesarchiv entscheidet in jedem Fall darüber, welche der angebotenen Unterlagen als archivwürdig übernommen werden. Diejenigen personenbezogenen Unterlagen, deren Übernahme das Landesarchiv ablehnt oder über deren Übernahme es nicht innerhalb von 12 Monaten seit dem Angebot entscheidet, sind zu löschen bzw. zu vernichten.

Eine Sonderstellung nehmen die *Datenbestände ehemaliger Einrichtungen der DDR* ein, die es auch in den östlichen Bezirken Berlins noch immer gibt. Die Datenschutzgesetze der anderen neuen Bundesländer enthalten durchweg eine Regelung über den Umgang mit diesen Datenbeständen, die sich zum Teil im Gewahrsam öffentlicher Stellen, zum anderen Teil aber auch privater Stellen befinden. Letzteres gilt vor allem für die Datenbestände der ehemaligen volkseigenen Betriebe, die bisher - auch nach der Privatisierung - zum großen Teil von der Treuhandanstalt in Depots aufbewahrt und verwaltet wurden. Das Berliner Datenschutzgesetz, das kurz vor der Vereinigung novelliert worden war, enthielt keine Sonderregelungen für Altdatenbestände der ehemaligen DDR. Deshalb wurde auf Vorschlag des Berliner Datenschutzbeauftragten eine entsprechende Vorschrift in das neue Landesarchivgesetz aufgenommen (§ 5). Sie sieht vor, daß personenbezogene Daten aus ehemaligen Einrichtungen der DDR, die vor der Vereinigung nach ihrer Zweckbestimmung überwiegend für Verwaltungsaufgaben verarbeitet wurden, die nach dem Grundgesetz von öffentlichen Stellen des Landes wahrzunehmen sind, derjenigen Stelle zustehen, die für die Verwaltungsaufgabe jetzt zuständig ist. Soweit private Stellen derartige Unterlagen im Gewahrsam haben, müssen sie sie an die zuständige öffentliche Stelle herausgeben. Davon ist der Berliner Datenschutzbeauftragte zu unterrichten. Bei hinreichenden Anhaltspunkten dafür, daß die Herausgabe- und Anzeigepflicht verletzt werden, muß der Private dem Berliner Datenschutzbeauftragten wie eine öffentliche Stelle Auskunft zu seinen Fragen und Einsicht in alle Unterlagen und Akten gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, diese Unterlagen und Akten herausgeben und dem Datenschutzbeauftragten jederzeit Zutritt in alle Geschäftsräume gewähren. Diese Erstreckung der Kontrollbefugnisse des Datenschutzbeauftragten auf nichtöffentliche Stellen ist schon deshalb sachgerecht, weil sie der Sicherung und Herausgabe von personenbezogenen Daten dient, die nach heutigem Recht einer öffentlichen Stelle zustehen.

Am 22. Juli 1993 ist das *Gesetz über den Rettungsdienst für das Land Berlin (Rettungsdienstgesetz - RDG -)*[34] in Kraft getreten, das erstmals auch die Verarbeitung personenbezogener Daten bei der Notfallrettung und dem Krankentransport regelt (§ 4). Diese Vorschriften gelten sowohl für die Berliner Feuerwehr, die die Notfallrettung im Regelfall als Ordnungsaufgabe wahrnimmt, als auch für die privaten Hilfsorganisationen, denen die Notfallrettung daneben übertragen werden kann und die in aller Regel den Krankentransport durchführen. Die Datenübermittlungsbefugnisse des Rettungsdienstgesetzes treten an die Stelle einer Vorschrift im Berliner Datenschutzgesetz (BlnDSG), die entsprechend gestrichen werden konnte (§ 34 Abs. 3 Nr. 2 BlnDSG). Bei den Beratungen des Rettungsdienstgesetzes wurden wir frühzeitig beteiligt und unsere Empfehlungen sind weitgehend berücksichtigt worden.

Durch das am 31. Januar 1993 in Kraft getretene *Gesetz über die Schaffung bereichsspezifischer Regelungen für die Verarbeitung personenbezogener Daten (Artikelgesetz)*[35] wurden für weite Verwaltungsbereiche erstmals Aufgabenzuweisungen und generelle Befugnisse zur Verarbeitung personenbezogener Daten festgelegt[36]. Diese gesetzlichen Verarbeitungsbefugnisse waren zum großen Teil unvollständig, weil sie den genauen Umfang der Datenverarbeitung nicht erkennen ließen. Dies beruhte vielfach darauf, daß die Fachverwaltungen sich nicht in der Lage gesehen hatten, rechtzeitig vor Ablauf der - insgesamt dreimal verlängerten - Übergangsvorschrift des § 34 Abs. 1 BlnDSG entsprechende

31 Jahresbericht 1990, 1.2

32 Dagegen haben die Bundesratsausschüsse in ihrer Stellungnahme zur Vorlage der Kommission (BR-Drs. 409/93) die Befürchtung geäußert, daß der Informationszugangsanspruch prinzipiell uneingeschränkt sein solle, und ihn deshalb abgelehnt

33 GVBl. 1993, S. 576 ff.

34 GVBl. 1993, S. 313 ff.

35 GVBl. 1993, S. 40 ff.

36 vgl. Jahresbericht 1992, 1.2

Gesetzentwürfe vorzulegen, die den Umfang der Datenverarbeitung genauer umschrieben. Zudem ist es angemessener, umfangreiche Datenkataloge in einer - flexibleren - Verordnung statt im Gesetz selbst festzulegen.

Der Gesetzgeber verpflichtete diese Verwaltungen daher im Artikelgesetz, bis zum 31. Dezember 1993 durch Rechtsverordnungen festzulegen, welche Daten für welche Zwecke verarbeitet und wie lange sie gespeichert bleiben dürfen. In der parlamentarischen Beratung ist dies treffend als „Nachspielzeit" für die Verwaltung bezeichnet worden. Ein Teil der Verwaltungen hat die Frist erfolgreich genutzt. Bis zum Ende des Jahres 1993, also rechtzeitig, traten folgende Rechtsverordnungen für folgende Bereiche in Kraft:

- die Berufsbildung im öffentlichen Dienst[37],
- die Verarbeitung von Studentendaten an Hochschulen[38],
- das Haushaltswesen[39],
- das Friedhofswesen[40],
- die Nutzung von Verwaltungsdaten durch das Statistische Landesamt[41],
- die Pflegeleistungen[42].

Die im Artikelgesetz vorgesehenen Regelungen zur Datenverarbeitung im Bereich der Stadtreinigung finden sich im *Gesetz über die Vermeidung und Entsorgung von Abfällen in Berlin (Landesabfallgesetz - LAbfG)* (§ 26)[43].

In anderen Bereichen ist es nur gelungen, vor Ablauf der im Artikelgesetz genannten Frist bis zum 31. Dezember 1993 Entwürfe für die erforderlichen bereichsspezifischen Vorschriften zur Verarbeitung personenbezogener Daten vorzulegen. Dabei handelt es sich um die Datenverarbeitung

- in Schulen,
- im öffentlichen Gesundheitsdienst,
- in der Bewährungshilfe für Jugendliche und Heranwachsende,
- bei den Eigenbetrieben,
- bei der Deutschen Dienststelle (WASt) für die Benachrichtigung der nächsten Angehörigen von Gefallenen der ehemaligen Deutschen Wehrmacht und
- für das Emissionskataster nach dem Bundesimmissionsschutzgesetz.

Die befristete Regelung der Datenverarbeitung im *Ausführungsgesetz zum Baugesetzbuch,* die die Datenverarbeitung für Zwecke der Stadtplanung geregelt hat, ist zum 31. Dezember 1993 außer Kraft getreten, ohne daß das noch immer in der Beratung befindliche Gesetz über die Datenverarbeitung für Zwecke der Stadtplanung inzwischen verabschiedet worden wäre. Auch die in § 7 a Satz 3 *Kita-Kostenbeteiligungsgesetz* in der Fassung vom 27. Mai 1993 enthaltene Verpflichtung zum Erlaß einer Rechtsverordnung über Art und Umfang der Verarbeitung personenbezogener Daten ist bisher nicht erfüllt worden.

Die bereits im Artikelgesetz für bestimmte Verwaltungsbereiche enthaltenen präziseren Grundlagen für die Verarbeitung personenbezogener Daten bilden zusammen mit den jetzt in Kraft getretenen Rechtsverordnungen eine deutlich verbesserte Grundlage für den bereichsspezifischen Datenschutz in Berlin. Der Bürger kann jetzt in den genannten Bereichen aufgrund klarer Rechtsvorschriften erkennen, in welchem Umfang seine personenbezogenen Daten von der Verwaltung für welche Zwecke verarbeitet werden. Dies ist ein entscheidender Schritt in Richtung auf die vom Bundesverfassungsgericht im Volkszählungsurteil geforderte Transparenz, denn der Bürger kann anhand des geltenden Rechts feststellen, welche öffentliche Stelle Berlins was, wann und bei welcher Gelegenheit über ihn wissen darf. Zugleich ist erst jetzt in diesen Bereichen die notwendige Ergänzung zum Berliner Datenschutzgesetz geschaffen worden, das seinerseits besondere Verarbeitungsbefugnisse für die einzelnen Verwaltungszweige voraussetzt und selbst nicht ersetzen kann.

Die verbesserte *Durchschaubarkeit und Kontrollierbarkeit* staatlicher Datenverarbeitung in diesen Bereichen ist sehr viel höher zu bewerten als das Schlagwort von der *„Deregulierung"*, das gegen das Berliner Datenschutzgesetz und die von ihm ausgelöste bereichsspezifische Datenschutzgesetzgebung angeführt wurde. Es gibt zweifellos in unserer Rechtsordnung immer wieder Rechtsvorschriften, die sich bei genauerem Hinsehen als zu perfektionistisch oder insgesamt überflüssig erweisen. Es sollte jedoch nicht vergessen werden, daß die bereichsspezifische Datenschutzgesetzgebung die Konkretisierung eines Grundrechts, nämlich das der informationellen Selbstbestimmung, zum Gegenstand hat.

Wir teilen deshalb nicht die in der Stellungnahme des Senats zum Jahresbericht 1992[44] geäußerte Auffassung, eine Änderung des § 6 BlnDSG, der den Erlaß von bereichsspezifischen Datenverarbeitungsbefugnissen voraussetzt, sei dringend geboten. Diese Vorschrift setzt konsequenter als die Datenschutzgesetze des Bundes und der übrigen Länder (mit Ausnahme Brandenburgs) die Vorgaben um, die das Bundesverfassungsgericht in seiner Rechtsprechung zum Grundrecht auf Datenschutz gemacht hat. Auch ist unverkennbar, daß selbst der Bundesgesetzgeber zunehmend besondere Datenverarbeitungsbefugnisse in bereichsspezifische Gesetze aufnimmt und die Bedeutung des Bundesdatenschutzgesetzes als eigenständige Verarbeitungsgrundlage abnimmt. Die allgemeinen Datenschutzgesetze sind auch wenig geeignet, auf Dauer eine tragfähige Grundlage für die differenzierten Informationsbedürfnisse der jeweiligen Fachverwaltung zu bieten.

Soweit es um die Ausführung von Landesrecht geht, besteht deshalb keinerlei Veranlassung, § 6 BlnDSG in seiner gegenwärtigen Fassung in Frage zu stellen. Der Landesgesetzgeber hat mit dieser Vorschrift sich selbst ein Gesetzgebungsprogramm gegeben, das nicht mit dem Schlagwort „Normenflut" abqualifiziert werden sollte, weil es zur Herstellung größtmöglicher Transparenz der Datenverarbeitung in den öffentlichen Stellen des Landes Berlin beiträgt.

Soweit die Anwendung von Bundesrecht in Frage steht, auf die der geltende § 6 BlnDSG seinem Wortlaut nach ebenfalls anzuwenden ist, ergeben sich allerdings in der Praxis Probleme[45]. Auch wenn der Landesgesetzgeber zu einer Reihe von Bundesgesetzen Ausführungsgesetze erlassen hat, die die Verarbeitung personenbezogener Daten regeln, halten wir dies nicht mehr in jedem Fall für zwingend. Wir haben deshalb gegenüber den Senatsverwaltungen für Inneres und Justiz eine Auslegung des § 6 Abs. 1 BlnDSG befürwortet, nach der öffentliche Stellen Berlins, die Bundesrecht auszuführen haben, personenbezogene Daten verarbeiten dürfen, wenn diese zur Erfüllung der ihnen gesetzlich zugewiesenen Aufgaben erforderlich sind und wenn diese Datenverarbeitung zumindest den Anforderungen des ersten und zweiten Abschnitts des Bundesdatenschutzgesetzes (BDSG) genügt. Dies gilt allerdings nur für diejenigen Phasen der Datenverarbeitung, für die das Berliner Datenschutzgesetz ausdrücklich auf seinen § 6 Abs. 1 verweist (Erhebung; Weiterverarbeitung der Daten zu Zwecken, für die sie nicht erhoben oder gespeichert worden sind, insbesondere ihre Übermittlung an andere öffentliche Stellen, die andere Zwecke als den Erhebungzweck verfolgen).

37 Azubi-Auswahl VO-Verwaltungsdienst vom 19. November 1993, GVBl. 1993, S. 596
38 Studentendatenverordnung - StudDatVO - vom 11. Dezember 1993, GVBl. 1993, S. 628 f.
39 VO über die Verarbeitung personenbezogener Daten des Haushaltwesens vom 14. Dezember 1993, GVBl. 1993, S. 630
40 VO über die Verarbeitung personenbezogener Daten im Bereich der landeseigenen Friedhöfe Berlins vom 16. Dezember 1993, GVBl. 1993, S. 645
41 VO über die Übermittlung von Daten aus dem Verwaltungsvollzug an das Statistische Landesamt (Übermittlungs-VO) vom 20. Dezember 1993, GVBl. 1993, S. 661
42 VO über die Verarbeitung personenbezogener Daten nach § 10 a des Gesetzes über Pflegeleistungen vom 21. Dezember 1993, GVBl. 1993, S. 662
43 GVBl. 1993, S. 651 ff.
44 Drs. 12/3081 (neu), S. 10 f.
45 vgl. Jahresbericht 1992, 1.2

Zusammenarbeit mit dem Land Brandenburg

Im Berichtszeitraum sind zwei weitere Staatsverträge zwischen den Ländern Berlin und Brandenburg in Kraft getreten, nämlich der *Staatsvertrag über die Feuersozietät Berlin Brandenburg und die Öffentliche Lebensversicherung Berlin-Brandenburg*[46] und der Staatsvertrag über die Bildung der Akademie der Künste in der Trägerschaft der Länder Berlin und Brandenburg[47]. Während die rechtsfähigen Anstalten des öffentlichen Rechts „Feuersozietät Berlin-Brandenburg" und „Öffentliche Lebensversicherung Berlin-Brandenburg" ihren Sitz in Berlin und Potsdam haben, hat die rechtsfähige Körperschaft des öffentlichen Rechts „Akademie der Künste" ihren Sitz in Berlin. Die Datenschutzkontrolle bei allen drei öffentlichen Stellen werden wir in enger Abstimmung mit dem Brandenburgischen Datenschutzbeauftragten durchführen[48].

Der im Oktober 1993 vorgelegte gemeinsame Zwischenbericht der Senatskanzlei des Landes Berlin und der Staatskanzlei des Landes Brandenburg zum *Staatsvertrag der Länder Berlin und Brandenburg über die Bildung eines gemeinsamen Bundeslandes* enthielt bereits wesentliche Elemente des *Neugliederungsstaatsvertrages,* der ursprünglich Ende 1993 vorgelegt werden sollte. Danach gehört das Datenschutzrecht zu denjenigen Rechtsvorschriften, die vorrangig in beiden Ländern vereinheitlicht werden sollen. Unabhängig davon, ob es letztlich zu einer Vereinigung der beiden Länder kommen wird, ist eine Harmonisierung in diesem Bereich schon deshalb wünschenswert, weil zunehmend neue gemeinsame Institutionen oder zumindest gemeinsame Datensammlungen länderübergreifend entstehen werden, die datenschutzrechtlich gerade auch im Interesse der Bürger einheitlich beurteilt und kontrolliert werden sollen.

Im Entwurf eines dem Zwischenbericht beigefügten *Organisationsstatuts für das gemeinsame Land* ist vorgesehen, daß die Position des Landesbeauftragten für den Datenschutz verfassungsrechtlich gesichert sein soll. Dies entspricht den Vorgaben des Bundesverfassungsgerichts, das im Volkszählungsurteil die Bedeutung unabhängiger Datenschutzbeauftragter für einen effektiven und vorbeugenden Schutz des Rechts auf informationelle Selbstbestimmung betont hat.

Offengelassen wird im Organisationsstatut allerdings die *organisatorische Stellung des Landesbeauftragten für den Datenschutz.* Die Einordnung in den ersten Abschnitt „Der Landtag" läßt vermuten, daß der Landesbeauftragte wie in Brandenburg als eine Organisationseinheit des Landtages errichtet werden soll. Demgegenüber übt zwar die Präsidentin des Abgeordnetenhauses auch in Berlin die Dienstaufsicht über den Berliner Datenschutzbeauftragten aus; die Behörde selbst ist aber als eigenständige oberste Landesbehörde eingerichtet.

Diese Berliner Lösung ist aus unserer Sicht vorzuziehen. Neben dem Umstand, daß dadurch statusrechtliche Probleme vermieden werden, wie sie in Ländern mit der im Organisationsstatus vorgesehenen Konstruktion aufgetreten sind, hat die Berliner Regelung den Vorteil, daß der Datenschutzbeauftragte Aufgaben mit übernehmen kann, deren Ansiedlung im Parlament schwer oder gar nicht möglich ist.

So hat die Senatsverwaltung für Inneres eine Prüfung angekündigt, ob der Datenschutzbeauftragte nicht die Aufgaben der *Aufsichtsbehörde für den Datenschutz* im Privatbereich und damit gewisse exekutive Funktionen übernehmen kann. Eine derartige Bündelung von Aufgaben läge sicherlich im Interesse der Verwaltungsreform.

Auch im Zusammenhang mit neuartigen Aufgaben auf dem Gebiet des Informationsrechts wurde vorgeschlagen, dem Datenschutzbeauftragten zusätzliche Aufgaben zuzuweisen, so etwa als Schiedsstelle bei Meinungsverschiedenheiten über den allgemeinen Informationszugang zu Behördenunterlagen oder als „Datentreuhänder" bei geplanten Datenabgleichen. Die organisatorische Stellung als oberste Landesbehörde würde die Übernahme derartiger Aufgaben sehr erleichtern und die Errichtung jeweils neuer Behörden für informationsrechtliche Aufgaben überflüssig machen.

2. Technische Rahmenbedingungen

2.1 Zentral, dezentral, überall - Berliner IuK-Politik im Spiegel der technischen Entwicklung

Informationstechnologische Trends

Bereits in früheren Jahresberichten dargestellte informationstechnologische Trends haben sich im vergangenen Jahr fortgesetzt und noch verstärkt.

Eine weitere Verbesserung des Preis-Leistungs-Verhältnisses, die sich bisher als Saldo starker Preisreduzierungen für Hardware und eher steigenden Preisen für aktuelle Software ergab, resultiert daraus, daß sich inzwischen ein Trend zur *Verbilligung von Software* abzeichnet. Diese Entwicklung betrifft sowohl Arbeitsplatz- und Mehrplatzsysteme als auch Großrechner mit proprietären Betriebssystemen. Letztere erreichen Leistungsbereiche, die von vielen einzelnen Anwendern kaum noch vollständig ausgelastet werden können.

Die *Miniaturisierung der Hardware* bringt immer kleinere Rechner mit immer größerer Leistungsfähigkeit und immer höherem Bedienungskomfort hervor. Laptops und Notebooks werden gewohnte Werkzeuge. Der Trend zum Westentaschenformat ist abzusehen. Außendienstler mit Pocket-PC und Handy-Funktelefon sind auch in der öffentlichen Verwaltung vorstellbar.

Die Leistungsfähigkeit und Einsatzbreite von *Chipkarten* steigt durch die Möglichkeit, immer mehr Speicherkapazitäten und Prozessorleistung selbst auf dem Raum einer scheckkartengroßen Plastikkarte unterzubringen[49].

Neben der immer komplexer werdenden Standardsoftware „von der Stange", die die Eigenprogrammierung bei den anwendenden Organisationen zunehmend überflüssig macht, spielen *Software-Werkzeuge* zur flexiblen Anpassung von Standardsoftware an jeweilige organisatorische Rahmenbedingungen eine größere Rolle.

Forschung und Entwicklung sowie die internationale Normierung im Bereich der Informationstechnik konzentrieren sich weiter verstärkt auf die *Vernetzung* von Systemen und damit auf die Kommunikation zwischen Rechnern.

Diese technologischen Entwicklungslinien bewirken Veränderungen von IuK-Einsatzstrategie und Organisation in den Verwaltungen. Alte Datenverarbeitungs-Berufsbilder verschwinden, neue entstehen, alte hierarchische Strukturen brechen auf, neue entwickeln sich.

Betreiber von Großrechnern müssen zur Auslastung ihrer Systeme zusätzliche Anwendungen akquirieren. Soweit dieses organisationsintern nicht mehr möglich ist, wird die IT-Dienstleistung auch anderen Organisationen angeboten, die dafür auf ein eigenes Rechenzentrum verzichten können *(Outsourcing).* Anwender schaffen ihre Großrechner ab und realisieren ihre Verfahren auf Rechnern mit Standardbetriebssystemen, die weltweit verbreitet sind und für die daher ein breites Softwareangebot zur Verfügung steht *(Downsizing).*

Bisher nicht automatisierte kleinere Verfahren werden durch *PC-Einsatz* automatisiert. Um die Verfahren allen damit beschäftigten Mitarbeitern am Arbeitsplatz zugänglich zu machen, werden die PCs vernetzt. Dies erzwingt auf lokaler Ebene die Zentralisierung der Datenhaltung auf Servern, um einerseits die Daten nicht mehrfach vorhalten zu müssen und andererseits jedem Benutzer die gleiche Daten- und Programmbasis bereitzustellen. Die Verbesserung des Preis-Leistungs-Verhältnisses erlaubt es, neben dem Anwendungsverfahren weitere nützliche Funktionen an den Arbeitsplätzen verfügbar zu machen, etwa Textverarbeitung und Bürokommunikation. Des weiteren erlaubt die Lei-

46 GVBl. 1993, S. 305 ff.
47 GVBl. 1993, S. 379 ff.
48 vgl. schon Jahresbericht 1992, 1.2

49 vgl. 2.3

stungsstärke moderner Server, lokale Netze zusammenzuschalten, so daß über solche Netze auf diverse Fachanwendungen und auf Büroinformations- und -kommunikationsdienstleistungen zurückgegriffen werden kann.

Die beiden letztgenannten Entwicklungslinien treffen zusammen und führen zur *lokalen Zentralisierung* der Datenverarbeitung großer, räumlich verteilter Organisationen, für die die Berliner Verwaltung ein gutes Beispiel ist. Von den einzelnen isolierten Personalcomputern geht der Weg über PC-Netze hin zu heterogenen lokalen Netzwerken (LAN - Local Area Network) mit UNIX-Servern und PCs als Arbeitsplatzrechner (Client-Server-Systeme). Um die Büro- und Datenkommunikation und den Zugriff auf spezielle Verfahren und Datensammlungen organisationsübergreifend zu ermöglichen, werden die lokalen Netze untereinander und ggf. mit zentralen Großrechnern über *Datenkommunikationsnetze* stadtweit (MAN - Metropolitan Area Network), sogar landes- und weltweit (WAN - Wide Area Network) vernetzt.

Dieser Trend führt zu einem offensichtlichen Rückgang der einzeln, also netzunabhängig betriebenen Personalcomputer in größeren Organisationen. Wegen des Umfangs der automationsunterstützten Arbeitsgebiete müssen meist mehrere Mitarbeiter mit den gleichen Verfahren und mit der gleichen Datenbasis arbeiten, so daß der Rechnerzugriff durch eine Vernetzung verteilt werden muß.

Diese Entwicklungen zeigen, daß die traditionelle Gegenüberstellung von zentraler und dezentraler Datenverarbeitung nicht mehr sachgerecht ist. Dezentralisierende überlagern sich mit zentralisierenden Tendenzen. Die Datenverarbeitung der Zukunft ist weder zentral noch dezentral, alles ist vielmehr überall verfügbar.

Herausforderungen für den Datenschutz

Die beschriebenen Trends haben Auswirkungen auf den Datenschutz und auf die Datensicherheit. Da sie von anderen Entwicklungszielen bewirkt und vorangetrieben werden als der Verbesserung der informationstechnischen Sicherheit und der Förderung der informationellen Selbstbestimmung, stellen sie eine Herausforderung dar, denen sich die Datenschutzbeauftragten und die ansonsten mit Datenschutz und informationstechnischer Sicherheit befaßten Institutionen stellen müssen.

Bereits im Vorjahr haben wir die Folgen des Trends zum *Downsizing* näher beschrieben:

- vermehrter Einsatz von Systemen mit geringem IT-Sicherheitsniveau,
- Entprofessionalisierung der sicherheitsrelevanten Aufgaben der Systemverwaltung,
- verstärkte Abhängigkeit von organisationsfremder Sachkompetenz und Leistungsbereitschaft[50].

Outsourcing bedeutet die Übertragung von Datenverarbeitungsfunktionen auf andere Organisationen, damit in der Regel auch die Offenbarung der dabei zu verarbeitenden personenbezogenen Daten. Die datenschutzrechtlich schon immer mögliche Datenverarbeitung im Auftrag in der öffentlichen Verwaltung erhält problematische Dimensionen durch die vermehrte Einschaltung privater Auftragnehmer und durch die Einbeziehung von Verfahren, bei denen Daten verarbeitet werden, die besonderen Berufsgeheimnissen wie der ärztlichen Schweigepflicht unterliegen.

Der Trend zur offenen Vernetzung und zur flexiblen, von genormten Schnittstellen begünstigten Datenkommunikation steht datenschutzrechtlichen Zielsetzungen zur Abschottung personenbezogenen Wissens aufgrund der verfassungsrechtlich gebotenen informationellen Gewaltenteilung prinzipiell entgegen. Es bedarf daher grundsätzlicher Überlegungen zur Bewältigung dieses Gegensatzes, da sonst Infrastrukturen entstehen können, die für die Wahrung des Grundrechtes auf informationelle Selbstbestimmung Risiken beinhalten.

Der Rückgang des Einsatzes von Einzelplatz-PCs ist aus Gründen der informationstechnischen Sicherheit und Ordnungsmäßigkeit als Vorteil zu werten, weil die Notwendigkeit dieser beiden Säulen datenschutzgerechter Datenverarbeitung in lokalen Netzen schon wegen der höheren Ansprüche an eine Benutzerorganisation und -authentisierung bei Mehrbenutzersystemen und an die Transparenz und Koordination der Datenverarbeitung in komplexeren Systemumgebungen eher akzeptiert wird als bei Einzelplatz-PCs.

Informationstechnische Infrastruktur der Berliner Verwaltung

Obwohl die lange geforderte Verwaltungsreform von widerstrebenden Interessen gehemmt wird, wird sie in informationstechnologischer Hinsicht mit Macht vorangetrieben. Wenn einerseits die Verwaltung angesichts der Sparvorgaben zu umfangreichen Personaleinsparungen gezwungen wird, so sollen andererseits die Ziele der Verwaltungsreform, nämlich die Steigerung von Effizienz und Leistungsfähigkeit bei gleichzeitiger Verbesserung der Bürgernähe durch eine technologische Aufrüstung von bisher nicht beobachtetem Umfang gesichert werden. Dies bedarf umfassender Koordination, um die verschiedenen Trends zu erfassen und für die Verwaltungsautomation nutzbar zu machen.

In der Vergangenheit waren die Modelle für eine einheitliche IuK-Politik kurzlebig und von unterschiedlichen Zielvorgaben geprägt. Die ADV-Grundsätze von 1984 und parlamentarische Vorgaben zur Beachtung von Normen und Standards waren lange Zeit die einzigen Richtlinien, die der planenden Verwaltung an die Hand gegeben wurden. So war unvermeidbar, daß sich neben der hergebrachten zentralen Datenverarbeitung mit Großsystemen eine ungeordnete Struktur von mehr oder weniger professionell geplanten und realisierten PC- und PC-Netz-Projekten entwickelte. Dieses war weder wirtschaftlich noch aus Sicht des Datenschutzes begrüßenswert, denn die Verfahren erfüllten die Ansprüche an Ordnungsmäßigkeit, Transparenz und Datensicherheit häufig nicht.

Inzwischen wird verstärkt entgegengewirkt. Insbesondere für die Neuentwicklung und Neueinführung von Verfahren, die bisher nicht automatisiert waren, werden unter der Betreuung des Landesamtes für Informationstechnik (LIT) *Modellprojekte* durchgeführt, bei denen ein Bezirksamt die Federführung und die Vorreiterrolle übernimmt, bis nach Feststellung der Einsatzreife eine Ausbreitung auf alle anderen Bezirke erfolgen kann. Ein solches Projekt ist z. B. die Entwicklung des Lehrer-Informations- und Verwaltungssystems (LIV) im Bezirksamt Wedding[51].

Es werden Projekte zu *Großverfahren* durchgeführt, bei denen über lokale Netze dezentrale Ressourcen an den Arbeitsplätzen verfügbar gemacht werden sollen, die gleichzeitig über das Verwaltungsnetz berlinweit kommunizieren und zentrale Großrechnerleistungen in Anspruch nehmen sollen (z. B. BASIS[52]), aber auch das Fachübergreifende Informationssystem (FIS) im Umweltschutz- und Stadtplanungsbereich, das Automatisierte Haushaltswesen (AHW) und die Integrierte Personalverwaltung (IPV)[53].

Im Bezirksamt Weißensee wird das Projekt *„Modellbezirksamt" (MBA)* realisiert, bei dem die Verbesserung der Bürgernähe durch die Einrichtung eines Bürgerbüros und durch intensiven IuK-Einsatz modellhaft angestrebt wird.

Vom LIT wird ein neues *Verwaltungsnetz* projektiert (Metropolitan Area Network - MAN), das die für die berlinweiten Großverfahren notwendige Datenkommunikation eines Tages tragen soll.

Ebenfalls im LIT wird ein Projekt zur Installation eines *Service- und Administrationszentrums (SAZ)* durchgeführt, von dem aus die Fachverfahrensbetreiber in den Haupt- und Bezirksverwaltungen unter Nutzung des MAN bei der Installation, Konfigurierung und Überwachung ihrer Systeme und lokalen Netze unterstützt werden sollen.

50 Jahresbericht 1992, 2.1

51 siehe Abschnitt 4.5
52 siehe Abschnitt 4.10
53 siehe Abschnitt 4.5

Bei dem vermutlich am weitesten fortgeschrittenen Projekt. BASIS wurde dem Projektmanagement klar, daß die Durchführung mehrerer solcher Großverfahren nebeneinander einer übergeordneten Koordination und Abstimmung auf einheitliche Normen, Standards und Strategien, eines „gemeinsamen Daches" bedarf. Das Parlament hat dann den Anstoß für das Projekt *„Grundlagen der Ausstattung mit IT-Infrastruktur für die Bezirks- und Senatsverwaltungen - GIBES -"* gegeben, das unter großem Zeitdruck die notwendigen Vorgaben für eine einheitliche IuK-Infrastruktur unter Beteiligung namhafter Unternehmensberatungen entwickeln soll.

Das Hauptaugenmerk unserer datenschutzrechtlichen Beratung der Infrastrukturprojekte wurde wegen der datenschutzrechtlichen Relevanz und des relativ fortgeschrittenen Projektstadiums den Projekten Modellbezirksamt und GIBES gewidmet. Das fachbereichsbezogene Projekt BASIS wird unter 4.10 näher behandelt.

Infrastrukturprojekt Modellbezirksamt Weißensee

Ausgangspunkt für dieses Projekt ist der Beschluß des Abgeordnetenhauses vom Juni 1991, im Hinblick auf die Verwaltungseinheit eine einheitliche, bürgernahe und effiziente Verwaltung für das Land Berlin zu schaffen.

Vom Senat wurde dieser Beschluß dahingegehend erweitert, im Ostteil der Stadt ein Modellbezirksamt zu schaffen. Dieses sollte mit seinen Strukturen, seinem bürgerfreundlichen Dienstleistungsangebot und seiner technischen Ausstattung beispielgebend für alle Berliner Bezirke bei der praktischen Umsetzung einer dringend notwendigen Verwaltungsreform sein. Im Ergebnis eines Auswahlverfahrens wurde das Bezirksamt Weißensee zur Realisierung des Projektes ausgewählt.

Mit fortschreitender Präzisierung der Aufgabenstellung kristallisierten sich drei Themen heraus, auf die wir unser besonderes Augenmerk richteten:

- Schaffung einer bedarfsgerechten und leistungsfähigen IT-Infrastruktur für das MBA,
- Auf- und Ausbau eines Bürgeramtes,
- Gestaltung des Bereiches „Soziale Dienste".

Zielrichtung bei der *Schaffung einer bedarfsgerechten, effizienten und zukunftsorientierten IT-Infrastruktur* war von Beginn an, eine *einheitliche Benutzungsoberfläche* für alle Anwender von IuK-Technik einzusetzen. Diese sollte es ermöglichen, sämtliche Funktionen, wie sie bei der täglichen Arbeit in einem Bezirksamt anfallen, so zu integrieren, daß sie sich sowohl hinsichtlich der einzusetzenden Hardware als auch in bezug auf bereits vorhandene bzw. künftig benötigte Software als offen und damit unabhängig vom jeweiligen Hersteller darstellt. Neben den fachspezifischen Anwendungen sollten auch allgemeine Büroaufgaben wie Vorgangsverwaltung, Terminplanung und Informationsaustausch unter dieser Oberfläche realisiert werden können. Nicht zuletzt sollte auch die Administration solch komplexer Systeme möglichst einheitlich und sicher gestaltet werden.

Die Belange des Datenschutzes wurden sowohl beim Teilnahmewettbewerb als auch bei der sich anschließenden beschränkten Ausschreibung eingebracht. Den Datenschutzaspekten wurde bei der Beurteilung der eingehenden Angebote ein hoher Stellenwert zugemessen. Der Anbieter hat den Zuschlag erhalten, dessen Datenschutzkonzeptionen unseren Ansprüchen am besten genügen.

Beispielsweise war eine wesentliche Forderung, daß ein Einstieg auf die Betriebssystemebene durch Sachbearbeiter zu verhindern ist. Auf der Grundlage der ausgewählten Hard- und Software soll die Funktionalität des Systems so gestaltet werden, daß ein Mißbrauch personenbezogener Daten nahezu ausgeschlossen werden kann. Das Angebot möglicher Funktionen ist so weit einzuschränken bzw. zu erweitern, daß diese auf die spezifischen Aufgaben der betreffenden Mitarbeiter zugeschnitten sind. Dies bezieht sich zum einen auf die Nutzung von Standard-Software, zum anderen aber auch auf den Einsatz von Fachverfahren. Selbst die Probleme, die sich bei Vertretungsregelungen hinsichtlich abwesender Mitarbeiter zwangsläufig ergeben, sind unter dieser objektorientierten, grafischen Benutzungsoberfläche unkompliziert und trotzdem sicher lösbar.

Für 1994 ist die Schaffung einer Pilotlösung innerhalb der Projektgruppe und später die Installation des Systems im Bezirksamt Weißensee vorgesehen. Wir werden auch bei der konkreten Umsetzung dieses Vorhabens auf die Einhaltung der einschlägigen gesetzlichen Bestimmungen achten.

Das in Weißensee eröffnete *Bürgerbüro* ist Ende 1993 in das mittlerweile geschaffene Datennetz eingebunden worden. Damit wurde eine wesentliche Grundlage zur Funktionserweiterung dieser dienstleistungsorientierten Einrichtung realisiert. Bis zu diesem Zeitpunkt beschränkte sich die Nutzung der installierten Rechner im wesentlichen noch auf die Textverarbeitung. Aufgaben der Lohnsteuerkartenstelle und die Wohnberechtigungsscheinanträge konnten aufgrund der fehlenden Vernetzung noch nicht abschließend bearbeitet werden, so daß sich das Bürgerbüro hinsichtlich seiner Funktion als Bürgerberatungsstelle mit Weiterleitungsaufgaben darstellte. Die Beratungsplätze sind so angeordnet, daß die Voraussetzungen für vertrauliche Gespräche mit den Mitarbeitern dieser Einrichtung gegeben sind. Diese günstigen Rahmenbedingungen, wie auch die zentrale Lage in der Hauptgeschäftsstraße des Bezirkes lassen eine hohe Akzeptanz durch die ratsuchenden Bürger erwarten.

Im Bereich der *sozialen Dienste* wird im Modellbezirksamt Weißensee an einem Projekt gearbeitet, mit dem das Angebot effektiver gestaltet und rationalisiert werden soll. Insbesondere sollen dem Bürger möglichst viele Behördenwege erspart werden. Dazu sollen Dienste zusammengefaßt werden. Unter anderem ist daran gedacht, soziale Dienste, Einrichtungen der Jugendämter und der Gesundheitsämter zusammenzufassen.

Infrastrukturprojekt GIBES

Der Unterausschuß Kommunikations- und Informationstechnik des Hauptausschusses des Abgeordnetenhauses von Berlin stellte im Juni 1993 fest, daß die entstehenden Großverfahren der Berliner Verwaltung bezogen auf ihre verfahrensübergreifenden informationstechnischen Rahmenbedingungen, Dienstleistungen und Infrastrukturanforderungen zu unterstützen seien und daß eine übergreifende Koordination aus wirtschaftlichen Gründen erfolgen müsse. Die Senatsverwaltung für Inneres wurde beauftragt, unter Einbeziehung externer Unterstützung kurzfristig die dafür erforderlichen Schritte einzuleiten.

Das Projekt stand unter erheblichem Zeitdruck, da die zu unterstützenden Großverfahren zum Teil schon so weit fortgeschritten waren, daß sie zumindest vor ihren Pilotinstallierungen (vor allem BASIS) standen. Offensichtlich sollten deswegen auch der Datenschutz und die informationstechnische Sicherheit nicht behandelt werden, denn das GIBES-Pflichtenheft für die Ausschreibung der externen Unterstützung wies diese beiden Themen nur als Umfeldthemen aus, die nicht Bestandteil der im Rahmen des Projektes zu lösenden Aufgaben sein sollten. Nach Anfrage wurden einzelne Untersuchungsfelder benannt, bei denen technische Datenschutzfragen eine Rolle spielen würden, jedoch bekräftigt, daß bei dem Abstraktionsniveau des GIBES-Projektes eine ganzheitliche Betrachtung der Datenschutz- und IT-Sicherheitsbelange nicht durchgeführt werden könne.

Diese Vorgehensweise übersah, daß die beim Projekt GIBES zugrundegelegte Kommunikation über offene Netze, die internationalen Normen genügen, prinzipiell in einem Spannungsverhältnis zu datenschutzrechtlichen Zielsetzungen wie der Umsetzung der verfassungsrechtlich gebotenen informationellen Gewaltenteilung steht. Es bedarf daher schon auf dem hohen Abstraktionsniveau des GIBES-Projektes grundsätzlicher Überlegungen zu seiner Bewältigung: Sonst besteht die Gefahr, daß entweder eine Infrastruktur entsteht, die für die Wahrung des Grundrechtes auf informationelle Selbstbestimmung Risiken beinhaltet, die dann nur noch unzulänglich im Rahmen von konkreten Verfahrensprojekten gemildert werden können, oder daß der Datenschutz als Grund zur Verhinderung zeitgemäßer Kommunikationsinfrastrukturen mißbraucht wird.

Zwar sollte der technische Aspekt der Sicherheit in GIBES angesprochen werden, die weitere Betrachtung jedoch den Verfahren überlassen werden. Demgegenüber sollte in GIBES jedoch zumindest analysiert werden, welche Probleme für die Verfahren erst durch GIBES-Empfehlungen aufgeworfen werden. Entsprechende Lösungsansätze sollten angeboten werden. Verfahrenssicherheit ist nämlich auch abhängig von der Sicherheit der dahinterstehenden IT-Infrastrukturen, ist also nicht allein Sache der Verfahrensgestalter und -betreiber.

Im Ergebnisbericht wurde den Aspekten von Datenschutz und IT-Sicherheit ein hinreichender Stellenwert eingeräumt. Im Bericht kommt zum Ausdruck, daß die Absicht besteht, die IT-Infrastruktur der Berliner Verwaltung unter Berücksichtigung modernster informationstechnischer Entwicklungen und international akzeptierter Normen und Standards auszubauen. Es wird darauf zu achten sein, daß unter den Zielen auch jene die notwendige Beachtung finden, die das Interesse der Bürger und der Mitarbeiter der Berliner Verwaltung an sicheren und ordnungsgemäßen Verfahrensabläufen und der Wahrung ihrer informationellen Selbstbestimmung sicherstellen. Dieses setzt aber nicht nur voraus, daß die richtigen Infrastrukturen ausgewählt und installiert werden, sondern auch, daß trotz der den personellen Bereich betreffenden Sparzwänge genügend Mitarbeiter zur Verfügung stehen, die für die Beherrschung dieser teilweise überaus komplexen Systeme die erforderliche Qualifikation mitbringen. Andernfalls wird die moderne IT-Infrastruktur zu einem unkalkulierbaren Risiko für das Verwaltungshandeln.

2.2 Stand der Automation in der Berliner Verwaltung

Im folgenden soll eine Übersicht über den Einsatz von IuK-Technik für die Verarbeitung personenbezogener Daten in der Berliner Verwaltung gegeben werden. Vollständigkeit war dabei nicht das Ziel, vielmehr die Erwähnung der repräsentativen und uns wichtig erscheinenden Großverfahren und die neueren Entwicklungen.

Automatisierte Textverarbeitung und Bürokommunikation gehört mittlerweile zur Grundausstattung öffentlicher Stellen. Bei der Erst- und Ersatzbeschaffung von Telefon-Nebenstellenanlagen besteht zur Auswahl digitaler Systeme keine Alternative mehr. In solchen Systemen werden grundsätzlich personenbezogene Daten auf der Grundlage des Berliner Informationsverarbeitungsgesetzes (IVG) verarbeitet.

In der Verwaltung des *Abgeordnetenhauses von Berlin* wird das Abgeordnetenhaus-Dokumentations- und -Informationssystem ADIS für die Verwaltung und Bereitstellung der Dokumente des Abgeordnetenhauses betrieben. Das Verfahren ist als ein besonders herauszuhebendes Bürokommunikationssystem anzusehen. § 3 Abs. 1 IVG öffnet ADIS auch für die Verwaltung allgemein und für die Öffentlichkeit.

Bei der *Senatsverwaltung für Arbeit und Frauen* wird IuK-Technik vor allem für die Organisation der Arbeitsplatzbeschaffungsmaßnahmen eingesetzt.

Im Geschäftsbereich der *Senatsverwaltung für Bau- und Wohnungswesen* werden diverse Großverfahren im Dialog mit Rechnern des LIT betrieben: Wohngeldverfahren, Wohnungskataster/ Wohnberechtigungsscheine, Fehlbelegungsabgabe/Mietausgleich, Bodenwirtschaftliche Datei (BOWIDA), Kaufpreissammlung für Grundstücke, Automatisiertes Liegenschaftsbuch und -karte (ALB, ALK).

Im Geschäftsbereich der *Senatsverwaltung für Finanzen* soll das veraltete Automatisierte Haushaltswesen (AHW) im Rahmen einer Neukonzeption durch ein neues großes Dialogverfahren abgelöst werden, auf das von allen Stellen, die Haushalte zu bewirtschaften haben, direkt zugegriffen werden soll.

Die Daten der steuerpflichtigen Bürger und Organisationen werden in einem Rechenzentrum der Oberfinanzdirektion im DCL-Verfahren (Dezentrale Computer-Leistung) verarbeitet, auf das auch alle Finanzämter im Dialog zugreifen können. Auf längere Sicht wird für diese Aufgaben in dem bundesweiten Projekt FISCUS (Föderales Integriertes Standardisiertes Computer-Unterstütztes Steuersystem) das Nachfolge-Verfahren bereits geplant.

Im Geschäftsbereich der *Senatsverwaltung für Gesundheit* ist vor allem die Datenverarbeitung in den bezirklichen Krankenhausbetrieben hervorzuheben. Deren Patienten- und Personalverwaltung sowie weitere Verwaltungsaufgaben werden in Krankenhaus-Rechenzentren automatisiert verarbeitet. Dabei werden Programmsysteme der Gesellschaft für Systemforschung und Dienstleistungen im Gesundheitswesen (GSD) verwendet, die von dieser Gesellschaft auch weiterentwickelt und gepflegt werden.

Naturgemäß sind im Geschäftsbereich der *Senatsverwaltung für Inneres* die meisten personenbezogenen IuK-Anwendungen konzentriert.

Im *Personalwesen* sind die großen Zahlungsverfahren für die Beamten, Angestellten, Arbeiter und Versorgungsempfänger des Landes sowie das neue Beihilfeverfahren BABSY zu erwähnen. Diese Verfahren werden im LIT im Auftrag des Landesverwaltungsamtes (LVwA) mit Großrechnern betrieben. Hinzukommen die Systeme für die Automatisierte Personalwirtschaft (APW) bei den meisten Personalwirtschaftsstellen und die Automation der Ausbildungsstellen (ABIDA) für die Bewerberauswahl und die weitere Unterstützung bei der Steuerung der Ausbildung.

In Planung befindet sich derzeit ein landesweit einzusetzendes und vernetztes System der Integrierten Personalverwaltung (IPV), das die genannten Verfahren zum Teil ersetzen soll und weitere Aufgaben der Personalverwaltung automatisieren soll.

Die amtliche Statistik wird im *Statistischen Landesamt* fast ausschließlich automationsunterstützt geführt. Dazu bedient es sich eines Großrechners des LIT sowie eines umfangreichen eigenen Maschinenparks.

Im *Personenstandswesen* (Standesämter) wird das bundesweit im Einsatz befindliche ADV-Verfahren AUTISTA (Automation im Standesamt) eingesetzt.

In der Verantwortung des *Landeseinwohneramtes (LEA)* sind verschiedene große Dialogverfahren im Einsatz, die mit Rechnern des LIT betrieben werden:

- Mit dem ADV-Verfahren Einwohnerwesen (EWW) wird mit dem Berliner Melderegister die größte Datensammlung über Berliner Bürger geführt, auf die von den Meldestellen, den Bezirkseinwohnerämtern, von Polizeidienststellen und diversen anderen Behörden auf der Grundlage der Durchführungsverordnung zum Meldegesetz direkt zugegriffen werden kann.
- Das ADV-Verfahren im Kraftverkehrsamt (KVA) enthält die Zulassungsdaten für alle Kraftfahrzeuge mit Berliner Kennzeichen. Auf dieses Verfahren kann ebenfalls von der Polizei zugegriffen werden.
- In der Ausländerverwaltung wird das automatisierte Ausländerregister (AusReg) für den Vollzug ausländerrechtlicher Vorschriften genutzt.

Weitere Projekte des LEA waren in letzter Zeit Gegenstand datenschutzrechtlicher Erörterungen: Erstautomation der Führerscheindatei (FÜDA), Ordnungswidrigkeitenverfahren Autowrackbeseitigung (OWA), Überwachung der Beseitigung von Schnee und Eis.

Der *Polizeipräsident in Berlin* betreibt auf Rechnern des LIT das Informationssystem für Verbrechensbekämpfung (ISVB) im Rahmen des bundesweiten Polizeiverbundes INPOL. Auf dieses System kann in abgestufter Weise von allen Polizeidienststellen des Landes zugegriffen werden.

Für das alte Bußgeld- und Ordnungswidrigkeiten-Verfahren (BOWI) für Verkehrsordnungswidrigkeiten, das auf Rechnern des LIT betrieben wird, ist jetzt eine umfassende Revision in Angriff genommen worden (BOWI II).

Im Geschäftsbereich der *Senatsverwaltung für Jugend und Familie* sind neben verschiedenen Aufgaben der allgemeinen Verwaltung das Verfahren der Zentralen Vormundschaftskasse und Unterhaltsvorschußkasse, die bezirkliche Kindertagesstättenverwaltung und die Beteiligung an BASIS im Bereich der Jugendhilfe zu erwähnen.

Im Geschäftsbereich der *Senatsverwaltung für Justiz* ist für die IuK-Unterstützung bei der Abwicklung der Strafverfahren in den Geschäftsstellen das ADV-Verfahren Amts- und Staatsanwaltschaften (ASTA) eingeführt. Dieses große Dialogverfahren wird auf einem Rechner des LIT betrieben.

Für die Unterstützung bei Ermittlungsverfahren bei Wirtschaftsstrafsachen und anderen komplexen Verfahren setzt die Staatsanwaltschaft am Landgericht das Verfahren COISTRA ein.

Für die Abrechnung von Justizkosten wird ein Verfahren JUKOS betrieben.

Auch in den Strafvollzugsanstalten werden diverse Verwaltungsaufgaben mit den Daten der Häftlinge computerunterstützt abgewickelt.

Zum Geschäftsbereich der *Senatsverwaltung für kulturelle Angelegenheiten* gehören zahlreiche Einrichtungen wie Bibliotheken, Orchester, Theater und Museen, die für Abrechnungszwecke, ihre Leser- und Abonnentenverwaltung, für den Kartenvertrieb, für die Personalverwaltung und den Personaleinsatz sowie für die Verwaltung von Büchern, Requisiten und Ausstellungsstücken automatiserte Datenverarbeitung einsetzen.

Im Geschäftsbereich der *Senatsverwaltung für Schulwesen, Berufsbildung und Sport* kann davon ausgegangen werden, daß in den meisten der fast 1 000 Schulen, zumindest in den Oberschulen und Oberstufenzentren, Schulverwaltungsaufgaben und Textverarbeitung computerunterstützt durchgeführt werden. Viele Lehrer benutzen ihre privaten Personalcomputer für die Verarbeitung von Schülerdaten und die Zeugniserstellung.

Die anonymisierte Lehrerindividualdatei (LID) dient den Planungsund Personalsteuerungsaufgaben der Senatsverwaltung. Auf bezirklicher Ebene wird die Ablösung der bisher zentral auf einem Rechner des LIT betriebenen bezirklichen Lehrerverzeichnisse durch die dezentralen bezirklichen Lehrer-Informations- und Verwaltungssysteme (LIV)[54] als Modellprojekt beim Bezirksamt Wedding geplant.

Im Geschäftsbereich der *Senatsverwaltung für Soziales* ist das Projekt BASIS für die Sozial- und Jugendhilfe-Sachbearbeitung in den Bezirksämtern und im Landesamt für Zentrale Soziale Aufgaben das derzeit ehrgeizigste neue Automationsprojekt[55]. Bereits seit langem werden die Zahlungsverfahren für soziale Leistungen mit Rechnern des LIT abgewickelt.

Im Geschäftsbereich der *Senatsverwaltung für Stadtentwicklung und Umweltschutz* sind die Stadtplanungsdatei sowie verschiedene Kataster zur Überwachung und Registrierung von umweltrelevanten Altlasten, Immissionen und Einleitungen als automatisierte Verfahren zu erwähnen.

In Planung ist das berlinweit vernetzte Fachübergreifende Informationssystem (FIS) für den Bereich der Stadtplanung und des Umweltschutzes.

Zum Geschäftsbereich der *Senatsverwaltung für Verkehr und Betriebe* gehören die Eigenbetriebe, die umfangreiche, teilweise berlinweit vernetzte Großverfahren für die Personalverwaltung, den Personaleinsatz, die Kundenverwaltung und den Betriebsmitteleinsatz betreiben.

Im Geschäftsbereich der *Senatsverwaltung für Wirtschaft und Technologie* sind als personenbezogene Anwendung die bezirklichen Gewerbe datenbanken (GEWDAT) für die Unterstützung bei der Verwaltung der Gewerbeanmeldungen und des gewerberechtlichen Meldewesens zu erwähnen.

Zu diesem Geschäftsbereich betreiben die Handwerkskammern und -Innungen, die Industrie- und Handelskammer und die öffentlichen Unternehmen wie z. B. die Landesbank Berlin, die Feuersozietät und die Öffentliche Lebensversicherung Berlin umfassende personal-, mitglieder- und kundenbezogen ADV-Verfahren.

Bei der *Senatsverwaltung für Wissenschaft und Forschung* wird eines der ersten und umfangreichsten Bürokommunikationssysteme auf UNIX-Grundlage betrieben.

In den dieser Verwaltung zugeordneten Hochschulen und Fachschulen des Landes werden in den zentralen Verwaltungen und den Fachbereichen, so vor allem auch in den Universitätskliniken, umfassende und miteinander vernetzte Systeme für Zwecke der zentralen und dezentralen Verwaltungen und für Zwecke in der Forschung und Lehre eingesetzt. Die Rechenzentren der drei Universitäten und das Konrad-Zuse-Rechenzentrum betreiben Systeme der höchsten Leistungsklassen vorwiegend im Forschungsbereich.

2.3 Chipkarten - nur Trümpfe für den Datenschutz?

Plastikkarten gehören heute einfach dazu - ob man an der Kaufhauskasse mit Kreditkarten bezahlen möchte, ob man an der Tankstelle unterschriftslos mit der Eurocheque-Karte das Benzin begleichen will, ob man bargeldlos telefonieren möchte. Hier vollzieht sich derzeit ein entscheidender Wandel: Die bisher gebräuchlichen Magnetstreifenkarten werden abgelöst von Chipkarten *(„smart-cards")*.

Magnetstreifenkarten enthalten einen *Magnetstreifen,* der wie ein Magnetband beschrieben, überschrieben, gelöscht und abgespielt bzw. gelesen werden kann. Sie sind billig, aber ihr Inhalt ist leicht verfälschbar, da Geräte zum Lesen, Kopieren und Überschreiben von Magnetkarten frei erhältlich sind.

Bei den *Chipkarten* wird die Möglichkeit genutzt, Halbleiterspeicherchips und/oder Prozessorchips in Plastikkarten der Größe und Dicke der Magnetstreifenkarten unterzubringen. In den Speicherchips gespeicherte Daten können zur Weiterverarbeitung gelesen und verändert werden, die Prozessoren in den „intelligenten" Chipkarten können mit dem Lesegerät interagieren und Daten aus den eigenen Speicherchips oder aus dem Lesegerät verarbeiten. Viele Anwendungen der Chipkarte, so auch für Sicherheitszwecke, machen es sich zunutze, daß Chipkarten auch mit nicht beschreibbaren Speicherchips (ROM - Read Only Memory, u. a. für die Aufnahme des Chipkarten-Betriebssystems) oder gar mit Speicherchips ausgestattet werden, die nur vom Prozessor auf der gleichen Chipkarte gelesen werden können (etwa zur Speicherung geheimer Schlüssel).

Eine sehr verbreitete Anwendung der Chipkarte ist die bekannte *Telefonkarte,* die als Sammlerobjekt dabei ist, den Briefmarken beinahe den Rang abzulaufen. Es handelt sich dabei um eine Chipkarte recht einfacher Technologie, denn sie enthält nur einen Speicherchip, auf dem ein Guthaben gespeichert ist. Dieses Guthaben wird bei einem Telefonat mit dem Kartentelefon automatisch reduziert. Die Vorteile liegen zum einen in der höheren Sicherheit für die öffentlichen Telefone, denn es gibt in ihnen kein Bargeld mehr, für das es sich lohnen würde, die Apparate aufzubrechen, und zum anderen in den zinslosen Krediten, die die Benutzer der Telekom durch die Vorauszahlung gewähren. Die Vorteile für den Kunden liegen in der Unabhängigkeit vom sonst nötigen Münzgeld. Für den Datenschutz gibt es bei solchen *Wertkarten (Prepaid-Karten)* keine Risiken, denn der gesamte Zahlungsverkehr läuft anonym ab.

Anders ist es bei den *Kreditkarten (Postpaid-Karten).* Wenn man mit ihnen bezahlt, wird eine Datenspur gelegt, deren Umfang für kaum einen Kunden durchschaubar ist: Der Kreditgeber will wissen, in welcher Höhe wann die Kreditkarte in Anspruch genommen wurde und wer der Begünstigte ist (wo die Karte also zum Bezahlen genutzt wurde), damit die Einhaltung des Kreditrahmens und die Identität des Karteninhabers geprüft werden können (Autorisierung) und die Buchungen in richtiger Weise erfolgen (Clearing). Der Benutzer von Kreditkarten nimmt also hin, daß er beim Einsatz der Karte Daten über sein Kaufverhalten preisgibt.

Keiner wird bestreiten, daß die Prepaid-Karte zumindest bei höheren Zahlbeträgen keine sinnvolle Konkurrenz zur Postpaid-Karte sein kann. Die vorauszuzahlenden Beträge würden eine Höhe erreichen müssen, die ihre Akzeptanz in Frage stellen

54 vgl. 4.5
55 vgl. 4.10

würde. Anders ist dies aber bei den kleineren Zahlbeträgen, wie sie beim Telefonieren, bei der Taxinutzung, bei der Nutzung des öffentlichen Personennahverkehrs, beim Eintritt in Museen, Ausstellungen, Kinos usw. anfallen. Aus den oben für die Telefonkarte genannten Gründen könnten diese Wertkarten eine Alternative zum Bargeld darstellen.

Einige Kommunen denken gleichwohl darüber nach, den elektronischen Zahlungsverkehr mit Postpaid-Karten auch für Kleinbeträge einzuführen, insbesondere für die Nutzung des öffentlichen Personennahverkehrs. Entsprechende Pläne gibt es in einigen Städten wie z. B. in Kiel und Hamburg. Die Gefahren für die informationelle Selbstbestimmung bei der Nutzung solcher Zahlungsverfahren, die unter Umständen Bewegungsprofile für einzelne Personen ermöglichen, haben die Konferenz der Datenschutzbeauftragten des Bundes und der Länder veranlaßt, in einer Entschließung vor solchen kartengestützten Zahlungssystemen im öffentlichen Nahverkehr zu warnen und sich für Prepaid-Systeme einzusetzen[56].

Es ist zu begrüßen, daß die *Berliner Verkehrsbetriebe (BVG)* in Zusammenarbeit mit der Studiengesellschaft Verkehr mbH und mit Förderung des Bundesministeriums für Forschung und Technologie und der Senatsverwaltung für Verkehr und Betriebe eine Pilotanwendung der *„elektronischen Geldbörse"* erprobt, die als Prepaid-Chipkarte realisiert wird. Von allen möglichen kartenunterstützten Varianten des elektronischen Zahlungsverkehrs wird diese Wertkarte den Anforderungen des Datenschutzes am meisten gerecht, da die einzelnen Zahlungsvorgänge weder für die Autorisierung der Zahlungen noch für das spätere Clearing zentral gespeichert werden müssen. Somit kann die Gefahr technisch ausgeschlossen werden, daß die Daten für personenbezogene Kauf- oder Verbraucherprofile, in diesem Falle Bewegungsprofile zweckentfremdet werden können.

Während der Pilotphase sollen Name und Anschrift der Teilnehmer bei der BVG festgehalten werden, da die BVG das Eigentumsrecht an den Chipkarten behalten will. Für die Datenverarbeitung bedarf es der Einwilligung der Betroffenen.

Es ist ferner auf Dauer vorgesehen, alle Datentransfers, die im Zuge der Chipkartenanwendungen anfallen (Aufbuchung, Abbuchung beim Fahrausweiserwerb, Chipkarten-Kontoführung usw.), mit der Seriennummer zentral zu speichern, um bei eventuellen Einwendungen der Kunden die Benutzung der Karte prüfen zu können. Dagegen bestehen wegen der Anonymität der Datensammlungen keine Bedenken.

Es wurde uns bestätigt, daß sichergestellt ist, daß Name und Anschrift der Teilnehmer nicht in Verbindung mit der Chipkarten-Seriennummer gespeichert werden, weil dies wegen der seriennummernbezogenen Speicherung der Datentransfers zur oben beschriebenen Gefahr von personenbezogenen Bewegungsprofilen führen würde.

Bei der Benutzung der Chipkarte in einem entsprechend ausgerüsteten Bus wird sowohl fahrer- als auch fahrgastseitig auf einer LCD-Anzeige das aktuelle Kartenguthaben dargestellt.

Die fahrgastseitige Anzeige dient dem Fahrgast zur Kontrolle seines Guthabens und ist rechtlich unbedenklich. Allerdings ist dringend darauf zu achten, daß Dritte (also die, die sich hinter dem Fahrgast in die Warteschlange einreihen oder Fahrgäste, die in der Nähe sitzen oder stehen) keinen Einblick in die fahrgastseitige Anzeige erhalten können. Anderenfalls bestehen nicht nur Risiken hinsichtlich der Wahrung der informationellen Selbstbestimmung, sondern auch hinsichtlich seiner persönlichen Sicherheit. Es wurde uns versichert, daß die Anzeige zum Fahrgast entsprechend plaziert ist.

Die fahrerseitige Anzeige des Guthabens ist allerdings überflüssig und daher unzulässig. Für den Fahrer ist von Bedeutung, ob das Guthaben ausreicht, um die gewünschten Fahrausweise zu bezahlen, nicht jedoch dessen Höhe. Eine Modifizierung der Technik wird vorgenommen.

56 vgl. Anlage 2.8

Ein grundsätzliches Risiko der Prepaid-Cards ist, daß im Falle der unbefugten Verwendung der Karte nach Verlust oder Diebstahl dem Inhaber ein Schaden in Höhe des Restguthabens droht. Da die Guthabenhöhe bis 999 DM betragen kann, sind Risiken für den Kunden und Anreiz für Gesetzesbrecher nicht unerheblich. Wir empfahlen eine Prüfung, ob für die Nutzung der Chipkarte nicht auch die Eingabe eines geheimen Paßwortes erforderlich sein sollte oder ob nicht bereits bei der Zahlung per Chipkarte im Bus eine Prüfung ermöglicht werden kann, ob die Karte gesperrt ist oder nicht.

Dem steht gegenüber, daß der Aufwand dafür sehr erheblich ist und die Akzeptanz beeinträchtigen würde. Die Abfertigungsdauer würde sich verlängern. Andererseits kann wegen der frei wählbaren Guthabenhöhe auf der Karte das Verlustrisiko in den gleichen Grenzen gehalten werden wie bei einer Geldbörse voller Bargeld. Da auf der Chipkarte ein Verfalldatum gespeichert wird, wird das Verlustrisiko reduziert. Nach dem Datum ist eine unbefugte Nutzung nicht mehr möglich, so daß die Chance besteht, daß der Kunde noch ein Restguthaben zurückbekommen kann. Diese Argumente wurden von uns akzeptiert.

Aber nicht nur bei Zahlungsverfahren soll die Speicherfähigkeit der Chipkarte genutzt werden.

Nach § 291 Sozialgesetzbuch V (SGB V) sind bis 1995 alle gesetzlich krankenversicherten Personen mit einer *Krankenversichertenkarte* auszustatten. Diese soll zum Nachweis der Berechtigung zur Inanspruchnahme von Kassenleistungen und Abrechnung mit den Leistungserbringern den Krankenschein ersetzen. Mit der Karte erhofft man sich Einsparungen im Gesundheitsbereich durch die Automatisierung der Datenflüsse und der verbesserten Auswertbarkeit der Datenbestände, eine Rationalisierung der Krankenscheinerstellung, Mißbrauchverhinderung und Verbesserung der Transparenz des Leistungsgeschehens.

Der Gesetzgeber hat keine Vorgaben zur Kartentechnologie gemacht. Die Tendenz geht dahin, Chipkarten einzusetzen. Auch in Berlin sollen ab dem 1. Januar 1995 solche Chipkarten für alle bei der AOK, den Betriebs- und den Innungskrankenkassen Versicherten eingeführt werden.

Nach § 291 Abs. 2 SGB V ist es zulässig, in der Chipkarte die Bezeichnung der ausstellenden Krankenkasse, den Familien- und Vornamen des Versicherten, das Geburtsdatum, die Anschrift, die Krankenversichertennummer, eine Angabe zum Versichertenstatus, Beginn und Ablauf des Versicherungsschutzes zu speichern.

Es muß sichergestellt werden, daß keine darüber hinausgehenden Daten auf der Karte gespeichert werden und daß über die in § 291 Abs. 2 SGB V genannten Zwecke hinaus keine weitere Nutzung der Karte möglich ist. Die Aufnahmekapazität des Chips muß also auf die Aufnahme der zulässigen Daten beschränkt sein. Tatsächlich verfügen die Chips über mehr *Speicherkapazität.* Die nicht benötigten Speicherplätze werden allerdings mit einem definierten Zeichen belegt und können nicht in manipulativer Absicht beschrieben werden. Die Lesegeräte dürfen nur den zulässigen Bereich lesen können. Zur Absicherung dieser Anforderung dürfen nur Lesegeräte von Ärzten und sonstigen Leistungserbringern eingesetzt werden, die vom Bundesamt für die Sicherheit in der Informationstechnik (BSI) zertifiziert worden sind. Diese Anforderung ist nach ersten Prüferfahrungen außerhalb Berlins nicht immer eingehalten worden.

Nur schwach ausgeprägt sind die *Maßnahmen gegen Fälschung der Karten und Mißbrauch gestohlener oder verlorener Karten.*

Die Empfehlung des Bundesbeauftragten für den Datenschutz, mit Hilfe eines kryptografischen Verfahrens die Chipkarte zu versiegeln, wurde auch hier aus Kostengründen abgelehnt. Eine Authentifizierung des Versicherten gegenüber der Karte (z. B. mit Hilfe einer geheimen Identifikationsnummer) findet nicht statt. Erste Prüferfahrungen bei Versicherungen in anderen Bundesländern, die bereits Chipkarten ausgeben, haben darüber hinaus ergeben, daß die Ersterfassung von Daten keineswegs immer so sicher erfolgt, daß die Verwendung von Identifikationsmerkmalen der Versicherten in anderen Chipkarten ausgeschlossen werden kann.

Es wurde zugesichert, daß jeder Versicherte jederzeit den Inhalt der auf der Karte über ihn gespeicherten Daten bei der Krankenkasse oder gar bei einem Arzt lesen und überprüfen kann. Auch die Beachtung dieser Vereinbarungen konnte bei den genannten Prüfungen nicht immer bestätigt werden.

Die Krankenversicherungs-Chipkarte stellt nur die Oberfläche einer umfassenden informationstechnischen Infrastruktur im Gesundheitswesen dar. Während des Datenflusses zwischen den Arztpraxen, den kassenärztlichen Vereinigungen und den Krankenkassen werden Patientendaten aus der Chipkarte angereichert mit diversen Daten, u. a. auch zum Gesundheitszustand des Patienten. Dies bedeutet: Nicht die Karte selbst ist der eigentliche datenschutzrechtliche Risikofaktor, sondern die dahinterstehende Vernetzung zur Kontrolle des Gesundheitsverhaltens des Versicherten und des Verschreibungsverhaltens der Ärzte.

Aus gesundheitspolitischen Erwägungen ist auch die zusätzliche Einführung einer *Chipkarte mit medizinischen Daten* der Patienten angeregt worden. Eine solche Karte könnte z. B. für den Notfall wichtige Daten wie Blutgruppe, besondere gesundheitliche Risiken, Allergien, Infektionen (z. B. mit HIV) usw. enthalten, die dem Arzt dann die richtige Behandlung ermöglichen könnten. Eine solche Karte bedürfte der Einwilligung der Versicherten und umfassenderer Sicherheitstechnik. Jedoch müßte in diesem Falle verhindert werden können, daß Patienten bei Gelegenheiten zur Preisgabe der Daten veranlaßt werden, für die die Karte nicht bestimmt ist (z. B. im Rahmen einer Bewerbung um einen Arbeitsplatz).

Die beschriebenen Anwendungsmöglichkeiten der Chipkarte nutzen die Speicherkapazitäten von Chips und zeigen, daß für den Datenschutz Chancen und Gefahren mit dieser Technik dicht beieinander liegen: Wenn die Bürger die sie betreffenden Datensätze für verschiedene Nutzungen auf Chipkarten mit sich herumtragen, wird einerseits ihre informationelle Selbstbestimmung dadurch gewahrt, daß sie - abgesehen von Notfallsituationen, in denen sie keine Willenserklärung mehr abgeben können - selbst über den Datenträger verfügen und darüber entscheiden können, wie sie ihn einsetzen. Andererseits wird sie jedoch dadurch gefährdet, daß die Verwendung dieser Daten unabhängig von Zugriffsberechtigungen auf Informationssysteme zu jeder Zeit möglich ist, insbesondere dann, wenn in irgendeiner Weise, ob durch die Ausnutzung von Notlagen (z. B. Arbeits- oder Wohnungssuche) oder mit psychischem Druck auf den Betroffenen Zwang ausgeübt wird, seine Daten auch ohne rechtlichen Grund preiszugeben. Ferner zeigt das Beispiel der Krankenversicherungskarte, daß der Bürger zwar die Verfügungsgewalt über seine Chipkarte hat, mit ihrer Nutzung jedoch komplexe Datenflüsse auslöst, die er nicht mehr überschauen kann.

Neben den beschriebenen Speicherchipkarten gibt es auch Chipkarten, die zusätzlich mit *Prozessoren* ausgestattet sind. Sie werden von den Lesegeräten mit Energie versorgt und können Datenverarbeitungsprozesse selbst oder in Interaktion mit den Geräten durchführen. Bisherige Entwicklungen solcher Chipkarten dienen meist der informationstechnischen Sicherheit bzw. der Umsetzung technischer Maßnahmen zum Datenschutz.

So können Prozessorchipkarten die Authentifizierung von Benutzern von Informations- und Kommunikationssystemen, bei Zugangskontrollsystemen oder an Geldautomaten sicherer machen, in dem sie eine Berechtigungsprüfung durchführen und dem System den Nachweis erbringen, daß die Nutzung berechtigt erfolgt.

3. Grundsatzprobleme

3.1 Magna Charta des Datenschutzes - Auskunfts- und Einsichtsrechte

„Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß."

Dieser Satz nimmt eine zentrale Stellung im Volkszählungsurteil des Bundesverfassungsgerichtes ein. An anderer Stelle betont das Gericht, auf das Volkszählungsgesetz bezogen, aber sicherlich verallgemeinerbar: „Würde das Volkszählungsgesetz 1983 demnach verhindern, daß der Bürger Kenntnis davon erlangen könnte, wer wo über welche seiner personenbezogenen Daten in welcher Weise und zu welchen Zwecken verfügt, so wäre sein Rechtsschutz verfassungsrechtlich unzureichend."

In materieller und prozessualer Hinsicht kommt demnach der Kenntnis des Bürgers über die Verarbeitung seiner Daten eine elementare Bedeutung zu. Manche Autoren haben das Recht der Bürger auf Zugang zu ihren Daten deshalb „Magna Charta der informationellen Selbstbestimmung" genannt.

Der Gesetzgeber hatte in der Vergangenheit diesem Bürgerrecht nicht hinreichend Rechnung getragen. Vielmehr beherrschte das Denken in den öffentlichen Verwaltungen das sog. „Arkanprinzip", d. h. der Grundsatz, daß verwaltungsinterne Vorgänge vor dem Bürger verborgen werden können, und er nur einen Anspruch darauf hat, von dem Ergebnis des Verwaltungshandelns zu erfahren.

Für die Beteiligten am Verwaltungsverfahren im engen Sinne wurde dieses Prinzip zunächst von der Rechtsprechung, später im Verwaltungsverfahrensgesetz gelockert. Den Beteiligten wird zwar ein Akteneinsichtsrecht in die das Verfahren betreffenden Akten gewährt, dieses jedoch von engen Voraussetzungen abhängig gemacht: Die Kenntnis der Akten muß zur Geltendmachung oder Verteidigung der rechtlichen Interessen erforderlich sein, Entscheidungsentwürfe und vorbereitende Arbeiten sind bis zum Abschluß des Verwaltungsverfahrens nicht vorzulegen. Weitere Ausnahmen sollen die ordnungsgemäße Aufgabenerfüllung, das Staatswohl oder Geheimhaltungsinteressen schützen; Vorgänge, die ihrem „Wesen nach" geheimgehalten werden müssen, schaffen zusätzliche Verweigerungsgründe.

Erst das Bundesdatenschutzgesetz von 1977 und die in der Folge erlassenen Landesdatenschutzgesetze schufen einen kategorischen Auskunftsanspruch des Bürgers über seine Daten, allerdings auch diesen mit gewichtigen Einschränkungen: Dem Bürger wurde nur ein *Auskunftsrecht* zugestanden, nicht aber ein Einsichtsrecht. Dies bedeutete, daß die speichernden Stellen es in der Hand hatten, die Form, und, wie die Praxis später zeigte, auch den Inhalt der offenbarten Informationen zu bestimmen. Wie der Geltungsbereich der ersten Generation der Datenschutzgesetze ganz allgemein, beschränkte sich der Auskunftsanspruch auf Daten, die in Dateien gespeichert waren; einen ausdrücklichen Anspruch auf Auskunft über Akten gewährten diese Gesetze mithin nicht. Schließlich wurden vom Auskunftsanspruch mehrere Geschäftsbereiche pauschal ausgenommen: die Nachrichtendienste, die Staatsanwaltschaft, die Polizei und die Finanzbehörden. Hinzu kamen weitere materielle Verweigerungsgründe - auch hier geisterten „ihrem Wesen nach geheimzuhaltende Daten" durch die Paragraphen.

Bereits vor dem Volkszählungsurteil zeigte sich, daß keiner dieser Ausschlußgründe uneingeschränkt Bestand haben konnte. Bürger gaben sich häufig mit Auskünften nicht zufrieden, sie wollten die Originalunterlagen sehen; Verwaltungen war der Aufwand zu hoch, aus Unterlagen einen Extrakt zu fertigen, der - jedenfalls bei korrekter Rechtsanwendung - ohnehin nicht weniger Informationen enthielt als die Originalunterlage. Im Ergebnis wurde in der Regel eben doch Einsicht gewährt. Die Beschränkung des Geltungsbereichs auf Dateien wurde auch hinsichtlich des Auskunftsrechtes von den Bürgern nicht akzeptiert: Für den Bürger ist es in der Regel uninteressant, auf welche Weise die Verwaltung Daten verarbeitet, ihm kommt es darauf an zu wissen, über welche Informationen die Verwaltung verfügt. Mit Hilfe analoger Anwendung oder unter extensiver Auslegung des Verwaltungsverfahrensrechtes wurde dem Bürger Auskunft aus Akten oder - siehe vorher - Einsicht in die Akten gewährt.

Auch die Behörden, die zuvor gehofft hatten, sich von Auskunftsansprüchen pauschal freihalten zu können, sahen sich enttäuscht: Zunächst von den Datenschutzbeauftragten postuliert, später von den Gerichten bestätigt, mußte man davon ausgehen, daß die Datenschutzgesetze zwar ein subjektives Recht auf Auskunft nicht gewährten, die privilegierten Behörden gleichwohl zu

einer Ermessensausübung verpflichtet waren, die dann doch zumindest zu einer eingeschränkten Auskunftspflicht führte: Dies akzeptierte z. B. der Polizeipräsident, als er sich frühzeitig einer Vielzahl von Auskunftsersuchen der Bürger konfrontiert sah. Lediglich der Verfassungsschutz beharrte jahrelang darauf, keinerlei Auskünfte zu erteilen.

Das Volkszählungsurteil machte allen Beteiligten klar, daß es nicht bei der bestehenden Gesetzeslage bleiben konnte. Nach den langen Jahren der Diskussion über die Novellierung der Datenschutzgesetze wurden die Rechtsgrundlagen in Bund und Ländern schließlich auf eine neue Grundlage gestellt.

Das Berliner Datenschutzgesetz von 1990 beseitigte sämtliche pauschalen Einschränkungen und ersetzte sie durch die Verpflichtung zur Überprüfung, ob im Einzelfall Verweigerungsgründe vorliegen: Der Betroffene kann seither selbst wählen, ob er Auskunft oder Einsicht verlangt; die unterschiedliche Behandlung von Dateien und Akten wurde beseitigt; keine Behörde einschließlich des Landesamtes für Verfassungsschutz ist mehr privilegiert. Einziger Verweigerungsgrund im Einzelfall ist, daß eine Erwägung ergibt, daß die Rechte des Betroffenen hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter aus zwingenden Gründen zurücktreten müssen.

Diese der verfassungsrechtlichen Lage sicherlich am nächsten kommende Lösung des Berliner Datenschutzgesetzes wurde allerdings durch die - in gewisser Weise durch das Gesetz selbst erzwungene Spezialgesetzgebung relativiert.

Landesamt für Verfassungsschutz

Die Aufarbeitung überschießender Vorgehensweisen des Landesamtes für Verfassungsschutz, die mit der Einsetzung eines Untersuchungsausschusses im Jahr 1987 begann und auch zu umfangreichen Beanstandungen des Datenschutzbeauftragten führte, veranlaßte das Landesamt bereits vor Inkrafttreten des neuen Gesetzes auf Ersuchen der Bürger nicht nur Auskunft über die Speicherung personenbezogener Daten zu erteilen, sondern großzügig Akteneinsicht zu gewähren, soweit keine überwiegenden Geheimhaltungsinteressen entgegenstanden. Dieses Verfahren hatte sich bewährt und war für das Landesamt eine vertrauensbildende Maßnahme. Eine eigens gebildete Arbeitsgruppe bemühte sich, die Belange des Amtes einerseits mit den Interessen und Befürchtungen andererseits abzuwägen. Die persönliche Teilnahme der Datenschutzbeauftragten an einem derartigen Gespräch mit dem Bürger bestätigte, daß hier in besonderer Weise auf die informationelle Selbstbestimmung Rücksicht genommen wurde.

Diese Praxis belegte, daß selbst die Belange des Verfassungsschutzes keine Einschränkung der allgemeinen Grundsätze des neuen Berliner Datenschutzgesetzes erforderlich machen[57].

Gleichwohl wurde die allgemeine Auskunftsregelung des Datenschutzgesetzes im Rahmen der Novellierung des Landesverfassungsschutzgesetzes (LVfG) durch eine spezialrechtliche Regelung ersetzt. Nach dieser - dem Bundesverfassungsschutzgesetz folgenden - Regelung wird zwar ein Anspruch auf Auskunft über die gespeicherten Informationen gewährt, die Akteneinsicht liegt jedoch im Ermessen des Landesamtes. Im Einzelfall kann das Landesamt Auskünfte (und damit auch die Einsicht) verweigern, wenn das öffentliche Interesse an der Geheimhaltung seiner Tätigkeit oder ein überwiegendes Geheimhaltungsinteresse Dritter gegenüber dem Interesse der Antragstellenden Person an der Auskunftserteilung überwiegt. Diese Geheimhaltungsinteressen werden, was positiv zu bewerten ist, zwar näher definiert, aber auch hier hebt das Gespenst des „Wesens der Daten" wieder seinen Kopf.

Gewichtiger ist die Einschränkung des Auskunftsanspruches darauf, daß die auskunftsersuchende Person ein „besonderes Interesse" an einer Auskunft darlegt. Bei den parlamentarischen Beratungen des Gesetzes hatten wir an der Auffassung festgehalten, daß diese Einschränkung verfassungswidrig ist.

Der praktische Umgang mit dieser Einschränkung hat die Befürchtungen bestätigt.

Die Betroffenen wurden anfangs nicht nur aufgefordert anzugeben, daß sie im „extremistischen Spektrum in Erscheinung getreten" sind. Auch die subjektive Befürchtung, daß erlittene Belastungen und Schwierigkeiten möglicherweise durch eine Beobachtung vom Verfassungsschutz verursacht wurden, wurden vom Landesamt für Verfassungsschutz als nicht ausreichend akzeptiert. Eine Bürgerin wurde aufgefordert darzulegen, weshalb sie Anlaß zu haben meint, beim Landesamt für Verfassungsschutz registriert zu sein. Was kann damit anderes gemeint sein als verfassungsfeindliche Bestrebungen oder Tätigkeiten mitzuteilen - sich also selbst zu bezichtigen? Dementsprechend wurde der Bürgerin auch ein Auszug des § 5 des Gesetzes über das Landesamt für Verfassungsschutz überlassen, in dem sie die verfassungsfeindlichen Bestrebungen im einzelnen nachlesen kann. Ebenso sind Aufforderungen des Landesamtes für Verfassungsschutz an auskunftbegehrende Bürger zu bewerten, nach denen sie Angaben zu machen haben, die im Zusammenhang mit der Aufgabenstellung des Landesamtes für Verfassungsschutz stehen.

Das Landesamt für Verfassungsschutz lehnte - mal als „unbegründet", mal als „unzulässig" - ohne jede weitere Prüfung die Anträge auf Auskunft ab, wenn die Bürger nicht diesen weitgehenden Darlegungspflichten nachkommen.

Diese Verfahrensweise ist verfassungsrechtlich höchst bedenklich.[58] Wir hielten es für die Betroffenen für unzumutbar, daß ihr Auskunftsrecht an eine Aufforderung zur Selbstbezichtigung gebunden wurde. Aus dem Recht auf informationelle Selbstbestimmung folgt, daß der Betroffene grundsätzlich wissen können muß, wer was bei welcher Gelegenheit über ihn weiß. Ein besonderes Interesse an einer Auskunft ergibt sich demnach unmittelbar aus dem Persönlichkeitsrecht der Betroffenen. Zumindest aber ist als ausreichend für die Darlegung des besonderen Interesses anzusehen, wenn erkennbar ist, daß die Auskunft für das weitere Verhalten des Antragstellers bedeutsam ist. Hier kommt es nicht darauf an, daß der Betroffene konkrete Schritte beabsichtigt, sondern es ist ausreichend, daß erkennbar ist, daß das Wissen um die über seine Person beim Verfassungsschutz gesammelten Informationen für Bedeutung für sein Verhalten, z. B. auch für die Aufklärung - möglicherweise - irrationaler Ängste, ist.

Anders als das „berechtigte" Interesse enthält der Begriff des „besonderen" Interesses keine objektiven Bedingungen. Einschätzungen, Ängste und Befürchtungen des Betroffenen über eventuelle Datenspeicherungen zu seiner Person beim Verfassungsschutz sind deshalb zu respektieren und dürfen nicht durch objektive Kriterien relativiert werden.

Nach unserer Beanstandung wurde auf die Aufforderung zur Selbstbezichtung verzichtet. Die Betroffenen werden auch nicht mehr darauf hingewiesen, daß ihr „besonderes Interesse" an einer Auskunft im Zusammenhang mit der Aufgabenerfüllung des Landesamtes für Verfassungsschutz stehen muß.

Es ist künftig beabsichtigt, folgende Darlegungen von auskunftbegehrenden Bürgern zu verlangen:

Der Betroffene muß angeben:

- einen rechtlichen oder tatsächlichen Nachteil erlitten zu haben oder erleiden zu können und zur Abwendung oder Verhinderung des Nachteils Informationen erforderlich sind, über die die zuständige Verfassungsschutzbehörde verfügen könnte,
- einen Rechtsanspruch durchsetzen zu wollen und hierfür Informationen erforderlich sind, über die die zuständige Verfassungsschutzbehörde verfügen könnte,

57 Nach dem Verfassungsschutzbericht 1992 hatten bis 31. Dezember 1992 1 238 Bürger einen Antrag auf Auskunft oder Akteneinsicht gestellt. Davon waren Daten über 662 Personen (= 53 %) gespeichert; davon erhielten 520 Personen Auskunft oder Einsicht.

58 BVerfGE 65, 1, 46

- daß das Ansehen seiner Person geschädigt ist und er zur Rehabilitierung Informationen benötigt, über die die zuständige Verfassungsschutzbehörde verfügen könnte.

Wenn die Anfrage diesen Anforderungen nicht genügt, wird auch weiterhin ohne weitere Prüfung die Auskunft verweigert.

Diese Fallkonstellationen sind immer noch eine zu weitgehende Einschränkung des Auskunftsrechtes. Es handelt sich hier durchgehend um Voraussetzungen, die zur Darlegung eines *rechtlichen* Interesses erforderlich sind. Dies wird jedoch in § 31 Abs. 1 LVfG nicht gefordert.

Alle Fallbeispiele setzen darüber hinaus zwingend die Darlegung eines konkreten Sachverhaltes voraus. Gerade diese - im Bundesverfassungsschutzgesetz kumulativ aufgeführte - Voraussetzung wurde jedoch vom Abgeordnetenhaus nicht in das Gesetz über das Landesamt für Verfassungsschutz übernommen, obwohl sich dieses Gesetz weitgehend am Bundesverfassungsschutzgesetz orientiert. Das Abgeordnetenhaus hat in Kenntnis dieser früheren Regelung und der sich hieran knüpfenden Kritik des Bundesbeauftragten für den Datenschutz[59] einen Auskunftsanspruch beschlossen, der zwar die Darlegung eines besonderen Interesses voraussetzt, jedoch nicht den Hinweis auf einen „konkreten Sachverhalt", und damit deutlich gemacht, daß es den Auskunftsanspruch gerade nicht von einer Sachverhaltsangabe abhängig machen wollte.

Die Darlegung des „besonderen Interesses" bezweckt, der abstrakten Gefahr einer allgemeinen Ausforschung vorzubeugen. Wenn aufgrund der Ausführungen anzunehmen ist, daß die Auskunft für das weitere Verhalten des Antragstellers bedeutsam ist, besteht diese Befürchtung nicht. Die Voraussetzung eines „besonderen Interesses" hat folgerichtig in der Auskunftspraxis des Bundesamtes für Verfassungsschutz keine Bedeutung. *Jedes* Interesse, das über das allgemeine Auskunftsinteresse hinausgeht, wird anerkannt.

Das Landesamt ist in letzter Zeit offenbar dazu übergegangen, daß auch Ängste und Befürchtungen von Betroffenen als „besonderes Interesse" anerkannt wurden.

Auch die Praxis, quasi von einem Auskunftsverbot auszugehen, wenn das besondere Interesse nicht dargelegt wird, ist bedenklich. In diesem Fall wird das Auskunftsbegehren abgelehnt, ohne daß überhaupt geprüft wird, ob die Auskunft nicht doch ohne Gefahr für die Aufgaben des Landesamtes erteilt werden kann.

Ein Verbot, Auskünfte auch in Fällen zu erteilen, in denen der Betroffene nicht ein besonderes Interesse an der Auskunft darlegt, kann jedoch § 31 Abs. 1 Satz 1 LVfG nicht entnommen werden. Vielmehr ist - auch bei nicht ausreichender Darlegung des „besonderen Interesses" - regelmäßig zu prüfen, ob einer Auskunft Versagungsgründe nach § 31 Abs. 2 LVfG entgegenstehen. Hierbei sind die schutzwürdigen Belange und Interessen sachgerecht gegeneinander abzuwägen.

Diese Verfahrensweise hat im übrigen auch am 5. Februar 1993 der Bundestag für Auskünfte durch das Bundesamt für Verfassungsschutz aufgrund eines entsprechenden Beschlusses des Innenausschusses[60] empfohlen. Er hat klargestellt, daß auch bei Nichtdarlegung des „besonderen Interesses" eine Auskunftserteilung möglich ist.

Staatsanwaltschaft

In besonderer Weise wird die Staatsanwaltschaft durch die spezialrechtliche Regelung der Zugangsrechte im Ausführungsgesetz zum Gerichtsverfassungsgesetz (AGGVG) begünstigt. Bereits im Vorjahr hatten wir berichtet, daß der Auskunftsanspruch der Betroffenen auf Dateien, und dies auch nur bei abgeschlossenen Verfahren, beschränkt wurde. Zugangsrechte während laufender Verfahren, sowie Auskunfts- und Einsichtsrechte bei Akten bleiben durch Verweis auf das „Verfahrensrecht" nahezu ungeregelt, da die Strafprozeßordnung und die sie interpretierenden Richtlinien über das Straf- und Bußgeldverfahren diesen Bereich nur dürftig abdecken.

Aber selbst der verbleibende Anspruch auf Auskunft aus Dateien der Staatsanwaltschaft macht im Vollzug offensichtlich Schwierigkeiten.

Auf Ersuchen der Bürger um Auskunfts- und Akteneinsicht reagierte die Staatsanwaltschaft mit der Mitteilung der Aktenzeichen der registrierten Ermittlungsverfahren sowie dem Hinweis auf § 147 Strafprozeßordnung (StPO), nach dem eine Akteneinsicht nur über einen Rechtsanwalt erfolgen könne.

Auf unseren Hinweis, diese aus dem staatsanwaltschaftlichen Informationssystem ASTA erfolgte Auskunft sei ungenügend, wurde geltend gemacht, daß dort neben dem Aktenzeichen selbst nur noch die rechtliche Qualifikation enthalten sei. Auf eine Mitteilung dazu könne verzichtet werden, da diese Vorwürfe den Betroffenen aus den Einstellungsverfügungen bekannt seien. Dem ist entgegenzuhalten, daß der Auskunftsanspruch von der Kenntnis der Betroffenen unabhängig ist, denn nur aufgrund einer vollständigen Auskunft hat der Betroffene die Möglichkeit zu überprüfen, ob die gespeicherten Daten zutreffen und seine Rechte nicht verletzen. Die Senatsverwaltung für Justiz hat sich unserer Auffassung angeschlossen.

Es bleibt die Frage, in welchem Umfang Auskunft aus Akten bzw. Akteneinsicht zu erteilen ist. Der im AGGVG enthaltene Verweis auf das Bundesrecht geht bislang nahezu ins Leere. Eingeräumt wird bisher lediglich, daß der Betroffene einen Anspruch auf Entscheidung nach pflichtgemäßen Ermessen über Auskünfte bzw. Einsicht nach abgeschlossenen Verfahren hat. Solange die bundesrechtliche Rechtslage noch unbefriedigend ist, sollte von dieser Möglichkeit im Sinne der informationellen Selbstbestimmung möglichst großzügig Gebrauch gemacht werden.

Auskunftsersuchen bei der Staatsanwaltschaft warfen erneut ein Problem auf, das früher schon Gegenstand datenschutzrechtlicher Erörterung war:

Informationszugangsrechte kommen nur den Betroffenen zu. Dies wirft die Frage auf, in welchem Verfahren die Identität des Betroffenen zu überprüfen ist. Die Empfehlung der Datenschutzbeauftragten geht dahin, die Auskünfte postalisch als „Einschreiben - eigenhändig" zu versenden. Bei diesem Verfahren übernimmt die Post die Überprüfung, ob der Adressat tatsächlich persönlich die Sendung entgegennimmt.

Demgegenüber ist die Staatsanwaltschaft dazu übergegangen, Antragsteller persönlich vorzuladen, sie um Vorlage des Personalausweises zu bitten und dabei auch die Identität zu überprüfen. Dieses Verfahren führt natürlich zu einem Erschwernis für den Bürger. Auf unseren Hinweis, die Angabe entsprechender identifizierender Daten durch den Bürger genüge für die Überprüfung, erwiderte die Staatsanwaltschaft, daß der Bürger alternativ die Kopie des Personalausweises seinem Auskunftsersuchen beilegen könne. Dieses Verfahren ist zumutbar, allerdings sollte jedenfalls dann, wenn Auskünfte über sensible Daten erteilt werden, gleichwohl die Versendungsart „Einschreiben - eigenhändig" gewählt werden.

Polizei und Ordnungsbehörden

Bei der grundlegenden Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG) im Jahre 1992 wurde der Auskunftsanspruch des Datenschutzgesetzes übernommen. Die Auskunft kann nur abgelehnt werden, wenn eine Abwägung im Einzelfall ergibt, daß die schutzwürdigen Belange der betroffenen Personen hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter zurücktreten müssen. Beschnitten wurde dagegen auch hier das Recht des Bürgers, neben der Auskunft auch Akteneinsicht zu verlangen. Sie steht nunmehr im Ermessen der Behörden.

In der Praxis des Polizeipräsidenten führt das dazu, daß ein Bürger auf sein Auskunftsersuchen eine Auflistung der im Informationssystem Verbrechensbekämpfung (ISVB) enthaltenen Vorgängen (Ermittlungen, Anzeigen usw.) erhält. Die übrigen im Computerausdruck enthaltenen Daten werden ebensowenig mit-

59 13. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz, Ziff. 19.1
60 BT-Drs. 12/4094

geteilt wie die in der Kriminalakte enthaltenen. Inzwischen erteilt der Polizeipräsident auch Auskunft über in Kriminalakten gespeicherte Daten. Dies geschieht allerdings nur in allgemeiner Form. Um vollständig über die Informationen Kenntnis zu erhalten, über die die Polizei verfügt, muß der Bürger auf seinem Einsichtsrecht bestehen.

Daß dies nicht unbedingt zum Erfolg führt, zeigt die Praxis der Ausländerbehörde.

Wird von einem Ausländer ein längerer Aufenthalt in der Bundesrepublik angestrebt, benötigt er in der Regel ein Visum. Dieses wird ihm von der jeweiligen deutschen Auslandsvertretung nur erteilt, wenn die örtlich zuständige Ausländerbehörde, in Berlin das Landeseinwohneramt, hierfür ihre Zustimmung erteilt.

Ein Rechtsanwalt wies darauf hin, daß die Ausländerbehörde nach Ablehnung der Empfehlung weder dem Antragsteller noch seinem Rechtsbeistand Akteneinsicht gewähre.

Begründet wurde diese Praxis zunächst damit, daß es sich bei der Bearbeitung der Einreisevorgänge durch die Berliner Ausländerbehörde lediglich um Mitwirkungshandlungen für die Entscheidungen der deutschen Auslandsvertretungen handele, die keine Außenwirkung hätten. Die Visaangelegenheiten seien damit allein als Vorgänge des Auswärtigen Amtes zu bewerten. Dieses Argument wurde allerdings nicht aufrechterhalten, vielmehr wurde eingeräumt, daß der Auskunftsanspruch unabhängig davon besteht, um welche Form des Verwaltungshandelns es sich handelt.

Allerdings weigert sich die Ausländerbehörde pauschal, auch Akteneinsicht in die Einreisevorgänge zu gewähren. Die ordnungsgemäße Aufgabenerfüllung der arbeits- und publikumsintensiven Ausländerbehörde sei es abträglich, wenn diese zusätzlich dadurch belastet werde, daß sie Akteneinsicht entweder in ihren Räumen oder durch Herausgabe der Akte an die Rechtsvertreter gewähren würde. § 50 Abs. 6 ASOG überläßt zwar die Akteneinsicht dem Ermessen der Behörde, die pauschale Verweigerung der Akteneinsicht stellt jedoch keine rechtmäßige Form der Ermessensausübung dar und wurde deshalb beanstandet.

3.2 Privatisierung öffentlicher Aufgaben zu Lasten des Datenschutzes?

Die drastischen Sparzwänge zwingen auch die öffentlichen Stellen des Landes Berlin zunehmend, ihre Aufgaben kritisch zu sichten und im Zuge einer *„Verschlankung" der Verwaltung (lean administration)* ihre Datenverarbeitung ganz oder teilweise auf Private zu verlagern. Dabei spielen in Berlin die seit längerem angestellten Überlegungen für eine Verwaltungsreform ebenso eine Rolle wie bundesweit die Bemühungen, öffentliche Verwaltungen stärker nach betriebswirtschaftlichen Kriterien („Unternehmen Stadt") zu organisieren. Derartige Bestrebungen sind auch im Ausland zu beobachten. So soll etwa in Großbritannien die Datenverarbeitung sowohl der Polizei als auch der gesamten Steuerverwaltung bereits in diesem Jahr auf Privatunternehmen ausgelagert werden. Ein solcher Schritt wäre in der Bundesrepublik nur nach einer Änderung des Grundgesetzes möglich, weil dieses die Steuerverwaltung den Finanzbehörden des Bundes und der Länder zuweist. Auch die Übertragung hoheitlicher Befugnisse nicht nur der Polizei, sondern der öffentlichen Verwaltung schlechthin auf Private ist nur durch Gesetz oder aufgrund eines Gesetzes durch einen förmlichen Beleihungsakt möglich. Derartige „beliehene Unternehmen" sind etwa die Notare, der Technische Überwachungsverein Berlin-Brandenburg, die Berliner Börse und die Bezirksschornsteinfegermeister. Sie gelten als öffentliche Stellen im Sinne des Berliner Datenschutzgesetzes.

Dem steht die Verlagerung der Datenverarbeitung oder der damit zusammenhängenden Aufgaben auf Private gegenüber. Sie wirft erhebliche datenschutzrechtliche Probleme auf. Sie beruhen darauf, daß in der Bundesrepublik nach geltendem Datenschutzrecht die öffentlichen Datenverarbeiter erheblich strengeren Regeln unterliegen als die nichtöffentlichen Datenverarbeiter. Möglicherweise wird dieses deutliche Datenschutzgefälle durch eine Anhebung des Datenschutzstandards im privaten Bereich ausgeglichen werden müssen, wenn die europäische Datenschutzrichtlinie verabschiedet werden sollte. Solange das Gefälle jedoch vorhanden ist, darf eine völlige oder teilweise Privatisierung der Verarbeitung personenbezogener Daten oder der öffentlichen Aufgaben, zu deren Zweck solche Daten verarbeitet werden müssen, die Stellung des Bürgers nicht verschlechtern.

Um dies sicherzustellen, enthalten sowohl das Berliner Datenschutzgesetz als auch das Bundesdatenschutzgesetz Bestimmungen, die eine *„Flucht des öffentlichen Datenverarbeiters ins Privatrecht"* verhindern oder jedenfalls negativen Folgen für die betroffenen Bürger vorbeugen sollen. So finden sich in allen Datenschutzgesetzen seit jeher Regeln über die Auftragsdatenverarbeitung, die ursprünglich für das Verhältnis zwischen einer öffentlichen Stelle, der die personenbezogenen Daten zustehen („Herrin der Daten"), und einem (öffentlichen) Rechenzentrum bestimmt waren: Insbesondere sind die Daten nur nach Maßgabe der Weisungen der speichernden Stelle zu verarbeiten. Die Weitergabe der Daten zwischen Auftraggeber und Auftragnehmer wird nicht als Übermittlung angesehen, für die besondere Voraussetzungen gelten. Der Auftragnehmer ist kraft gesetzlicher Fiktion Teil der auftraggebenden Stelle. Alles was der Auftragnehmer tut, und mithin auch die datenschutzrechtlichen Mängel, die bei ihm festgestellt werden, werden dem Auftraggeber zugerechnet.

Für den immer häufigeren Fall, daß ein Privater mit der Datenverarbeitung beauftragt werden soll, enthält das Berliner Datenschutzgesetz besondere Regelungen (§ 3 Abs. 4). Er muß sich gegenüber der öffentlichen Stelle, der die Daten zustehen, vertraglich verpflichten, daß er selbst die Vorschriften des Berliner Datenschutzgesetzes zusätzlich zu den für ihn ohnehin geltenden Vorschriften des Bundesdatenschutzgesetzes befolgt und sich, sofern er seinen Sitz in Berlin hat, der Kontrolle des Berliner Datenschutzbeauftragten unterwerfen. Wird die Datenverarbeitung in einem anderen Bundesland durchgeführt, muß der Auftraggeber sicherstellen, daß sich der Auftragnehmer der Kontrolle des jeweiligen Landesbeauftragten unterwirft. Der Auftraggeber hat den Datenschutzbeauftragten und die Aufsichtsbehörde nach dem Bundesdatenschutzgesetz über die Beauftragung zu unterrichten.

Diese Regelungen machen das Bestreben des Gesetzgebers deutlich, den hohen Datenschutzstandard für den öffentlichen Bereich auch auf private Auftragnehmer von öffentlichen Stellen des Landes Berlin zu erstrecken. In der Praxis erfolgt dies durch detaillierte vertragliche Bestimmungen, die in die ohnehin abzuschließenden Verträge zwischen dem Auftragnehmer und dem Auftraggeber aufgenommen werden müssen. Die öffentliche Stelle kann sich im Fall der Auftragsdatenverarbeitung allerdings auch durch Abschluß solcher Verträge nicht ihrer datenschutzrechtlichen Verantwortung entledigen. In den Verträgen hat sie ausreichende Möglichkeiten zur Kontrolle des Auftragnehmers anzusehen, die z. B. dem behördlichen Datenschutzbeauftragten des Auftraggebers die Wahrnehmung seiner Aufgaben auch beim Auftragnehmer ermöglichen, u. a. die Kontrolle der Wahrnehmung der Auftragskontrolle gem. § 5 Abs. 3 Nr. 8 BlnDSG durch den Auftragnehmer. Nicht selten erhoffen sich öffentliche Stellen durch die Beauftragung privater Datenverarbeiter starke Einsparungseffekte, ohne dabei zu berücksichtigen, daß die öffentliche Stelle für die Datenverarbeitung rechtlich verantwortlich bleibt und Personal für die Überwachung des privaten Auftragnehmers bereithalten muß.

Nicht jeder Auftrag zur Datenverarbeitung, den eine öffentliche einer nicht-öffentlichen Stelle erteilt, ist jedoch auch datenschutzrechtlich als Datenverarbeitung im Auftrag einzuordnen.

Überträgt nämlich die Verwaltungsbehörde dem Privatunternehmen nicht nur Datenverarbeitungsprozesse (z. B. die Erhebung bestimmter Daten oder das Erfassen und Auswerten von Belegen), sondern eine ihrer Aufgaben vollständig einschließlich der dazu notwendigen Datenverarbeitung, so ist dies - im Gegensatz zur Auftragsdatenverarbeitung - eine *Funktionsübertragung.* Die Weitergabe von Daten ist in diesem Fall als Datenübermittlung einzuordnen, die nach dem Berliner Datenschutzgesetz nur zulässig ist, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat (§ 13). Diese strengen Voraussetzun-

gen an eine Datenübermittlung an Stellen außerhalb des öffentlichen Bereiches sind deshalb gerechtfertigt, weil die Daten der Betroffenen nach dieser Übermittlung nur noch den weniger strengen Regeln des 3. Abschnitts des Bundesdatenschutzgesetzes unterliegen, so daß die Rechtsstellung der Betroffenen durch eine solche Übermittlung wesentlich verschlechtert wird. Der private Übermittlungsempfänger unterliegt zudem nicht mehr der Kontrolle durch den Berliner Datenschutzbeauftragten.

Die Abgrenzung zwischen Auftragsdatenverarbeitung und Funktionsübertragung bereitet in der Praxis Schwierigkeiten. Zwei Beispiele mögen dies verdeutlichen:

Die *Berliner Verkehrsbetriebe (BVG)* haben im vergangenen Jahr ein privates Wachschutzunternehmen mit der Beratung von Fahrgästen, aber auch mit der Fahrscheinkontrolle beauftragt, die bisher ausschließlich von BVG-Mitarbeitern (Schaffnern im Kontrolldienst) durchgeführt wurde. Hintergrund für diese Maßnahme war das Bestreben der BVG, sowohl Kosten im eigenen Bereich einzusparen (vor allem auch die Verarbeitung der Daten von „Schwarzfahrern" auszulagern), als auch die Fahrscheinkontrolle effektiver zu gestalten. Die Mitarbeiter der privaten Wachschutzfirma sollen die Daten von Personen, die ohne Fahrschein angetroffen werden, auf von der BVG zur Verfügung gestellten Blocks erfassen und diese Daten in demselben Umfang wie bisher die BVG nach deren Weisung verarbeiten. Falls der Kunde sich weigert, daß erhöhte Beförderungsentgelt zu zahlen, wird dies der BVG mitgeteilt, die den Kunden daraufhin vor den Zivilgerichten verklagen muß.

Wir haben die Beauftragung des privaten Wachschutzunternehmens als Datenverarbeitung im Auftrag der BVG eingestuft und verlangt, daß der entsprechende Vertrag ergänzt wurde, um die datenschutzrechtliche Verantwortlichkeit der BVG klarzustellen. Diese muß das Recht haben, mit eigenem Personal die Tätigkeit des privaten Wachschutzunternehmens jederzeit und ohne Vorankündigung zu überprüfen. Jedes Fehlverhalten eines Mitarbeiters der Privatfirma wird datenschutzrechtlich unmittelbar der BVG zugerechnet. Schon aus diesem Grund wird der von der BVG beabsichtigte Einsparungseffekt im Personalbereich nur zum Teil eintreten, weil das private Wachschutzunternehmen seinerseits überwacht werden muß. Die Daten von „Schwarzfahrern" dürfen von dem privaten Auftragnehmer nicht länger gespeichert werden als dies die BVG darf. Der private Auftragnehmer unterliegt selbst der Kontrolle durch den Berliner Datenschutzbeauftragten.

Inzwischen ist die BVG auch dazu übergegangen, die nächste Phase der Eintreibung der erhöhten Beförderungsentgelte bis zur gerichtlichen Geltendmachung auf ein Privatunternehmen, und zwar ein bundesweit tätiges, in Frankfurt ansässiges Inkasso- und Auskunftei-Büro zu übertragen. Dies kann nicht mehr als Datenverarbeitung im Auftrag angesehen werden, zumal die Datenverarbeitung nicht mehr in Berlin, sondern in Frankfurt stattfindet und sich deshalb schon räumlich einer direkten Kontrolle durch die BVG entzieht. Im übrigen haben die Datenschutzbeauftragten und die Aufsichtsbehörden für den privaten Bereich seit jeher die Weitergabe von Daten an Dritte für Zwecke des Inkassos als echte Datenübermittlung - und nicht als Datenverarbeitung im Auftrag - angesehen. Mithin ist die Weitergabe von Schwarzfahrerdaten an das private Inkasso-Unternehmen durch die BVG nur aufgrund einer Rechtsvorschrift. Das am 1. Januar 1994 in Kraft getretene *Berliner Betriebe-Gesetz (BerlBG)* enthält eine Befugnis zur Verarbeitung (und damit auch zur Übermittlung) personenbezogener Daten zur Verfolgung von Forderungen, die den Betrieben (u. a. der BVG) zustehen. Die ergänzende Rechtsverordnung, die nach dem früheren Eigenbetriebsgesetz in der Fassung des Artikelgesetzes bis zum 31. Dezember 1993 hätte erlassen werden müssen, steht noch aus.

Die Senatsverwaltung für Verkehr und Betriebe hat nach dem Ende des Berichtszeitraumes allerdings den Entwurf einer entsprechenden Rechtsverordnung vorgelegt, der aufgrund unserer Empfehlung auch regelt, in welchem Umfang personenbezogene Daten von der BVG an ein privates Inkasso-Unternehmen übermittelt werden dürfen. In jedem Fall muß sichergestellt werden, daß das Inkasso-Unternehmen, das gleichzeitig als Auskunftei tätig ist, die von der BVG übermittelten Daten nur zur Eintreibung der erhöhten Beförderungsentgelte verwendet und nicht zugleich auch für ihre Tätigkeit als Auskunftei nutzt. Diese Verpflichtung hat das Inkasso-Unternehmen aufgrund unseres Hinweises gegenüber der BVG vertraglich übernehmen müssen.

Auch das *Landesamt zur Regelung offener Vermögensfragen (LAROV)* ist bemüht, Privatfirmen verstärkt bei der Aufgabenerledigung zu beteiligen. Zum einen soll eine private Beratungsgesellschaft zur Beschleunigung der Verfahren im Zusammenhang mit der Behandlung von Mauergrundstücken eine Kartendarstellung anfertigen und zu diesem Zweck Einsicht in die Liegenschaftszeichnungen und Liegenschaftsbücher der Vermessungs- und Liegenschaftsämter nehmen. Zum anderen soll dieselbe Gesellschaft zur beschleunigten Untersuchung der als Standorte für künftige Bundesministerien vorgesehenen Grundstücke das gesamte Rückübertragungsverfahren nach dem Vermögensgesetz bis zur Entscheidungsreife durchführen.

Während das erste Vorhaben als Auftragsdatenverarbeitung anzusehen und bei einer vertraglichen Festlegung der genauen Zugriffsrechte des privaten Unternehmens auf Daten in den Liegenschaftskatastern zulässig war, soweit nach Abschluß der vertraglichen Leistungen alle im Zusammenhang mit dem Vertrag gespeicherten personenbezogenen Daten dem LAROV übergeben werden, handelt es sich bei dem zweiten „Auftrag" nicht um eine bloße Auftragsdatenverarbeitung. Der privaten Beratungsfirma soll in diesem Fall gerade nicht nur ein Teilbereich der Datenverarbeitung ohne eigene Entscheidungsbefugnis übertragen werden, sie soll vielmehr für bestimmte Grundstücke nahezu das gesamte Verfahren einschließlich bestimmter Amtsermittlungshandlungen für das LAROV durchführen, das seinerseits nur noch die vorbereiteten Bescheide erlassen soll. Eine Beleihung des privaten Beratungsunternehmens hat nicht stattgefunden. Sie wäre auch nur aufgrund einer gesetzlichen Regelung zulässig, die nicht vorhanden ist. Deshalb dürfen dem Beratungsunternehmen für die Vorbereitung von Rückerstattungsbescheiden personenbezogene Daten erst dann übermittelt werden, wenn das Vermögensgesetz um eine entsprechende Befugnis ergänzt worden ist.

Besondere Probleme ergeben sich, wenn die Verwaltung Privatunternehmen mit der Verarbeitung solcher personenbezogenen Daten betrauen will, die *Berufs- oder besonderen Amtsgeheimnissen* (z. B. dem Steuer-, Sozial-, Statistik-, Personaldaten- oder Meldegeheimnis oder der ärztlichen Schweigepflicht) unterliegen. Solche besonders sensiblen Daten unterliegen speziellen Geheimhaltungsvorschriften, die teilweise eine Verarbeitung durch Private völlig ausschließen, teilweise - wie das Sozialgeheimnis - nur unter besonders engen Voraussetzungen zulassen.

Für die Verarbeitung von *Patientendaten in öffentlichen Krankenhäusern* gilt der Grundsatz, daß sie nur einer anderen medizinischen Einrichtung, nicht aber einer anderen öffentlichen Stelle oder gar einem Privatunternehmen übertragen werden darf. Über das besondere Problem der Verwaltung von Patientenunterlagen der ehemaligen Einrichtungen des ambulanten Gesundheitswesens (Polikliniken) in den östlichen Bezirken haben wir bereits im Vorjahr berichtet[61]. Dabei mußten beispielsweise in einem Ost-Berliner Bezirk mindestens 2 Millionen Patientenakten gesichtet und erfaßt werden, damit der Bezirk als verantwortliche Stelle seinen gesetzlichen Auskunftspflichten nachkommen konnte. Diese Aufgabe wurde - mit unserer Billigung - in diesem und mehreren anderen östlichen Bezirken einer privaten *Beschäftigungs- und Qualifizierungsgesellschaft* und einer *Beschäftigungsinitiative* übertragen, die mit ABM-Mitteln der Arbeitsverwaltung und Vorgaben der Gesundheitsverwaltung unter ärztlicher Leitung die Erfassung und Sichtung der Patientenunterlagen durchzuführen hatten. Die Archivierung der Akten in den ehemaligen Polikliniken wurde von ärztlichem Personal geleitet und beaufsichtigt.

Vergleichbare private Gesellschaften sind auch in großem Umfang im Umweltschutzbereich tätig, um etwa für die bezirklichen Umweltämter *Altlastenkataster* oder für die Stadtplanungs-

61 Jahresbericht 1992, 4.1

ämter *Planungsdateien* zu erstellen. In derartigen Fällen können die privaten Stellen - selbst wenn sie im Auftrag einer öffentlichen Stelle Daten beim Bürger erheben - die Auskunft nicht erzwingen. Soweit gesetzlich nichts anderes bestimmt ist (z. B. in § 138 Baugesetzbuch für die Auskunftspflicht bei städtebaulichen Sanierungsmaßnahmen), können private Daten im Auftrag öffentlicher Stellen nur auf freiwilliger Basis erheben und müssen die Betroffenen darauf auch hinweisen. Ebenso müssen sie die Betroffenen auf etwaige Auskunftsverweigerungsrechte hinweisen, die gegenüber der auftraggebenden Stelle bestehen, wenn der Betroffene durch die Auskunft sich oder seine Angehörigen der Gefahr strafgerichtlicher Verfolgung und eines Bußgeldverfahrens aussetzen würde[62].

Soweit die Verwaltung erwägt, die *Textverarbeitung* zur Erstellung amtlicher Schreiben auf private Schreibbüros zu verlagern, sind ihr auch dabei enge Grenzen gesetzt. Dies ist allenfalls zulässig für konkret begrenzte Schreibaufträge, bei denen - z. B. in einem Planfeststellungsverfahren - massenhaft Schreiben an Bürger nach genauen Weisungen der auftraggebenden öffentlichen Stelle gefertigt werden müssen. Dagegen scheidet eine auftragsweise Textverarbeitung durch private Schreibbüros in all den Verwaltungsbereichen aus, in denen personenbezogene Daten verarbeitet werden, die Berufs- und besonderen Amtsgeheimnissen unterliegen.

Zunehmend bilden *öffentliche Stellen des Bundes und der Länder auch privatrechtliche Vereinigungen* (z. B. einen Nahverkehrsverbund), die Aufgaben der öffentlichen Verwaltungen wahrnehmen. Auch für solche Fallgestaltungen hat der Bundesgesetzgeber eine Regelung getroffen, die verhindern soll, daß öffentliche Stellen durch solche Vereinigungen vor dem für sie geltenden strengen Datenschutzrecht „in das Privatrecht fliehen" können. Soweit derartige Vereinigungen nämlich entweder über den Bereich eines Landes hinaus tätig werden (etwa bei einem zukünftigen Nahverkehrsverbund Berlin-Brandenburg) oder dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht, gelten solche Vereinigungen auch dann als öffentliche Stellen des Bundes, wenn Private sich an ihnen beteiligen. Liegt eine der beiden genannten Voraussetzungen (länderübergreifende Tätigkeit oder Mehrheitsanteile des Bundes) nicht vor, so gelten solche Vereinigungen als öffentliche Stellen der Länder, falls Berlin an ihnen beteiligt ist, also als öffentliche Stelle Berlins, die dem Berliner Datenschutzgesetz unterliegt (§ 2 Abs. 3 BDSG). Im einzelnen wird noch zu prüfen sein, welche Auswirkungen diese Bestimmungen auf die zahlreichen Unternehmen des privaten Rechts hat, an denen das Land Berlin mehrheitlich oder sogar zu 100% beteiligt ist[63]. Jedenfalls entscheidet nicht die Rechtsform eines Datenverarbeiters darüber, ob er als öffentliche oder als nicht-öffentliche Stelle anzusehen ist. Es kommt vielmehr darauf an, inwieweit er Aufgaben der öffentlichen Verwaltung wahrnimmt und ob der Bund oder das Land Berlin mit beherrschendem Einfluß Anteilseigner oder Stimmberechtigte in den Unternehmensorganen sind.

4. Ausgewählte Geschäftsbereiche

4.1 Arbeit und Frauen

Genomanalyse im Arbeitsverhältnis

Die Bundesregierung hat am 3. November 1993 den Entwurf eines *Arbeitsschutzrahmengesetzes (ASRG)* beschlossen, der gegenwärtig in Bundestag und Bundesrat beraten wird[64]. Der Gesetzentwurf regelt die Durchführung von Vorsorgeuntersuchungen bei Beschäftigten und enthält in diesem Zusammenhang die ausdrückliche Bestimmung, daß Untersuchungen zur bloßen Aufdeckung von Erbanlagen der untersuchten Person „nicht durchgeführt werden dürfen" (§ 22 Abs. 2). Diese grundsätzliche Festlegung wird jedoch dadurch relativiert, daß der Gesetzentwurf Untersuchungen zulassen will, durch die ererbte Veranlagungen für Erkrankungen zu ermitteln sind, die an einem bestimmten Arbeitsplatz oder bei einer bestimmten Tätigkeit entstehen können. Die am einschneidendsten in den Persönlichkeitskern des Arbeitnehmers eingreifende Methode der DNA-Analyse, bei der der gesamte Bauplan der menschlichen Zelle offengelegt wird, soll nur bei ausdrücklicher Zulassung durch ein Gesetz erlaubt sein. Zusätzlich zu der gesetzlichen Grundlage muß nach gesicherten Erkenntnissen der Arbeitsmedizin eine schwere bleibende Schädigung möglich sein; die Beschäftigten müssen nach umfassender Aufklärung über die Untersuchungen und die durch sie möglicherweise bekanntwerdenden Erbanlagen schriftlich in die Untersuchung eingewilligt haben.

Die vorgesehene Regelung trägt dem Recht auf informationelle Selbstbestimmung des Arbeitnehmers, das auch ein Recht auf Nichtwissen bezüglich seiner genetischen Anlagen einschließt, nicht genügend Rechnung. Wir haben deshalb in unserer Stellungnahme gegenüber der Senatsverwaltung für Soziales betont, daß eine Genomanalyse an Arbeitnehmern, selbst wenn sie nur unter noch so eng formulierten Voraussetzungen durchgeführt werden darf, stets die Freiheit berührt, selbst darüber zu entscheiden, ob man über anlagebedingte und damit unausweichliche Risiken für die eigene Gesundheit informiert werden will oder nicht. Die im Gesetzentwurf vorgesehene schriftliche Einwilligung des Arbeitnehmers wird selten in voller Entscheidungsfreiheit erteilt werden, weil diese im Verhältnis zwischen Arbeitnehmer und Arbeitgeber häufig nicht vorhanden ist. Noch extremer ist die Situation des Stellenbewerbers, für den der Entwurf des Arbeitsschutzrahmengesetzes keine Regelungen enthält.

Der Gesetzentwurf der Bundesregierung mit seinem grundsätzlichen Verbot der Genomanalyse an Arbeitnehmern mit Erlaubnisvorbehalt unter engen Voraussetzungen ermöglicht langfristig eine Entwicklung, in der Arbeitgeber mit Hilfe der neuen Untersuchungsmethoden die Widerstandsfähigsten unter ihren Arbeitnehmern für gesundheitsgefährdende Arbeitsplätze aussuchen könnten.

Demgegenüber sollte nach den Grundsätzen des objektiven Arbeitsschutzrechts der Arbeitgeber verpflichtet bleiben, die Arbeitsplätze seinerseits so zu gestalten, daß das Risiko einer Erkrankung von vornherein ausgeschlossen oder auf ein Minimum begrenzt ist[65].

Beschneidet der Datenschutz die Rechte der Frauen?

Das Landesgleichstellungsgesetz (LGG) - zuvor: Landesantidiskriminierungsgesetz (LADG) - gewährt der Frauenvertreterin erhebliche Rechte im Bereich des Personalwesens. § 17 LGG umschreibt die Befugnisse, die der *Frauenvertreterin* hierfür eingeräumt werden. Neben der allgemeinen Verpflichtung, die Frauenvertreterin am Auswahlverfahren zu beteiligen, hat die Dienststelle der Frauenvertreterin die Teilnahme an Bewerbungsgesprächen zu ermöglichen, Einsicht in Bewerbungsunterlagen zu gewähren sowie Auskunft in allen mit ihren Aufgaben im Zusammenhang stehenden Angelegenheiten zu erteilen.

Diese Befugnisse, die von einer Einwilligung der Betroffenen unabhängig sind, greifen in der Tat in die informationelle Selbstbestimmung der Bediensteten und der Bewerber ein. In einer Reihe von Fällen ist daher die Frage aufgeworfen worden, ob diese Befugnisse nicht im Hinblick auf den Datenschutz restriktiv auszulegen sind.

So vertritt die Senatsverwaltung für Schule, Berufsbildung und Sport die Auffassung, daß die Frauenvertreterinnen nicht das Recht hätten, an den bei Bewerbungsverfahren im Schulbereich regelmäßig stattfindenen *Unterrichtsbesuchen der Schulaufsicht* teilzunehmen. Diese Vorführstunden seien nicht Teil der Bewerbungsgespräche, sondern Vorgänge außerhalb des Bewerbungsverfahrens. Tatsächlich kommt dem Ergebnis der Unterrichtsbesuche eine ganz erhebliche Bedeutung bei der endgültigen Bewerberauswahl zu. Von Seiten des Datenschutzes kann nicht entschieden werden, in welchem Umfang den Frauenvertreterinnen die Teilnahme an allen Verfahrensteilen gewährt werden muß, die bei Personalentscheidungen eine Rolle spielen. Datenschutzrechtlich kann allerdings eine Beschränkung der Beteiligungsrechte nicht begründet werden; § 17 LGG enthält für alle Formen der Beteiligung hinreichende Rechtsgrundlagen.

62 vgl. z. B. § 52 Abs. 5 BImSchG

63 vgl. den 9. Bericht über Beteiligungen des Landes Berlin an Wirtschaftsunternehmen (Stand: 31. Dezember 1991), Drs. 12/3375

64 BR-Drs. 792/93

65 vgl. Jahresbericht 1989, 2.3

Ähnlich ist die Frage zu beurteilen, ob die der Frauenvertreterin gewährte *„Einsicht in Bewerbungsunterlagen"* auch die Einsicht in die entsprechenden Personalakten umfaßt bzw. ob für die Einsicht eine ausdrückliche Zustimmung des Betroffenen erforderlich ist. Geht man richtigerweise davon aus, daß zu den Bewerbungsunterlagen alle Unterlagen gehören, die von der Dienstbehörde zur Entscheidung über die Personalauswahl herbeigezogen werden, steht es außer Zweifel, daß jedenfalls dann, wenn dies geschieht, die Personalakten zu den Bewerbungsunterlagen gehören. Ob und wann dies allerdings der Fall ist, hängt von den Umständen ab. Da jedenfalls bei externen Bewerbungen die Beiziehung der Personalakte die Zustimmung der Betroffenen voraussetzt, hängt hier in der Tat das Einsichtsrecht der Frauenvertreterin mittelbar vom Betroffenen ab. Wird dagegen bei internen Bewerbungen möglicherweise ohne ausdrückliche Zustimmung des Betroffenen die Personalakte in den Auswahlvorgang einbezogen, steht der Frauenvertreterin von Gesetzes wegen ein Einsichtsrecht zu. Die Bestimmung des § 17 Abs. 2 4. Anstrich stellt insoweit eine Befugnisnorm zur Nutzung der Personaldaten dar (§ 14 Abs. 2 Ziff. 1 des hier anzuwendenen BDSG).

Das Recht der Frauenvertreterin auf *Auskunft* in allen mit ihren Aufgaben im Zusammenhang stehenden Angelegenheiten (§ 17 Abs. 2 5. Anstrich LGG) unterliegt dem Erforderlichkeitsprinzip. Allerdings sind der Frauenvertreterin so viele Daten zur Verfügung zu stellen, wie diese zu ihrer Aufgabenerfüllung benötigt. Uns sind demgegenüber Praktiken bekannt geworden, die der Aufgabe der Frauenvertreterin widersprachen und auch datenschutzrechtlich nicht geboten sind: So wurde bei Unterlagen über die Durchführung von Fortbildungsmaßnahmen nur die Tatsache der Maßnahme, nicht aber ihr Inhalt und Zweck bekanntgegeben.

Ein anderer Konflikt entstand bei der Frage, ob bei dem *Beanstandungsverfahren* bei angenommenen Verstößen gegen das LGG die Frauenvertreterin berechtigt ist, an das für Frauenpolitik zuständige Mitglied des Senats personenbezogene Daten zu übermitteln. Die Senatsverwaltung ist der Auffassung, sie könne diese Aufgabe auch ohne Personenbezug erledigen. Da diese selbst über den erforderlichen Umfang der für ihre Entscheidung zu verwendenden Daten zu bestimmen hat, folgt daraus, daß die Frauenvertreterinnen bei der Übermittlung von Unterlagen im Beanstandungsverfahren die Daten anonymisieren müssen. Die damit verbundenen Arbeiten müssen aus datenschutzrechtlichen Gründen hingenommen werden.

4.2 Bau- und Wohnungswesen

Ist der Berliner Datenschutzbeauftragte mieterfeindlich?

Große Aufregung verursachten verschiedene Presseerklärungen, mit denen bekannt wurde, daß einige Wohnungsämter der Bezirksämter von Berlin bei einer Antragstellung des Eigentümers auf eine sogenannte Abgeschlossenheitsbescheinigung, die eine der Voraussetzungen für die Umwandlung von Miet- in Eigentumswohnungen ist, die betroffenen Mieter über diese Antragstellung informieren.

Die rechtliche Zulässigkeit dieser gezielten Information wird seitdem zwischen den beteiligten Behörden und Interessenverbänden kontrovers diskutiert. Natürlich sieht auch der Berliner Datenschutzbeauftragte die Notwendigkeit einer möglichst frühzeitigen Information der Mieter über eine eventuell bevorstehende Umwandlung ihrer Wohnung. Allerdings darf dieser Gesichtspunkt nicht dazu führen, bestehende gesetzliche Vorschriften zu umgehen. Die Information der Mieter über die Antragstellung des Eigentümers unterliegt grundsätzlich - bis auf einige Ausnahmen - dem Berliner Datenschutzgesetz. Danach ist zur Datenübermittlung gemäß § 13 BlnDSG eine Rechtsvorschrift bzw. die Einwilligung des Betroffenen nötig. Eine solche klare gesetzliche Grundlage ist nicht vorhanden. Statt sich in öffentlicher Auseinandersetzung zu verlieren, sollten die Beteiligten im Rahmen ihrer Möglichkeiten darauf hinwirken, daß die erforderlichen gesetzgeberischen Aktivitäten in die Wege geleitet werden. Dies wäre eine mieterfreundliche Haltung. Inzwischen liegt ein Gesetzentwurf der Fraktion Bündnis 90/DIE GRÜNEN vor.

Mieterbefragung

*Auch 1993 wurden die Vorbereitung und Durchführung der Befragung zum **Mietspiegel 1994** begleitet. Aufgrund einer telefonischen Vorbefragung von 27 000 Mietern wurden rund 5 000 Interviews im Auftrag der Senatsverwaltung durch ein privates Meinungsforschungsinstitut durchgeführt.*

Im Vorfeld der Untersuchung ergab sich aus der unterschiedlichen Interessenlage der beteiligten Mieter- und Vermieterverbände, daß das Erhebungsprogramm möglicherweise nicht die Streuung der Mieten innerhalb eines vergleichbaren Mietspiegelfeldes erklären kann. Daher wurden die Befragten gebeten, einzuwilligen, möglicherweise Anfang des Jahres 1994 nochmals ergänzend befragt zu werden. Diese Einwilligung ist erforderlich, da im Normalfall bei Befragungen die Hilfsmerkmale (Adressen, Namen) unmittelbar nach einer Plausibilitätsprüfung vom Erhebungsbogen abgetrennt und damit die Daten einer gewissen Anonymisierung unterzogen werden. Eine Deanonymisierung der Angaben zum Zweck einer Nachbefragung ohne Einwilligung der Betroffenen ist datenschutzrechtlich nicht zulässig.

Insbesondere in den östlichen Bezirken wurden im Auftrag der Bezirksämter verschiedene Mieterbefragungen initiiert. Häufig wiesen die Erhebungsbögen Mängel auf. Für derartige Befragungen sollte das Befragungsdesign vom Bezirksamt vorgegeben und damit eine Datenverarbeitung im Auftrag (§ 3 Abs. 4 BlnDSG) vereinbart werden. Mittels Erhebungsbögen und Anschreiben sollten die Betroffenen sowohl über die Freiwilligkeit der Teilnahme als auch über andere Datenschutzfragen - wie z. B. den Verwendungszweck und die Löschung der Daten - informiert werden.

Wohin mit zurückgenommenen Anträgen?

Nachdem ein Bürger gegen die Ablehnung seines Antrags auf Erteilung eines Wohnberechtigungsscheines Widerspruch eingelegt hatte, zog er im Laufe dieses Rechtsbehelfsverfahrens seinen Antrag zurück. Anschließend begehrte er vom bezirklichen Wohnungsamt die Herausgabe sämtlicher Unterlagen.

Das betroffene Bezirksamt vertrat die Auffassung, der durch die Bearbeitung des Antrags entstandene personenbezogene Verwaltungsvorgang müsse beim Wohnungsamt bleiben, da anderenfalls das Verwaltungshandeln nicht nachvollziehbar sei. Da sich im Verwaltungsvorgang keinerlei Originalunterlagen des Bürgers befänden, könne er keine Herausgabe verlangen. Wir konnten das Herausgabebegehren des Bürgers nicht unterstützen, da die Auffassung des Wohnungsamtes insoweit zutreffend ist.

Andererseits ist die Aufbewahrung von Akten nicht unbegrenzt zulässig, da nach § 17 BlnDSG eine Verpflichtung zur Sperrung und Löschung der personenbezogenen Daten besteht, wenn ihre Kenntnis für die datenverarbeitende Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist. Daher müssen über die Dauer der Aktenaufbewahrung Festlegungen getroffen werden, die jedoch von datenverarbeitender Stelle zu datenverarbeitender Stelle aus fachlichen Gründen unterschiedlich sein können. Bei den Wohnungsämtern erfolgt die Aktenaufbewahrung entsprechend den Richtlinien über die Schriftgutverwaltung der Wohnungsämter mittels Mikroverfilmung, nach der mit Ablauf von drei Jahren die Akten zu vernichten sind. Auch die Mikrofilme dürfen jedoch nicht unbegrenzt aufbewahrt werden.

4.3 Finanzen

Abgabenordnung - noch immer keine datenschutzrechtlichen Verbesserungen

Seit 1988 erfolgen zwischen den Finanzministern des Bundes und der Länder Abstimmungen über die Ergänzung und Präzisierung der Datenschutzregelungen in der Abgabenordnung. Hieran sind auch die Datenschutzbeauftragten des Bundes und der Länder beteiligt worden. Bislang bestand Einvernehmen, der neueren Datenschutzgesetzgebung Rechnung zu tragen und den Umgang mit Daten, die dem Steuergeheimnis unterliegen, klarer als bisher zu regeln.

Nach den jahrelangen Arbeiten an dem Entwurf eines Gesetzes zur Änderung der Abgabeordnung und anderer Rechtsvorschriften (AOÄG) stellt nunmehr das Bundesministerium für Finanzen Überlegungen an, die datenschutzrechtlichen Bestimmungen aus dem AOÄG herauszunehmen und zunächst nicht weiterzuverfolgen. Die übrigen Regelungen wurden - mit Ausnahme derjenigen, die das Rechtsbehelfsverfahren betreffen - in den Entwurf eines Gesetzes zur Bekämpfung des Mißbrauchs und zur Bereinigung des Steuerrechtes (StMBG) übernommen und vom Vermittlungsausschuß verabschiedet[66].

Demgegenüber ist daran festzuhalten, daß die Abgabenordnung zum Schutz der Betroffenen und im Interesse der Normenklarheit - auch in Bezug auf die Anwendbarkeit des jeweiligen Landesdatenschutzgesetzes - um detaillierte bereichsspezifische Datenschutzregelungen zu ergänzen ist.

Wir haben die Senatsverwaltung für Finanzen gebeten, den Überlegungen im Bundesministerium der Finanzen entgegenzutreten und sich für die erforderlichen bereichsspezifischen Datenschutzregelungen in der Abgabenordnung einzusetzen.

Kontrollmitteilungen an die Finanzämter

Zur vollständigen Erfassung von Steuerquellen haben seit jeher andere Behörden aufgrund von Verwaltungsvorschriften und Vereinbarungen Kontrollmitteilungen an die Finanzämter über bestimmte, steuerlich relevante Sachverhalte gegeben, so z. B. über Nebentätigkeiten. Für derartige Mitteilungen bestand bisher keine gesetzliche Grundlage[67].

Von der in § 93 a Abgabenordnung (AO) enthaltenen Ermächtigung, durch Rechtsverordnung Behörden und öffentlich-rechtliche Anstalten zur Abgabe derartiger Kontrollmitteilungen zu verpflichten, hat der Bundesminister für Finanzen nunmehr Gebrauch gemacht[68]. Sozialdaten unterfallen nicht der Übermittlungspflicht. Eine Mitteilung soll - mit Ausnahme von wiederkehrenden Bezügen - nur erfolgen, soweit die an denselben Empfänger geleisteten Zahlungen im Kalenderjahr mehr als 3 000,- DM betragen haben. Nach dem Wortlaut der Verordnung ist die Summe der geleisteten Zahlung nicht mitzuteilen. Die mitteilungspflichtige Behörde hat den Betroffenen von ihrer Verpflichtung, Mitteilungen zu erstellen, spätestens bei Übersendung der ersten Mitteilung an die Finanzbehörde zu unterrichten.

Neues vom LAROV

Wir hatten im Jahresbericht 1992[69] über unsere Prüfung beim Landesamt zur Regelung offener Vermögensfragen berichtet.

Das Vermögensgesetz deckt auch nach seiner Novellierung im Juli 1992 die von der Verwaltung für erforderlich gehaltenen Datenübermittlungen nicht ab. Nachdem das Land Berlin in Bonn mit seinen Initiativen zur Ergänzung des Vermögensgesetzes nicht weitergekommen ist, soll nunmehr ein Landes-Ausführungsgesetz zum Vermögensgesetz erlassen werden. Darin sollen die notwendigen Datenübermittlungsbefugnisse, wie sie unter anderem zur Durchführung des Investitionsvorranggesetzes, zu städtebaulichen Sanierungsmaßnahmen und zur Hauptstadtplanung erforderlich sind, aufgenommen werden.

4.4 Gesundheit

Garantien für den Persönlichkeitsschutz der Schwangeren bei der Beratung

Das Bundesverfassungsgericht (BVerfG)[70] hat in seinem Urteil zur Neuregelung des § 218 StGB eine Beratungspflicht angeordnet, sofern die schwangere Frau einen Schwangerschaftsabbruch beabsichtigt.

Die Anordnung umfaßt auch Regelungen, die die Persönlichkeitsrechte der schwangeren Frau im Rahmen der Pflichtberatung gewährleisten sollen. Die schwangere Frau kann auf ihren Wunsch gegenüber der sie beratenden Person anonym bleiben. Die beratende Person hat in einer Weise, die keine Rückschlüsse auf die Identität der Betroffenen erlaubt, in einem Protokoll das Alter, den Familienstand und die Staatsangehörigkeit der Beratenen, die Zahl der Schwangerschaften, ihrer Kinder und frühere Schwangerschaftsabbrüche festzuhalten. Sie hat ferner die für den Abbruch genannten wesentlichen Gründe und die Dauer des Beratungsgesprächs zu vermerken. Das Protokoll muß auch ausweisen, welche Informationen der Schwangeren vermittelt und welche Hilfen ihr angeboten worden sind. Die Protokollierung dient nur der Kontrolle der Beratungsstätigkeit der betreffenden Beratungsstelle, aber nicht der Überprüfung und Bewertung einzelner Abbrüche.

In einer Umfrage bei allen bezirklichen Sozialmedizinischen Diensten Berlins (SMD) hinsichtlich der Umsetzung dieser Grundsätze konnte festgestellt werden, daß in der Regel ein mündlicher Hinweis auf die Anonymität der Beratung bei der *Aufnahme der Beratungsgespräche* stattfindet. Bis auf einen SMD, in dem die schwangeren Frauen ihren Namen nennen müssen, um aufgerufen zu werden, erfolgten die Terminvergabe und das Aufrufen der Schwangeren zum Gespräch anonym.

Bei der *Protokollierung der Beratungsgespräche* wird der Katalog des BVerfG beachtet und nur in zwei Fällen um die Frage nach dem Wohnort - „Berlin" oder „außerhalb Berlins" - erweitert. Darüberhinaus fragt ein SMD nach dem Bezug von Leistungen nach dem Bundessozialhilfegesetz. Hieraus ergibt sich eine unerwünschte Steigerung des Reidentifizierungsrisikos. Allerdings verlangt ein SMD die Vorlage eines Personalausweises zur Identitätsfeststellung. Das hat zur Folge, daß die beratene Frau ihre Anonymität aufgeben muß.

Hinweise auf die *Kostenübernahme* durch das Sozialamt liegen in den meisten Fällen vor. Nur in einem Fall bearbeitet der SMD die Anträge auf Kostenübernahme des Schwangerschaftsabbruchs gemäß Absprache mit dem Sozialamt.

Die *Bescheinigung über den Abschluß der Beratung* wird in allen Fällen von der beratenden Person ausgegeben. In mehr als der Hälfte der befragten Beratungsstellen kann die schwangere Frau ihren Namen selbst in die Bescheinigung eintragen.

Dort, wo die Bescheinigung von der beratenden Person mit dem Namen der beratenen Frau versehen wird, ist die Anonymität der Schwangeren nicht gewahrt. Das widerspricht der Anordnung des BVerfG, daß hilfesuchende schwangere Frauen selbst entscheiden können, ob sie ihre Anonymität aufgeben wollen oder nicht.

Wir empfehlen daher den Beratungsstellen, der schwangeren Frau die Eintragung des Namens selbst zu überlassen. Wird dem nicht entsprochen, müssen organisatorische Schritte eingeleitet werden, um die Arbeitsvorgänge zu trennen, damit das Ausstellen der Bescheinigung nicht mehr von der beratenden Person vorgenommen werden kann, sondern von anderen Mitarbeitern, die ebenfalls an die Schweigepflicht gebunden sind. Nur so kann gewährleistet werden, daß die Beratung von Anfang bis Ende anonym bleibt. Das entspricht auch der Anordnung des BVerfG, die vorsieht, daß die Ausstellung der Bescheinigungen von den Beratungsstellen und nicht von den beratenden Personen durchgeführt wird.

Die Trennung der Arbeitsbereiche würde die bezirklichen Beratungsstellen personell und organisatorisch stark belasten, denn die Ausstellung muß getrennt von der Beratung und dem übrigen Publikumsverkehr vorgenommen werden. Außerdem verschärft die gerade stattfindende „Regionalisierung" der sozialen Dienste, die eine Zentralisierung der verbleibenden SMD in wenigen Bezirken Berlins zur Folge hat und zu einer Erhöhung der Anzahl der Beratungen je SMD führen wird, die Engpässe. Daher erscheint die Vorgehensweise, die Eintragung des Namens durch die schwangere Frau selbst durchführen zu lassen, effizienter und praktikabler, um die Anonymität der schwangeren Frau zu gewährleisten.

66 vgl. 1.1
67 Jahresbericht 1987, Ziff. 5.1
68 Verordnung über Mitteilungen an die Finanzbehörden durch andere Behörden und öffentlich-rechtliche Rundfunkanstalten (Mitteilungsverordnung) - MV vom 7. September 1993, BGBl. I, S. 1554
69 3.3
70 NJW 93, 1751 ff.; vgl. oben 1.1

Wahrung der ärztlichen Schweigepflicht

Eine Ärztin wies darauf hin, daß in Berlin und auch in anderen Bundesländern Röntgeninstitute und Nuklearmediziner bei der Versendung von Befunden Versandtaschen verwenden, auf deren Außenhülle nicht nur die Namen der Patienten, sondern auch deren Geburtsdaten, der Tag der Untersuchung und das untersuchte Organ aufgedruckt waren. Diese Umschläge wurden zum Versand bei der Post aufgegeben.

Unsere Überprüfung bei der Ärztekammer Berlin und eine entsprechende Prüfung des Bundesbeauftragten bei der Bundesärztekammer hat ergeben, daß dies allgemein üblich war. Es bedarf kaum einer Begründung, daß dieses Verfahren mit der ärztlichen Schweigepflicht nicht zu vereinbaren ist. Die Berliner Ärztekammer hat sofort reagiert und in ihrem Mitteilungsblatt „Berliner Ärzte" dazu aufgefordert, künftig beim Versand von Befundunterlagen derartige Umschläge nicht mehr zu verwenden. Auch die Bundesärztekammer hat den von uns vertretenen Standpunkt geteilt.

Im Fernsehen wurde berichtet, daß Blutproben aus einem Krankenhaus mit dem Taxi zur Untersuchung in ein Labor befördert werden. Dabei wurden durchsichtige Plastiktüten verwendet, so daß der Taxifahrer den Namen des Patienten lesen sowie Rückschlüsse auf die durchzuführenden Untersuchungen ziehen konnte.

Bei dieser Versandform ist selbstverständlich ein verschlossenes Behältnis zu wählen, so daß der Taxifahrer nicht den Inhalt einsehen kann. Die Senatsverwaltung für Gesundheit hat unverzüglich eine entsprechende Anweisung erlassen.

Die Aufdeckung unzureichender Testmethoden auf HIV-Erreger in einer Koblenzer Pharmafirma wurde zum Anlaß genommen, die in Berlin betroffenen Krankenhäuser daraufhin zu überprüfen, ob der Datenschutz bei der Suche nach betroffenen Patienten gewahrt wurde.

Aufgrund der Laborbücher, durch die eine lückenlose Kontrolle der Blutempfänger möglich war, konnte diese Aufgabe durch die zuständigen Mitarbeiter in den meisten Krankenhäusern problemlos bewältigt werden. In einem Krankenhaus, in dem die Überprüfung wesentlich aufwendiger war, weil die Blutspendenempfänger nicht in den Laborbüchern vermerkt waren, wurde die Überprüfung ebenfalls ohne feststellbaren datenschutzrechtlichen Mangel durchgeführt. Dort mußten nahezu alle Patientenunterlagen in den einschlägigen Behandlungsbereichen durchgesehen werden, um mögliche Blutspendenempfänger ausfindig zu machen.

Ein Gesundheitsamt hat uns um Stellungnahme gebeten, ob die gemeinsame Führung einer Patientenkartei mit einer Frauenklinik im Rahmen der Schwangerschaftsberatung zulässig sei.

Durch die gemeinsame Führung der Patientendokumentation war eine klare Trennung der Aufgabenbereiche und damit der datenschutzrechtlichen Verantwortung nicht mehr möglich. Wir haben daher empfohlen, den Kooperationsvertrag dahingehend abzuändern, daß die Dokumentation beider Einrichtungen getrennt zu führen ist und eine Übermittlung von Daten nur dann stattfindet, wenn die Voraussetzungen der ärztlichen Berufsordnung dafür gegeben sind. Dies ist jeweils im Einzelfall zu prüfen.

Die Gesundheitsministerien der anderen Bundesländer haben Personen mit meldepflichtigen Erkrankungen an die obersten Gesundheitsbehörden aller anderen Bundesländer gemeldet, wenn der Aufenthaltsort dieser Personen unbekannt war. Die Meldungen enthielten Name, Geburtsdatum und Angaben zur Erkrankung und erfolgten häufig per Telefax oder auf dem Postweg, ohne daß der Vertraulichkeit der Daten Rechnung getragen wurde. Häufig handelte es sich um Asylbewerber.

Die Vorschrift des § 5 Bundesseuchengesetz war hier nicht einschlägig, da diese Meldepflicht nur für Ärzte und Krankenhäuser gilt, nicht jedoch für solche Stellen, von denen hier eine entsprechende Meldung abgegeben wurde. Diese Bestimmung enthält keine Übermittlungsgrundlage dafür, daß die obersten Landesbehörden solche Meldungen an andere Stellen weiterleiten, es sei denn an das für den jeweiligen Wohnsitz des Erkrankten zuständige Gesundheitsamt. Für vertretbar haben wir es zwar gehalten, eine Meldung an diejenige Stelle abzugeben, in deren Zuständigkeitsbereich die Krankheit erstmalig bekannt wurde. Im übrigen aber haben wir empfohlen, solche Meldungen künftig zu unterlassen und, soweit sie hier in Berlin eingehen, zurückzuweisen. Die Gesundheitsverwaltung hat uns bestätigt, daß ein Einvernehmen unter den Bundesländern hergestellt werden konnte, daß diese Praxis einzustellen ist und künftig eingehende Meldungen nicht mehr weitergeleitet werden.

Patientenrechte

Ein Berliner war vor mehreren Jahren vom sozialpsychiatrischen Dienst des Bezirksamtes beraten und betreut worden. Dies war mit Einverständnis des Betroffenen seinerzeit auch dem Sozialamt bekannt geworden. Nunmehr drohte dem Beschwerdeführer eine Räumungsklage seines Wohnungsgebers. Das im Verfahren beteiligte Sozialamt übermittelte die Klage an den sozialpsychiatrischen Dienst ohne zu prüfen, ob von dort noch eine Betreuung erfolgte. Der sozialpsychiatrische Dienst fertigte daraufhin einen Betreuungsvorgang an und versuchte Kontakt mit dem Betroffenen aufzunehmen. Dieser lehnte die Betreuung ab und verlangte die Vernichtung der Unterlagen.

Der sozialpsychiatrische Dienst wies darauf hin, daß die Eigentümlichkeit des Patientenkreises die Ablehnung der Betreuung mitbedinge und daß die Ablehnung sogar als Krankheitsmerkmal bezeichnet werden könne. In diesen Fällen wurde die Dokumentation des Vorganges als besonders wichtig bezeichnet.

Gleichwohl ist eine derartige Datenvorratshaltung abzulehnen. Es ist zwar richtig, daß die Ablehnung der Behandlung zum Krankheitsgeschehen gehören kann und die sozialpsychiatrischen Dienste für einen kurzen Zeitraum zur Anbahnung eines Betreuungsverhältnisses personenbezogene Daten vorhalten dürfen. Wenn die Betreuung jedoch abgelehnt wird, ohne daß Maßnahmen nach dem Gesetz über psychisch Kranke (PsychKG) ergriffen werden können, muß der vorhandene Datenbestand gelöscht werden. Wenn es nicht zu einer Betreuung kommt, liegen weder die Voraussetzungen des § 3 Abs. 3 PsychKG vor noch eine Behandlung oder ärztliche Beratung und Betreuung, so daß auch keine Aufzeichnungspflicht im Sinne von § 11 Berufsordnung Ärzte besteht. Wir haben daher dem sozialpsychiatrischen Dienst zur Vernichtung der Unterlagen geraten.

Einige Überraschungen hatte die Entscheidung der Senatsverwaltung für Gesundheit ausgelöst, daß Patienten aus dem Ostteil der Stadt, die ihre Behandlungsunterlagen einsehen oder zur weiteren ärztlichen Behandlung an ihre Ärzte übermitteln wollten, dafür 15 DM an die Bezirksverwaltung bezahlen sollten.

Wie in den Vorjahren berichtet, werden die Behandlungsunterlagen von Patienten, die in jetzt aufgelösten oder stillgelegten Einrichtungen der DDR behandelt wurden, zum großen Teil von den Gesundheitsämtern der regional zuständigen Bezirksverwaltungen archiviert. Dadurch entstehen zwar der Verwaltung Kosten, es ist jedoch nicht mit dem informationellen Selbstbestimmungsrecht der Patienten vereinbar, diese auf den einzelnen Patienten abzuwälzen. Die Gebührenpflicht wurde wieder aufgehoben.

Prüfung eines bezirklichen Krankenhauses

Der Personalrat des örtlichen Bereichs eines Krankenhauses in einem westlichen Bezirk hatte mehrfach auf die offensichtliche Vernachlässigung des Datenschutzes in dem Krankenhaus hingewiesen. Die Hinweise wurden übergangen. Daraufhin bat uns der Personalrat nun um eine Überprüfung der dortigen Verhältnisse.

Die unangekündigte Prüfung deckte schwerste datenschutzrechtliche Mängel auf, die gerade angesichts der in diesem Bereich besonders sensiblen Datenbestände eine erhebliche Beeinträchtigung des Rechts auf informationelle Selbstbestimmung der Betroffenen darstellten:

- PCs verfügten zwar über begrenzte technische Mittel zum Schutz der Daten, jedoch wurden selbst diese bescheidenen Mittel nicht hinreichend eingesetzt.

- Räume, in denen personenbezogene Unterlagen und PCs untergebracht waren, waren nicht mit Sicherheitsschlössern ausgestattet.
- Akten und sonstige patientenbezogene Unterlagen befanden sich nicht in ausreichend verschließbaren Schränken. Im ungesicherten Kopiererraum lagen patientenbezogene Unterlagen offen herum.
- Die Aktenvernichtung war nicht hinreichend organisiert. Zur Vernichtung vorgesehene Unterlagen wurden nicht so gelagert, daß Unbefugte davon ferngehalten werden konnten.
- Die Postverteilung erfolgte über offene Postfächer und -körbe, die in öffentlich zugänglichen Fluren untergebracht waren. Entgegen eindeutiger Regelungen wurde die Post auch ohne Postmappen verteilt.
- In der Aufnahme wurde ein aktives Terminal, welches patientenbezogene Daten auf dem Bildschirm enthielt, unbewacht aufgefunden - nach Beteuerung der Krankenhausverwaltung eine bedauerliche Einzelfallverfehlung.
- Meldungen zum Geräteregister fehlten zu allen vorgefundenen Systemen.

Die festgestellten Mängel lagen keineswegs in tiefen technischen Details oder in komplizierten Organisationsproblemen. Sie waren von der Art, die vorzufinden ist, wenn dem Datenschutz und dem sorgfältigen Umgang mit personenbezogenen Datenart nur eine untergeordnete Priorität zugemessen wird und wenn die Mitarbeiter dafür nicht sensibilisiert worden sind. Daraus ergibt sich dann leicht persönliches Fehlverhalten von Mitarbeitern.

Die Prüfung wurde dadurch erschwert, daß die Antworten zu den Prüffragen gelegentlich mit den vorgefundenen Verhältnissen nicht übereinstimmten oder zu gleichen Fragen widersprüchliche Antworten gegeben wurden. In der Stellungnahme des Krankenhauses wurde dies damit begründet, daß die eigentlich kompetenten Gesprächspartner bei der Prüfung nicht zugegen waren, ein Umstand, der bei unangekündigten Prüfungen hinzunehmen ist. Dort wird im wesentlichen auf die vorhandenen ausreichenden organisatorischen Regelungen verwiesen. Solche Regelungen sind natürlich Voraussetzung für eine zufriedenstellende Beachtung datenschutzrechtlicher Vorschriften. Sie sind aber nicht hinreichend, wenn der Durchsetzung dieser Regelungen und der Kontrolle ihrer Beachtung kein Gewicht geschenkt wird.

4.5 Inneres

4.5.1 Polizei

ASOG als Auffanggesetz für die Datenverarbeitung

Bei Ermittlungen wegen Verletzung der Unterhaltspflicht verwendet der Polizeipräsident einen Fragebogen für den Arbeitgeber des Beschuldigten, der keinen Hinweis auf die Freiwilligkeit der Angaben bei privaten Arbeitgebern enthält.

Ein derartiger Hinweis ist nach § 18 Abs. 5 des Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG) erforderlich.

Die Datenerhebung durch den Fragebogen ist eine polizeiliche Ermittlung. Dies wird schon dadurch deutlich, daß im Kopfteil des Fragebogens als Absender „Der Polizeipräsident in Berlin" benannt ist. Zumindest für einen privaten Arbeitgeber besteht somit keine Verpflichtung, diesen Fragebogen auszufüllen. Die Polizei hat sich bei einer Aussageverweigerung durch Nichtausfüllen des Fragebogens an die Staatsanwaltschaft zu wenden, die den Arbeitgeber als Zeugen daraufhin selbst vernehmen kann. Auf diese Rechtslage ist der Betroffene hinzuweisen.

Der Polizeipräsident ist dagegen der Auffassung, daß das Ausführungsgesetz zum Gerichtsverfassungsgesetz (AGGVG) heranzuziehen ist, das keine Aufklärungs- und Hinweispflichten bei Datenerhebungen enthält. In einer Neuauflage des Fragebogens soll deshalb lediglich auf die Zeugnis- und Auskunftsverweigerungsrechte der Strafprozeßordnung hingewiesen werden.

Bei der Bearbeitung dieser Eingabe hat sich einmal mehr gezeigt, daß Unsicherheiten bei der Frage bestehen, welche Befugnisnormen für die Datenverarbeitung der Polizei im Rahmen der Strafverfolgung heranzuziehen sind.

Der Berliner Gesetzgeber hat die Forderung des Bundesverfassungsgerichtes im Volkszählungsurteil, die Verarbeitung personenbezogener Daten in der öffentlichen Verwaltung normenklar zu regeln, konsequent umgesetzt und im Berliner Datenschutzgesetz festgeschrieben, daß die Verarbeitung personenbezogener Daten nur zulässig ist, wenn eine besondere Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat (vgl. § 6 Abs. 1 BlnDSG). Zweifelhaft ist, welche Rechtsvorschrift in Fällen wie diesen anzuwenden ist.

Ein Rückgriff auf die Datenverarbeitungsbefugnisse des AGGVG ist im vorliegenden Zusammenhang ausgeschlossen, da die Polizei nicht Adressat dieser Normen ist. Durch § 21 AGGVG werden Eingriffsbefugnisse in das Recht auf informationelle Selbstbestimmung auf allen Ebenen des gerichtlichen und staatsanwaltschaftlichen Geschäftsbetriebes geregelt. Soweit ausnahmsweise Polizeibeamte als Hilfsbeamte der Staatsanwaltschaft betroffen sind, wird dies ausdrücklich erwähnt (vgl. § 21 Abs. 4 Satz 1 und Abs. 5 Satz 1 Ziff. 1 AGGVG). Auch in den §§ 27 ff. AGGVG sind ausschließlich Befugnisse für die Justiz enthalten. Ausschließlich deren Mitarbeiter bzw. Behörden sind als Normadressaten aufgeführt.

Demgegenüber sind Aufgaben und Befugnisse, aber auch grundsätzliche Fragen zu Organisation und Verfahren der Polizeibehörde im Allgemeinen Sicherheits- und Ordnungsgesetz (ASOG) geregelt. Soweit die Polizei Aufgaben zu erfüllen hat, die ihr durch andere Rechtsvorschriften übertragen sind, wird im ASOG hierauf jeweils ausdrücklich Bezug genommen (z. B. §§ 1 Abs. 2, 18 Abs. 1 Satz 2 ASOG). Die Strafprozeßordnung ist eine derartige Vorschrift, so daß der Polizei die dort enthaltenen Befugnisse zustehen, soweit deren Dienstkräfte bei der Strafverfolgung tätig sind.

Die Strafprozeßordnung (StPO) enthält allerdings nur punktuell Befugnisse zur Datenverarbeitung (vgl. die §§ 163 a, 94, 102, 100 a, 100 b, 81 b 1. Alternative, 163 b StPO). Für Informationseingriffe, die nicht auf diese Normen gestützt werden können, fehlt es an der erforderlichen speziellen Eingriffsbefugnis. Diese können insbesondere nicht allein auf die §§ 160, 161, 163 StPO gestützt werden. Diese Normen regeln nicht hinreichend bestimmt, welche konkreten Eingriffe in das Recht auf informationelle Selbstbestimmung zulässig sind. Die Formulierung „Ermittlungen jeder Art" ist eher das Gegenteil einer normenklaren Eingriffsbegrenzung.

Zur Schließung dieser Gesetzeslücke muß vielmehr das ASOG herangezogen werden. In § 18 Abs. 1 Satz 2 ASOG ist eine Datenerhebungsbefugnis enthalten, die sich nicht nur auf den Bereich der Gefahrenabwehr beschränkt, sondern auch zur Erfüllung der der Polizei durch andere Rechtsvorschriften - also der Strafprozeßordnung - übertragenen Aufgaben herangezogen werden kann. Dies gilt auch für die in § 42 Abs. 1 Satz 1 ASOG vorgesehene Befugnis zur Speicherung und Nutzung personenbezogener Daten zur Aufgabenerfüllung der Polizei.

Das ASOG ist ein Polizei-Organisations-Gesetz und sieht deshalb für die Polizei einheitliche Regelungen auch bei Datenschutzsekundärpflichten - wie z. B. Aufklärungspflichten - vor. Nur damit ist der Polizei ein einheitliches Handeln möglich - unabhängig davon, ob sie präventiv oder repressiv tätig wird. Dies kommt z. B. auch beim Auskunftsrecht zum Ausdruck: § 50 Abs. 5 ASOG geht ersichtlich davon aus, daß diese Vorschrift während des Strafverfahrens anwendbar ist - also in einer Phase, in der Erhebung und Speicherung der Daten auf der Grundlage der Strafprozeßordnung erfolgen.

Verordnung über Prüffristen bei polizeilicher Datenspeicherung (Prüffristenverordnung)

Ermächtigt durch § 48 Abs. 4 ASOG hat der Senat von Berlin die Verordnung über Prüffristen bei polizeilicher Datenspeicherung (Prüffristenverordnung) erlassen, die am 22. Februar 1993 in

Kraft getreten ist. Die Verordnung regelt die Fristen, nach denen personenbezogene Daten, die in Dateien oder personenbezogen geführten Akten bei der Polizei gespeichert sind, regelmäßig daraufhin zu überprüfen sind, ob eine weitere Speicherung erforderlich ist (Prüffristen).

Unsere Anregungen sind in die nunmehr geltende Fassung der Prüffristenverordnung nur zum kleinen Teil eingegangen.

Zur Klarstellung hatten wir empfohlen, zusätzlich zu den Prüffristen auch die im ASOG festgelegten Löschungsfristen (vgl. §§ 43 Abs. 1, 24 Abs. 2 ASOG) in die Verordnung aufzunehmen. Dies hätte der Rechtssicherheit gedient und allgemein den praktischen Umgang mit den Vorschriften erleichtert, wurde von der Senatsverwaltung für Inneres jedoch aus formalen Gründen abgelehnt.

In § 1 Prüffristenverordnung sind die Fristen geregelt, nach denen eine Datenspeicherung bei Tatverdächtigen, geordnet nach bestimmten Personengruppen - Kinder zwei Jahre, Jugendliche fünf Jahre, Personen über 70 Jahre fünf Jahre und alle anderen Personen zehn Jahre - zu überprüfen ist. Unsere Anregung, die Zeitspanne der Prüffristen bei jugendlichen Tatverdächtigen und Personen über 70 Jahre auf drei Jahre und bei allen anderen Personen auf fünf Jahre zu verkürzen, wurde nicht aufgegriffen.

In Fällen von geringer Bedeutung sieht diese Bestimmung bei Kindern Prüffristen von einem Jahr, bei Jugendlichen von drei Jahren und bei allen übrigen Personen von fünf Jahren vor. Wir hatten hier empfohlen, in Anlehnung an die Prüffristenverordnung des Landes Hessen vom 28. August 1990 Fristen von zwei Jahren bei Jugendlichen und drei Jahren bei Erwachsenen festzuschreiben.

Die Prüffristen bei Daten vermißter Personen betragen gemäß § 2 Prüffristenverordnung in unaufgeklärten Fällen zehn Jahre, in aufgeklärten Fällen allgemein fünf Jahre und bei Kindern zwei Jahre. Die Erforderlichkeit einer jahrelangen Speicherung der Daten ehemals vermißter Personen bei aufgeklärten Fällen ist nicht ersichtlich.

Die Speicherung von Daten gefährdeter Personen unterliegt gemäß § 3 Abs. 2 Prüffristenverordnung einer Prüffrist von drei Jahren. Welche Personen als „gefährdet" einzustufen sind, ist der Prüffristenverordnung nicht zu entnehmen. Eine Konkretisierung wäre hier wünschenswert gewesen. In der Vergangenheit wurden die Daten gefährdeter Personen nur mit deren Einverständnis von der Polizei gespeichert. Wir gehen davon aus, daß diese Praxis auch in Zukunft beibehalten wird.

Bei der Speicherung der Daten von Verstorbenen, wie sie in § 3 Abs. 3 Prüffristenverordnung geregelt ist, wurde die Klarstellung abgelehnt, daß dies nur Personen betrifft, bei denen Tatsachen die Annahme rechtfertigen, daß die Datenspeicherung der Aufklärung von Straftaten dient oder daß die Betroffenen eines unnatürlichen Todes gestorben sind.

Olympia-Gegner im Informationssystem Verbrechensbekämpfung

Anläßlich der Bewerbung Berlins für die Austragung der Olympischen Spiele im Jahr 2000 besuchte die IOC-Prüfungskommission die Stadt im April 1993.

Zur Vorbereitung auf diesen Besuch wurde auf Veranlassung des polizeilichen Staatsschutzes, bei 217 Personen der Hinweis „Sofortanruf VB C zuständig" in das Standardabfrageprogramm des Informationssystems Verbrechensbekämpfung Berlin (ISVB) eingetragen. Dieser Hinweis erschien bei jedem Aufruf der Personalien auf dem Bildschirm. Abfrageberechtigt ist fast jeder Polizist.

Der Polizeipräsident sowie die Senatsverwaltung für Inneres sind der Auffassung, bei diesem „Merker" handele es sich lediglich um einen arbeitstechnischen Hinweis ohne Personenbezug, mit dem nur eine Zuständigkeitsregelung zur weiteren Bearbeitung des Vorganges getroffen werde. Tatsächlich handelt es sich bei dem Hinweis jedoch um ein personenbezogenes Datum im Sinne einer Einzelangabe über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 4 Abs. 1 BlnDSG). Der Hinweis wurde ausschließlich in Verbindung mit den Personalien der Betroffenen abgerufen. Er erweckte beim Abrufenden die durchaus beabsichtigte Vorstellung, daß der Betroffene ein militanter Gegner der Bewerbung von Berlin für die Olympischen Spiele im Jahr 2000 sei und daß der Polizeiliche Staatsschutz aus diesem Grund ein gesteigertes Interesse an seiner Person habe.

Eine derartige Verarbeitung von personenbezogenen Daten ist nach § 6 Abs. 1 BlnDSG nur zulässig, wenn eine besondere bereichsspezifische Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Beide Alternativen lagen nicht vor.

Nach § 42 Abs. 1 ASOG kann die Polizei rechtmäßig erhobene Daten in Akten und Dateien speichern, soweit dies zur Erfüllung ihrer Aufgaben - u. a. die Verfolgung von Straftaten - erforderlich ist. Dies lag unseres Erachtens hier nicht vor.

Mit der Vergabe des Merkers wurde nach Auskunft der Polizei vornehmlich bezweckt, daß alle Vorgänge, in denen die Betroffenen als Beschuldigte, Geschädigte oder Anzeigende in Erscheinung treten, zur Entscheidung über die Bearbeitungszuständigkeit an den Polizeilichen Staatsschutz gegeben werden. Damit sollte sichergestellt werden, daß alle Vorgänge, die im Sachzusammenhang zur Anti-Olympia-Bewegung stehen, durch den Polizeilichen Staatsschutz bearbeitet werden.

Die Vergabe von personenbezogenen Merkern ist für eine derartige Zuständigkeitszuweisung nicht erforderlich. Ein Meldedienst, der nicht personenorientiert ist, sondern auf die Begehung von Straftaten abstellt, erfüllt diesen Zweck in gleicher Weise und entspricht darüber hinaus dem Grundsatz der straftatbezogenen Datenspeicherung. Danach dürfen die Polizeibehörden nur straftaten- und nicht personenorientierte Ermittlungsverfahren führen. Die Vergabe des personenbezogenen Hinweises im ISVB bei „Olympia-Gegnern" wird diesem Grundsatz nicht gerecht. Sie kehrt ihn vielmehr um, indem sie durch die Einbeziehung von Zeugen, Anzeigenden, Opfern und anderen Nichtverdächtigen nicht eine Straftat, sondern persönliche Merkmale angetroffener Personen zum Ausgangspunkt informationeller Maßnahmen durch die Polizei macht.

Für die Betroffenen bedeutete die Vergabe des Hinweis einen erheblichen Eingriff in ihr Recht auf informationelle Selbstbestimmung. Der Hinweis war über das Standardabfrageprogramm des ISVB fast jedem Mitarbeiter der Polizei in Berlin - unabhängig von seiner eigentlichen Aufgabenzuweisung - zugänglich. Durch den Abruf der Daten erhielt der Abrufende - auch in Sachvorgängen, die in keinem Zusammenhang zum Speicherungszweck stehen (z. B. Verkehrskontrollen) - Kenntnis über die Einstellung des Betroffenen zur Olympia-Bewerbung Berlins und die Tatsache, daß der Polizeiliche Staatsschutz ein gesteigertes Interesse an dieser Person hat.

Das vorliegende Verfahren ist mit der Verwendung „personenbezogener/taktischer Hinweise" im ISVB und in INPOL zu vergleichen. Aufgrund der hohen Eingriffsintensität derartiger „personenbezogener Hinweise" hat das Abgeordnetenhaus von Berlin mit Beschluß vom 1. Dezember 1988[71] den Katalog derartiger Hinweise erheblich reduziert. Auf Weisung des Senators für Inneres dürfen seit dem 15. Februar 1989 nur noch die Hinweise „bewaffnet", „gewalttätig", „Ausbrecher", „BTM-Konsument" und „Freitod-Gefahr" im ISVB und in INPOL gespeichert werden. Die Vergabe des personenbezogenen Hinweises im Zusammenhang mit der Anti-Olympia-Bewegung widerspricht dieser Anweisung.

In ihrer Eingriffsintensität entspricht die Vergabe des personenbezogenen Hinweises auch den Merkmalen einer polizeilichen Beobachtung nach § 27 ASOG. Danach kann die Polizei die Personalien einer Person zur polizeilichen Beobachtung speichern, damit andere Polizeidienststellen das Antreffen der Person melden können, wenn das bei Gelegenheit einer Überprüfung aus anderem Anlaß festgestellt wird. Vergleichbares war hier vorgesehen. Jeder polizeiliche Kontakt eines Betroffenen sollte dem Polizeilichen Staatsschutz gemeldet werden. Die strengen Zulässigkeitsvoraussetzungen, die an die Ausschreibung zur polizeilichen Beobachtung geknüpft sind, wurden bei der Vergabe der personenbezogenen Merker jedoch nicht beachtet.

71 Drs. 10/2304

Unbeschadet der Problematik der Rechtsgrundlage wurde stichprobenweise überprüft, ob die Vergabe der Hinweise den eigenen Kriterien entsprach. Zum Zeitpunkt der Prüfung fanden sich in keinem der untersuchten Fälle schriftliche Belege über die Gründe, die zur Vergabe des Hinweises bei dem jeweiligen Betroffenen geführt haben. Dies ist unter dem Gesichtspunkt der Nachvollziehbarkeit von verwaltungsinternen Entscheidungen unzureichend. Diese Unzulänglichkeit wurde nach Auskunft des Polizeipräsidenten in Berlin zwischenzeitlich dadurch behoben, daß die Unterlagen über die Eingabe des Merkers - versehen mit dem jeweiligen Entscheidungskriterium für seine Vergabe - beim Polizeilichen Staatsschutz gesondert erfaßt wurden.

In drei Fällen wurde bereits unsere Prüfung zum Anlaß genommen, den personenbezogenen Hinweis bei den Betroffenen zu löschen, da nicht mehr nachvollziehbar war, warum er überhaupt vergeben worden war.

Seit der Entscheidung des IOC über den Austragungsort der Olympischen Spiele im Jahr 2000 am 23. September 1993 wird das beschriebene Verfahren noch bei insgesamt 137 Personen, die sich militant gegen „Umstrukturierungsmaßnahmen im weitesten Sinne" richten, weiter betrieben. Allerdings werden Unterlagen, in denen die Betroffenen als Anzeigende, Geschädigte oder Zeugen erfaßt sind, nicht mehr an den Polizeilichen Staatsschutz weitergeleitet. Das neue Verfahren wird noch geprüft.

Erfolgskontrolle beim Einsatz von besonderen polizeilichen Ermittlungsmethoden

Ausgelöst durch eine Kleine Anfrage im Abgeordnetenhaus hat der Senat zum Einsatz und Erfolg der besonderen Ermittlungsmethoden, die nach dem neuen ASOG zulässig sind, Stellung genommen.

Danach wurden technische Mittel zum Abhören oder Aufzeichnen des nicht öffentlich gesprochenen Wortes seit dem Inkrafttreten des ASOG am 26. April 1992 in keinem einzigen Fall eingesetzt. Von insgesamt 40 Fällen einer längerfristigen Observation führten nach Aussage der Senatsverwaltung für Inneres zwei Observationen zu Festnahmen von Tatverdächtigen. Verdeckte Ermittler wurden in zwei Fällen und V-Personen in sechs Fällen eingesetzt. Erfolge für die Straftatenbekämpfung hat die Senatsverwaltung für Inneres nicht mitgeteilt[72].

In der gegenwärtig intensiv geführten Diskussion über die Einführung weiterer polizeilicher Befugnisse zur Aufrechterhaltung der inneren Sicherheit verweisen die Befürworter auf die Notwendigkeit von zusätzlichen, weitreichenden staatlichen Befugnissen, während deren Gegner auf die nicht hinnehmbaren Gefährdungen für existentielle Grundrechte hinweisen.

Im Rahmen dieser Auseinandersetzung wäre es aus Sicht der Datenschutzbeauftragten ein Gewinn, wenn sich die Diskussion auf Erkenntnisse stützen würde, die stärker als bisher gesichert sind. Die Zusammenstellung und Veröffentlichung der bereits vorhandenen polizeilichen Befugnisse und der durch sie erzielten Ermittlungsergebnisse sind ein wichtiger Beitrag zur Erfolgskontrolle dieser Befugnisse.

Private Sicherheitsdienste

In zunehmendem Maße ist der Einsatz von privaten Sicherheits- oder Wachdienste nicht nur im Privatbereich, sondern auch zur Wahrnehmung von Sicherheitsaufgaben im Bereich der öffentlichen Verwaltung zu beobachten. Dabei werden von den Unternehmen oft auch polizeiähnliche Tätigkeiten ausgeübt - wie z. B. verdeckte Beobachtungen - und in erheblichem Umfang Daten von betroffenen Bürgern verarbeitet.

Während die Polizeibehörden im Umgang mit den Daten der Bürger besondere gesetzliche Beschränkungen zu beachten haben, existieren derartige Regelungen für die Datenverarbeitung bei privaten Sicherheitsunternehmen nicht. Die Bestimmungen des Bundesdatenschutzgesetzes für die Datenverarbeitung nichtöffentlicher Stellen sind angesichts der besonderen Problemlage, die mit der Sammlung und Nutzung von personenbezogenen Daten durch private Sicherheitsdienste verbunden ist, nicht ausreichend.

Im Zusammenhang mit Vorschlägen für eine Bundesratsinitiative zur strengeren Überwachung von privaten Wachdiensten haben wir auf diesen unbefriedigenden Zustand hingewiesen und die Schaffung von besonderen gesetzlichen Regelungen für die Datenverarbeitung bei privaten Sicherheits- und Wachdiensten sowie Detekteien gefordert.

Übernahme von Abschlußberichten der Strafvollzugsanstalten der ehemaligen DDR in Kriminalakten

Nach Haftentlassung sind in der ehemaligen DDR von den Strafvollzugsanstalten Abschlußberichte über die Strafhaft der Gefangenen erstellt und von der Volkspolizei zu den Kriminalakten genommen worden.

Befanden sich diese Berichte zum Zeitpunkt der Übernahme der Kriminalakten durch den Polizeipräsidenten noch in den Unterlagen, so wurden sie in vielen Fällen weiter in der Akte des Betroffenen belassen. Diese Berichte enthielten zum Teil besonders sensible Daten, die die schutzwürdigen Belange der Betroffenen stark berühren.

Auf unsere Anregung hat der Polizeipräsident angewiesen, die noch vorhandenen Abschlußberichte den Kriminalakten zu entnehmen, gesondert zu archivieren und nur noch zu Rehabilitationszwecken zu nutzen. Vom ordnungsgemäßen Abschluß dieser Maßnahme konnten wir uns im Rahmen einer Prüfung durch die Einsichtnahme in stichprobenartig ausgewählte Kriminalakten überzeugen.

Polizeiliche Registrierung von Prostituierten hat zugenommen

In unserem Jahresbericht 1990[73] hatten wir erstmals über die beim Polizeipräsidenten geführte Kartei „Zuhälterei, Menschenhandel und ähnliche Delikte" berichtet, die überwiegend Daten von Prostituierten enthält. Nachdem die Senatsverwaltung für Inneres zunächst darauf beharrte, daß eine Speicherung der Daten von Prostituierten aufgrund der „Eigenheit des Kriminalitätsfeldes" erfolgen dürfe[74], konnte über die Beurteilung der Rechtslage Einigkeit erzielt werden: Frauen dürfen nicht bei der Polizei registriert werden, nur weil sie der Prostitution nachgehen. Es müssen in jedem Einzelfall konkrete Tatsachen vorliegen, die die Annahme rechtfertigen, daß die Speicherung der Daten zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich ist[75].

Die Prostitution ist weder mit Strafe bedroht noch verboten. Strafbestimmungen knüpfen an außerhalb der Prostitution liegende Merkmale an. Es müssen konkrete Anhaltspunkte für eine „Verstrickung" mit einer Straftat von erheblicher Bedeutung, wie Zuhälterei oder Menschenhandel, bestehen.

Nachdem im Juni 1992 die Kartei noch 4 201 Karteikarten enthalten hatte, stellten wir bei einer erneuten Prüfung fest, daß die Zahl der registrierten Personen nicht abgenommen, sondern um 1 190 Personen zugenommen hatte.

Unsere stichprobenartige Überprüfung hat ergeben, daß eine Bereinigung nach den genannten Kriterien nicht erfolgt sein kann. So ist es offenbar weiterhin gängige Praxis, daß allein die Feststellung als Prostituierte auf dem Straßenstrich oder in bordellartigen Betrieben zu einer Registrierung der Betroffenen in der Kartei führt.

Nach wie vor waren von Prostituierten, die sich keiner Straftat verdächtig gemacht haben, Fotos in der Kartei enthalten. Auch Strafanzeigen, die Prostituierte bei der Polizei erstatten, führten zu ihrer Registrierung.

72 Antwort des Senats auf die Kleine Anfrage Nr. 4297, LPD v. 28. Oktober 1993

73 Ziff. 3.5

74 Jahresbericht 1990, 3.5; Stellungnahme des Senats zum Jahresbericht 1990, Drs. 12/375, S. 5

75 Jahresbericht 1992, 4.2.2; Stellungnahme des Senats zum Jahresbericht 1992, Drs. 12/3081 (neu)

Trotz einer dringenden Empfehlung, die Kartei in einen Zustand zu bringen, der den rechtlichen Vorgaben entspricht, sowie einer entsprechenden Aufforderung des Unterausschusses Datenschutz hat eine grundlegende Bereinigung nicht stattgefunden.

INPOL-Neukonzeption

Im Januar 1992 beschloß der Arbeitskreis „Innere Sicherheit" der Arbeitsgemeinschaft der Innenministerien der Bundesländer, das polizeiliche Informationssystem INPOL weiterzuentwickeln. Zu diesem Zweck wurde eine Projektgruppe damit beauftragt, die wichtigsten Aussagen zu Funktion und Ausgestaltung eines zukünftigen Systems „INPOL-neu" zu erarbeiten. Im November 1992 wurde das Projekt abgeschlossen und als Ergebnis ein „Grobes Fachkonzept" zur INPOL-Neukonzeption vorgelegt.

Als neues Konzept für die Datenorganisation in INPOL ist die Einführung eines *anwendungsunabhängigen Datenpools* vorgesehen. Diese Abkehr von der bisherigen Form der getrennten Dateien eröffnet die Möglichkeit, alle personenbezogenen Daten unterschiedslos ohne Differenzierung ihrer Rolle in einem polizeilichen Vorgang zu speichern. Die Eigenschaften der Daten (z. B. ob sie einem Beschuldigten, Opfer, Zeugen oder Hinweisgeber zuzuordnen sind) ergeben sich nur aufgrund eines komplexen Beziehungsgeflechtes (hinterlegte Logik) in der Datenbank.

Mit dieser technischen Vereinfachung sind aber auch Risiken für schutzwürdige Belange von Betroffenen verbunden. Die in einem anwendungsunabhängigen Datenpool gespeicherten personenbezogenen Daten werden gemeinsam verwaltet. Sie stehen somit grundsätzlich allen Anwendern zur freien Verfügung. Damit nicht jeder, der Zugang zum Datenbestand hat, alle Informationen - unabhängig von seiner polizeilichen Aufgabenzuweisung - zur Kenntnis nehmen kann, ist ein differenziertes Zugriffsverfahren vorgesehen. Für eine eingehende datenschutzrechtliche Bewertung, ob die vorgesehenen Zugriffsdifferenzierungen ausreichen, liegen jedoch noch keine hinreichend konkreten Lösungsvorgaben vor.

INPOL-neu eröffnet vielfältige *neuartige Recherchemöglichkeiten.* Auf die damit verbundenen Fragen zur Zweckbindung der Datenspeicherung und zur Verantwortlichkeit für den Datenbestand enthält das „Grobe Fachkonzept" keine nachvollziehbaren Aussagen.

Die Datenerfassung in INPOL soll zukünftig auf einer *automationsgestützten Vorgangsbearbeitung* basieren. Bei der Übernahme von INPOL-Daten aus den Vorgangsbearbeitungssystemen der Teilnehmer (z. B. dem ISVB) bleibt die Frage offen, wie landesrechtliche Regelungen, die zum Teil besondere Restriktionen und Zweckbindungsregelungen enthalten, eingehalten werden können.

Weiter ist in der INPOL-Neukonzeption vorgesehen, die Möglichkeit zur Freitextrecherche und des direkten Zugriffs auf Fremdsysteme zu erweitern.

Diese nur beispielhaft genannten Elemente zeigen auf, daß mit INPOL-neu eine erhebliche Qualitätsveränderung in der polizeilichen Datenverarbeitung verbunden sein wird. Dies macht einen adäquaten datenschutzrechtlichen Standard erforderlich, der insbesondere Vorgaben

- zur Verhältnismäßigkeit,
- für Auswertungs-/Recherchefunktionen,
- für die Verantwortlichkeit von Datenspeicherungen,
- für Zweckbindungsregelungen,
- für eine hinreichende Protokollierung

enthält.

Speicherungsdauer ausländerrechtlicher Verstöße in INPOL

Wir wurden darauf aufmerksam gemacht, daß die Daten von Ausländern, die wegen ausländerrechtlicher Verstöße zur Fahndung ausgeschrieben worden waren, entgegen den bundeseinheitlichen KpS-Richtlinien länger als zulässig gespeichert werden.

Tatsächlich wurden die Daten im Zusammenhang mit ausländerrechtlichen Verstößen auf Veranlassung der Ausländerbehörde beim Landeseinwohneramt Berlin im Rahmen der Amtshilfe in den Fahndungsdatenbestand von INPOL eingespeichert, wenn die Aufenthaltsgenehmigung abgelaufen war und die Aufforderung zur freiwilligen Ausreise vom Ausländer nicht befolgt wird. Die Fahndungsdatensätze blieben allerdings auch nach erfolgter Festnahme und Ausreise bzw. Abschiebung weiterhin gespeichert. Alle Fahndungsdatensätze wurden nach Ablauf von zehn Jahren nach Beginn der Fahndungsauschreibung daraufhin geprüft, ob die Gründe für die Ausschreibung weiterhin bestehen. In diesem Fall wurden die Daten generell für weitere zehn Jahre im Fahndungsdatenbestand gespeichert. Gegebenenfalls war eine weitere Fristverlängerung nach erneuter Überprüfung möglich.

Diese Verfahrensweise steht im Widerspruch zu § 48 ASOG sowie den bundeseinheitlichen KpS-Richtlinien. In Dateien gespeicherte personenbezogene Daten sind gemäß § 48 Abs. 2 Nr. 2 ASOG zu löschen, wenn festgestellt wird, daß ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgabe nicht mehr erforderlich ist. Zur polizeilichen Aufgabenerfüllung nicht mehr erforderlich sind die Daten von den Ausländern, die bereits festgenommen und abgeschoben wurden. Eine polizeirechtliche Grundlage für eine Aufrechterhaltung der Fahndungsausschreibung und eine weitere Speicherung der Daten im Fahndungsdatenbestand ist in diesen Fällen nicht gegeben.

Der Polizeipräsident in Berlin hat sich dieser Auffassung angeschlossen und zugesagt, das bisher praktizierte Verfahren, wonach auch nach einem Fahndungserfolg und anschließender Abschiebung die Daten weiter gespeichert wurden, umgehend aufzugeben.

Unzureichende Protokollierung von Datenabfragen

Eine Bürgerin beschwerte sich darüber, daß sie mehrfach von einer ihr unbekannten männlichen Person angerufen und dabei belästigt worden sei. Den Äußerungen des Anrufers entnahm sie, daß sich dieser ihre Personalien und Wohnanschrift unter Verwendung ihrer Kfz-Nummer durch eine unberechtigte Abfrage aus dem Datenbestand des Kraftverkehrsamtes verschafft hat.

Im Zuge von staatsanwaltschaftlichen Ermittlungen konnte geklärt werden, daß tatsächlich eine Abfrage aus dem KVA-Datenbestand zum Kfz-Kennzeichen der Petentin erfolgt ist. Der Datenabruf konnte einem bestimmten ISVB-Terminal bei der Polizei zugeordnet werden.

Die daraufhin vorgenommene Protokollbandauswertung des ISVB ergab, daß die Datenabfrage unter Verwendung des ISVB-Benutzerausweises eines bestimmten Polizeibeamten durchgeführt wurde. Dieser war zum Zeitpunkt der Abfrage am betreffenden ISVB-Terminal als sog. „Fernmeldebeamter" eingesetzt. In dieser Funktion hat der Beamte mit den Dienstkräften außerhalb der Dienststelle Funkkontakt zu halten und für Anfragen von außen zur Verfügung zu stehen. Er hat auch Abfragen für andere Beamte vorzunehmen und diesen das Ergebnis mitzuteilen. Dabei ist es ihm nicht möglich, die Rechtmäßigkeit der an ihn herangetragenen Anfragen zu überprüfen. Eine Protokollierung der fernmündlichen Anfragen erfolgt weder durch den Fernmeldebeamten selbst noch im Rahmen der Benutzung des ISVB-Terminals.

In seiner zeugenschaftlichen Vernehmung konnte sich der Beamte an eine konkrete Anfrage externer Dienstkräfte zum Kfz-Kennzeichen der Petentin nicht mehr erinnern. Auf weiterführende Protokollierungsunterlagen konnte - da diese nicht angefertigt werden - nicht zurückgegriffen werden. Anhaltspunkte für eine bewußt rechtswidrige Datenabfrage durch den Beamten selbst konnte die Staatsanwaltschaft nicht feststellen. Das staatsanwaltschaftliche Ermittlungsverfahren wurde daraufhin gemäß § 170 Abs. 2 Strafprozeßordnung eingestellt.

Dieses Ergebnis ist nicht nur aus datenschutzrechtlicher Sicht unbefriedigend. Durch die von uns bereits mehrfach geforderte Protokollierung von Datenabfragen über ISVB-Terminals unter

Einbeziehung des Abfrageveranlassers und -grundes wären die notwendigen Voraussetzungen gegeben, um mißbräuchlichen Datenabrufen wirksamer entgegentreten zu können. Letztlich trägt eine derartige erweiterte Protokollierung - insbesondere bei sensiblen Datenverarbeitungssystemen wie dem ISVB - zur Sicherung der Funktionsfähigkeit der polizeilichen Datenverarbeitung bei.

Ausführungsvorschriften zu § 49 ASOG (Dateienrichtlinien)

In § 49 Abs. 1 ASOG ist bestimmt, daß für jede von der Polizei betriebene automatisierte Datei über personenbezogene Daten und für nicht automatisierte Dateien, aus denen personenbezogene Daten an andere Stellen übermittelt werden, eine Errichtungsanordnung zu erlassen ist. Diese tritt an die Stelle der in § 19 Abs. 2 BlnDSG geforderten Dateibeschreibung.

Das Nähere hat die Senatsverwaltung für Inneres in den am 4. Dezember 1992 erlassenen und am 1. Januar 1993 in Kraft getretenen Ausführungsvorschriften zu § 49 ASOG (Dateienrichtlinien) geregelt.

Unsere Vorschläge wurden dabei im wesentlichen umgesetzt. Nicht berücksichtigt wurde unsere Anregung, die Anzahl der betroffenen Personen in Schätzwerten anzugeben sowie die Löschungsvorschriften nach §§ 43 Abs. 1, 24 Abs. 2 ASOG und die Unterrichtungsfrist gemäß § 43 Abs. 3 ASOG aufzunehmen.

Dies ist bedauerlich, da unsere Vorschläge auf die Schaffung einer bürgernahen, verständlichen und damit der Rechtsklarheit dienenden Anwendung der Ausführungsvorschriften zu § 49 ASOG gerichtet waren. Dies gilt insbesondere für den Hinweis auf die Löschungfristen, die neben den Prüfungsfristen auch zu beachten sind. Durch die Nichtangabe der Anzahl der betroffenen Personen wurde im übrigen eine Sonderregelung für die Polizei vorgesehen, die von der Meldepraxis aller anderen Berliner Verwaltungen abweicht. Das nunmehr von der Polizei praktizierte Verfahren macht unnötige Nachfragen erforderlich, um zu einer angemessenen Beurteilung der gemeldeten Dateien zu gelangen.

4.5.2 Verfassungsschutz

Sicherheitsüberprüfungsgesetz

Rund 600 000 Betroffene, die irgendwann einer Sicherheitsüberprüfung unterzogen wurden, sind in der Verbunddatei der Verfassungsschutzämter erfaßt[76]. Personen, die Zugang zu geheimzuhaltenden Informationen (VS) erhalten sollen, werden mit ihrer Einwilligung einer derartigen Überprüfung unterzogen. Bisher ist die Materie in Verwaltungsvorschriften geregelt[77]. Sicherheitsüberprüfungen sind ein erheblicher Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen und bedürfen einer bereichsspezifischen gesetzlichen Grundlage[78]. Auf Bundesebene befindet sich ein Entwurf eines *Sicherheitsüberprüfungsgesetzes (SÜG)* in der parlamentarischen Beratung[79]. Der Anwendungsbereich dieses Gesetzentwurfes erstreckt sich auf sicherheitsempfindliche Tätigkeiten, die vom Bund zugewiesen bzw. übertragen werden oder zu denen der Bund ermächtigt. Da dieses Gesetz auch für das Land prägende Wirkung haben wird, haben wir sowohl zu diesem Gesetzentwurf als auch zu dem abgeänderten Gesetzentwurf in der vom Bundestag am 2. Dezember 1993 angenommenen Fassung[80] Stellung genommen. Wir haben insbesondere folgende Bedenken geäußert:

Die Stelle, die den Betroffenen mit der sicherheitsempfindlichen Tätigkeit betraut, muß in jeder Phase der Überprüfung - insbesondere bei der Ausdehnung der Überprüfungsmaßnahmen - die Sachleitungsbefugnis haben. Für alle Datenabfragen über Ehe- und Lebenspartner muß deren Zustimmung vorliegen. Angaben über den Ehe- und Lebenspartner sind bei ihm selbst auf einem gesonderten Erhebungsbogen zu erfragen. Der Umfang der in Dateien gespeicherten Daten der überprüften Personen ist zu reduzieren. Besonders bedenklich ist die vorgesehene Nutzung der Daten für fast alle Aufgaben des Verfassungsschutzes. Damit würde der Verfassungsschutz durch seine mitwirkende Tätigkeit bei der Sicherheitsüberprüfung in den Besitz von Daten gelangen, die er nach den Verfassungsschutzgesetzen nicht hätte erheben dürfen. Die im Rahmen der Sicherheitsüberprüfung erlangten Erkenntnisse sollten allenfalls für die Bereiche Spionage- und Terrorismusabwehr genutzt werden[81].

Ein weiterer wesentlicher Mangel des Gesetzentwurfes ist auch hier wieder die Beschränkung des Akteneinsichtsrechtes des Betroffenen. Die Akteneinsicht ist eine wesentliche Voraussetzung für die Gewährleistung des Rechtes auf informationelle Selbstbestimmung und sollte unter der gleichen Voraussetzung erfolgen wie die Auskunft und nicht auf das Vorliegen rechtlicher Interesssen beschränkt werden. Der grundsätzliche Ausschluß der Sicherheitsüberprüfungsakten bei dem mitwirkenden Bundesamt für Verfassungsschutz oder MAD von der Akteneinsicht ist mit dem Recht auf informationelle Selbstbestimmung nicht zu vereinbaren. Überwiegende Geheimhaltungsinteressen oder überwiegende Interessen Dritter, die einer Akteneinsicht entgegenstehen, können - wie bei jeder Entscheidung über eine Akteneinsicht - berücksichtigt werden. Für einen pauschalen Ausschluß der Verfassungsschutzakten vom Einsichtsrecht besteht keine Notwendigkeit.

Auch zu einem Entwurf über *SÜG-Ausführungsvorschriften,* die bis zum Abschluß der parlamentarischen Beratungen des SÜG-Entwurfes vorliegen sollten, haben wir Stellung genommen:

Bedenklich ist insbesondere der weit gefaßte Personenkreis für Sicherheitsüberprüfungen. Wir haben angeregt, eine funktionale Trennung der Organisationseinheit, die für die Sicherheitsüberprüfung zuständig ist, vorzunehmen. Die aufgeführten Sicherheitsrisiken bei Ehe- und Lebenspartnern halten wir für zu weitgehend. Eine Anhörung des Betroffenen über alle gesammelten Informationen sollte soweit wie möglich sichergestellt werden. Der Betroffene und sein Ehe- bzw. Lebenspartner sind umfassend über den Umfang der Datenerhebungen und der beabsichtigten Maßnahmen aufzuklären. Die vorgesehene Befugnis, Daten nicht beim Betroffenen, sondern bei Dritten zu erheben, ist zu weitgehend. Die genannten Beispiele - Aggression oder Depression bei Konfrontation mit dem möglichen Sicherheitsrisiko - sind bedenklich. Einer möglichen Aggression durch Befragung Dritter aus dem Weg zu gehen, scheint uns eher im Interesse der erhebenden Stelle als im schutzwürdigen Interesse des Betroffenen zu liegen. Von der Datenerhebung beim Betroffenen darf nur im zwingenden Ausnahmefall abgesehen werden. Ob der Betroffene so erheblich in seinen Gesundheitszustand eingreifende Depressionen bei Offenbarung der Informationen bekommen wird, kann aber vom Verfassungsschutz oder MAD nicht entschieden werden.

Die Bundesländer sind für den Verfassungsschutz in ihrem Bereich zuständig. Bei der Senatsverwaltung für Inneres wird seit März 1993 ein Entwurf eines Berliner Landesgesetzes erarbeitet, der uns bisher nicht zur Stellungnahme übersandt wurde. Wir gehen jedoch davon aus, daß unsere zum Sicherheitsüberprüfungsgesetzentwurf des Bundes geäußerten Bedenken und Vorschläge berücksichtigt werden.

Zu dem in Berlin gebrauchten *Sicherheitsfragebogen,* der zum Teil sogar weitergehendere Datenerhebungen als der Gesetzentwurf des Bundes enthält, haben wir inhaltliche Bedenken gegenüber der Senatsverwaltung für Inneres geäußert. Unter anderem auch deswegen hat der Hauptpersonalrat seine Zustimmung zu dem Fragebogen gem. § 55 Abs. 2 Ziff. 5 Personalvertretungsgesetz verweigert. Daraufhin hat die Senatsverwaltung für Inneres mit Rundschreiben vom 26. November 1993 die Geheimschutzbeauftragten in der Berliner Verwaltung gebeten, die Vordrucke mit sofortiger Wirkung nicht mehr auszugeben bzw. zu verwenden.

76 DER SPIEGEL 42/93, S. 58 ff.
77 Richtlinien für die Sicherheitsüberprüfung von Personen im Rahmen des Geheimschutzes - Sicherheitsrichtlinien - GMBl. 1991, S. 70 ff.
78 Beschluß der Datenschutzkonferenz vom 26./27. September 1991, Jahresbericht 1991, Anlage 2.4
79 BT-Drs. 12/4891
80 BT-Drs. 12/6307
81 vgl. auch die Stellungnahme des Bundesrates, Drs. 97/93

Nachdem eine Reihe von Verbesserungen inhaltlicher und verfahrensmäßiger Art vereinbart worden waren, können inzwischen für eine Übergangszeit trotz fehlender Rechtsgrundlage die Überprüfungen wieder durchgeführt werden.

Personenlisten über Demonstrationsteilnehmer

Bei Prüfungen haben wir festgestellt, daß die Polizei Personenlisten an das Landesamt für Verfassungsschutz gesandt hat, auf denen anläßlich von Demonstrationen und Veranstaltungen festgestellte oder festgenommene Personen aufgeführt waren. Diese Listen wurden kurz nach den Veranstaltungen bei der Polizei vernichtet. Beim Verfassungsschutz hingegen wurden die Listen über Jahre gespeichert.

Nach früheren Mangelfeststellungen hatte das Landesamt für Verfassungsschutz zugesagt, die von uns aufgefundenen Personenlisten zu vernichten. Bei neu entdeckten Listen über andere Demonstrationen weigert sich das Landesamt für Verfassungsschutz nun jedoch, diese zu vernichten.

Das Landesamt steht auf dem Standpunkt, daß eine Teilnahme und insbesondere vorläufige Festnahme bei gewalttätig verlaufenden Demonstrationen, die von bestimmten Gruppierungen geplant, organisiert und durchgeführt werden, den Verdacht der Unterstützung verfassungsfeindlicher Bestrebungen und damit eine Speicherung rechtfertigt.

Von Maßnahmen des Verfassungsschutzes - und dazu gehören auch die Überprüfung, der Abgleich und die Speicherung derartiger Personenlisten - darf nur derjenige erfaßt werden, dessen Verhalten konkrete Anhaltspunkte für relevante verfassungsfeindliche Bestrebungen i. S. v. § 2 Abs. 1 Nr. 1 Landesverfassungsschutzgesetz (LfVG) gezeigt hat. Allein die Teilnahme an einer Veranstaltung oder Demonstration, die von extremistisch eingestuften Gruppen organisiert oder durchgeführt werden, reicht für die Annahme, daß die festgestellten Personen selbst verfassungsfeindliche Bestrebungen vorhatten oder durchführten, nicht aus. Es ist nicht ausgeschlossen, daß auch Personen auf den Listen stehen, die keine Verbindung zu diesen Gruppierungen haben.

Die Teilnahme an Demonstrationen, die von einer Gruppierung durchgeführt werden, die Beobachtungsobjekt des Landesamtes für Verfassungsschutz ist, mag für eine gewisse Sympathie der festgestellten Demonstrationsteilnehmer für diese Gruppierung sprechen, rechtfertigt aber noch nicht den konkreten Verdacht, alle festgestellten Personen ließen sich bei ihren Tätigkeiten von Bestrebungen i. S. d. § 6 Abs. 2 LfVG leiten.

Auch die vorläufige Festnahme ist kein hinreichender Ansatzpunkt. Zum einen waren zum Teil die Umstände der Festnahmen zweifelhaft. So war der Presseberichterstattung zu einer Demonstration zu entnehmen, daß die Festnahmen „unter den meist passiven, mehrheitlich friedfertigen Versammlungsteilnehmern" erfolgten. Zum anderen handelt es sich um eine Liste, auf der überwiegend Festnahmen nach dem ASOG enthalten waren, die zudem ohne Angabe zu dem Verhalten des einzelnen oder dem Ausgang des Ermittlungsverfahrens übermittelt wurden.

Darüber hinaus ist bei Demonstrationsteilnehmern nach der Rechtsprechung des Bundesverfassungsgerichts eine besondere Zurückhaltung bei Informationseingriffen erforderlich: „Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung ... behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."[82]

Da diese Personenlisten für die Aufgabenerfüllung des Landesamtes für Verfassungsschutz nicht erforderlich sind, bestand nicht nur keine Verpflichtung der Polizei, sondern auch keine Befugnis zur Übermittlung dieser Daten. Dies gilt auch für die Rechtslage nach Inkrafttreten des neuen LfVG. Die Verpflichtung des Landesamtes für Verfassungsschutz, nach § 27 Abs. 6 LfVG übermittelte Informationen nach ihrem Eingang unverzüglich daraufhin zu überprüfen, ob sie zur Erfüllung seiner Aufgaben erforderlich sind, stellt nur eine zusätzliche Absicherung dar. Wenn - wie bei den Demonstrationsteilnehmerlisten - die mangelnde Erforderlichkeit für die Polizei erkennbar ist, hat die Übermittlung zu unterbleiben. Daraus folgt, daß auch eine Speicherung der Personenlisten beim Landesamt für Verfassungsschutz unzulässig ist.

Kontrollfreier Raum

Nach der Vereinigung erhielten die Landesämter für Verfassungsschutz Abschriften von Kontrollaufträgen des MfS. Diese Unterlagen betrafen Telefonkontrollen, die das MfS vorgenommen hatte. Das Berliner Landesamt für Verfassungsschutz erhielt etwa 5 000 Kontrollaufträge zur Prüfung, inwieweit es ausgespäht wurde. Berlin war das einzige Land, das dem Beschluß der Innenministerkonferenz auf Vernichtung der Kontrollaufträge nicht nachgekommen war und konnte deshalb die Unterlagen Ende 1991 dem Generalbundesanwalt für ein Ermittlungsverfahren gegen einen leitenden Mitarbeiter des MfS übergeben.

Die Senatsverwaltung für Inneres hat vor der Weiterleitung der Kontrollaufträge die G-10-Kommission unterrichtet und diesen parlamentarischen Gremien zur Prüfung stichprobenartig Einsicht in die Unterlagen gewährt. Bei Maßnahmen, die vor der Wiedervereinigung in Berlin vorgenommen wurden und über die personenbezogene Daten in den Unterlagen des Verfassungsschutzes vorhanden sind. Dies betrifft nicht nur die Unterlagen des MfS (für die mit dem Stasi-Unterlagengesetz inzwischen ohnehin eine Ablieferungspflicht besteht), sondern auch Unterlagen, die von den West-Alliierten an das Landesamt für Verfassungsschutz gelangt sind.

Das Ausführungsgesetz zu Art. 10 GG enthält hierüber keine Regelungen. Es sieht nach seinem Wortlaut für derartige Datensammlungen keine Zuständigkeit der für die Kontrolle von Eingriffen des Landesamtes für Verfassungsschutz in das Post- und Fernmeldegeheimnis eingerichteten G-10-Kommission vor.

Wir halten es für unerläßlich, daß für diese Unterlagen eine Instanz vorgesehen wird, die den Umgang mit diesen zum Teil erheblich in das Persönlichkeitsrecht eingreifenden Datenspeicherungen kontrolliert. Eine Lösungsmöglichkeit wäre es, die Kontrollaufgaben der G-10-Kommission insoweit zu erweitern. Dabei könnte eine weitere Lücke geschlossen werden. Ausdrücklich sollte geregelt werden, in welchem Umfang die G-10-Kommission nicht nur bei der Anordnung der Maßnahmen bzw. der Löschung der Daten einerseits und der Benachrichtigung der Betroffenen andererseits, sondern auch bei der Verwendung der Daten - insbesondere der Weitergabe der Daten an andere Behörden - mitwirken soll. Da gerade hierin ein schwerwiegender, zur heimlichen Überwachung hinzukommender Eingriff in die informationelle Selbstbestimmung liegt, würden entsprechende Kontrollrechte einen erheblichen Gewinn für die Legitimität derartiger Maßnahmen bringen.

Der Senator für Inneres hat unsere Anregungen aus verschiedenen Gründen nicht aufgegriffen. Eine Fraktion hat unsere Vorschläge zur Besprechung im Ausschuß für Verfassungsschutz des Abgeordnetenhauses angemeldet.

Organisation der Datenverarbeitung

Die *NADIS-Richtlinien,* die die Grundsätze für den Betrieb des bundesweiten Datenverbunds der Verfassungsschutzämter regeln, sind unter Berücksichtigung des novellierten Bundesverfassungsschutzgesetzes überarbeitet worden und sollen demnächst nach Billigung der Innenminister/-senatoren in Kraft treten.

Wir haben u. a. gegen die Regelungen über die Verantwortlichkeit für die in NADIS eingegebenen Daten Bedenken geäußert. Es muß sichergestellt sein, daß die speichernde Verfassungsschutzbehörde nach den für sie geltenden gesetzlichen Bestim-

82 BVerfGE 65, 43

mungen nicht nur über Umfang, Inhalt und Dauer der Datenspeicherungen, sondern auch über die Übermittlung der eingegebenen Daten an andere Stellen entscheiden kann. Dies ist nach dem Entwurf der Richtlinie nicht der Fall.

Gemäß § 12 Abs. 2 Bundesverfassungsschutzgesetz sind personenbezogene Daten in Dateien nicht zu löschen, sondern stattdessen zu *sperren,* wenn Grund zu der Annahme besteht, daß die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden. Im Bundesamt für Verfassungsschutz ist dazu ein Sperrverfahren eingerichtet worden, das - anders als die vorangegangene Planung[83] - den datenschutzrechtlichen Bedenken besser Rechnung trägt. Das Verfahren wird allerdings vom Landesamt für Verfassungsschutz noch nicht genutzt, da amtsinterne Regelungen über die Nutzung und den Umgang mit gesperrten Daten noch ausstehen. Wir haben einige Verfahrensvorschläge hierzu vorgelegt.

Das Landesamt für Verfassungsschutz hat unmittelbar nach Aufhebung des Löschungs- und Vernichtungsverbotes für die vorhandenen Datensammlungen im April 1992 mit den Maßnahmen zur Durchführung des Bereinigungsprozesses begonnen[84]. Die *Löschung der gesperrten Daten* im Nachrichtendienstlichen Informationssystem (NADIS) ist erfolgt. Die Anzahl der Personendatensätze hat sich um 71 % reduziert. Es wurden zehntausende von Akten und Unterlagen gesperrt. Entgegen dem Beschluß des Ausschusses für Verfassungsschutz des Abgeordnetenhauses konnten allerdings wegen fehlender Räumlichkeiten in vielen Bereichen die *Altakten* nicht räumlich getrennt von den Aktenbeständen der laufenden Bearbeitung untergebracht werden. Nachdem inzwischen das Landesarchivgesetz verabschiedet wurde, können die Akten dem Landesarchiv zur Übernahme angeboten und die nicht archivwürdigen Unterlagen vernichtet werden. Dadurch dürfte sich das Raumproblem etwas entschärfen. Dennoch muß sichergestellt sein, daß in der Zwischenzeit eine räumliche Trennung erfolgt und Maßnahmen zur Lösung des Raumproblems ergriffen werden.

4.5.3 Einwohnerwesen

Nach der Auflösung des *Zentralen Einwohnerregisters der ehemaligen DDR (ZER)* zum 30. Oktober 1992[85] blieb noch offen, unter welchen Voraussetzungen der vorsorglich erstellte verkürzte Meldebestand, der insbesondere auch die Personenkennzahl (PKZ) enthält, weiter verwertet werden darf. Die Datenschutzbeauftragten hatten dies nur aufgrund einer ausdrücklichen Rechtsgrundlage für möglich gehalten.

Abweichend von bisherigen Planungen war im Januar 1993 zwischen den Innenministerien der neuen Länder einschließlich Berlins und dem Bundesminister des Innern ein Verwaltungsabkommen im Gespräch, in dem vereinbart werden sollte, daß die 20 Millionen Bürger betreffenden reduzierten Bestände an den *Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes* übermittelt werden sollen. Dies sollte bereits im Vorgriff auf eine künftige gesetzliche Rechtsgrundlage erfolgen, da der Bundesbeauftragte *vorgetragen hatte,* daß er die Daten zur Personenidentifizierung benötige und es nicht im Interesse Berlins und der neuen Länder liege, die Nutzung bis zu einer Gesetzesänderung zu verzögern.

Im März 1993 waren die Innenminister der fünf neuen Länder und Berlins bereit, auch ohne ein Verwaltungsabkommen die Daten an den Bundesminister des Innern als den für den Bundesbeauftragten zuständigen Bundesminister weiterzugeben. Die Datenschutzbeauftragten der fünf neuen Länder und Berlins stellten gegenüber den Innenministern klar, daß eine Übergabe der ZER-Daten und damit die Aufhebung des nach dem Einigungsvertrag bestehenden Verwertungsverbotes ohne gesetzliche Grundlage unzulässig ist. Wir haben uns an die Senatsverwaltung für Inneres gewandt und diese gebeten, dem Verfahren so nicht zuzustimmen. Dies wurde abgelehnt.

Die für den 16. Juni 1993 vom Brandenburgischen Innenministerium geplante Übergabe des reduzierten Meldedatenbestandes aus dem ZER an das Bundesministerium des Innern in Absprache mit den anderen neuen Bundesländern wurde erst nach einem Antrag auf Erlaß einer einstweiligen Anordnung beim Verwaltungsgericht Potsdam und einer Sondersitzung des Brandenburger Landtages wieder aufgegeben. Obwohl der Landtag Brandenburg - entgegen einer Empfehlung des Innenausschusses - einer Übergabe der Daten an das Bundesministerium des Innern dann doch zugestimmt hat, wollte das Innenministerium Brandenburg die Daten nun doch nicht mehr ohne gesetzliche Grundlage herausgeben. Auch die Senatsverwaltung für Inneres hat ihre Zustimmung für die Übermittlung des Berliner Datensatzes zurückgezogen.

Nunmehr kam es endlich zu der längst geforderten Gesetzesinitiative. Am 2. Dezember 1993 hat der Bundestag einen Gesetzentwurf zur Änderung des Stasi-Unterlagen-Gesetzes[86] angenommen. Danach erhält der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes den reduzierten Meldedatenbestand mit den Personenkennziffern und darf diese Daten an die Zentrale Polizeiliche Ermittlungsstelle für die Strafverfolgung von Mitgliedern ehemaliger SED-geführter DDR-Regierungen und Verfolgung von Straftaten im Zusammenhang mit dem Wiedervereinigungsgeschehen (ZERV) im Einzelfall auf Ersuchen zur Erfüllung ihrer Aufgaben übermitteln. Die Anregungen der Datenschutzbeauftragten der fünf neuen Länder und Berlins zur Verbesserung der datenschutzrechtlichen Regelungen wurden im Gesetzgebungsverfahren nicht berücksichtigt. Diese hatten insbesondere gefordert, im Entwurf stärker auf die Erforderlichkeit und die Zweckbestimmung abzuheben, beim Bundesbeauftragten eine abgeschottete Stelle für die übermittelten Daten zu schaffen und eine Schutzvorschrift für die Daten Jugendlicher zu verankern. Auch im Bundesrat wurden die Vorschläge der Datenschutzbeauftragten nicht aufgegriffen. Vielmehr hat der Bundesrat mit Erfolg den Vermittlungsausschuß angerufen mit dem Ziel, auch eine Datenübermittlung an Gerichte und Strafverfolgungsbehörden vorzusehen[87] eine Ausweitung der Nutzungsmöglichkeiten, die das im Einigungsvertrag vorgesehene Verbot der weiteren Nutzung der PKZ auf Dauer in Frage stellt.

4.5.4 Statistik

Rechtsgrundlagen

Nach dem 1992 verabschiedeten *Landesstatistikgesetz* war bis zum 31. Dezember 1993 durch *Rechtsverordnung* zu regeln, welche Daten, die beim Vollzug eines Landesgesetzes erhoben worden sind, dem Statistischen Landesamt aus Registern oder Dateien des Verwaltungsvollzuges zur Verfügung gestellt werden. Eine Überprüfung ergab, daß dies lediglich für Daten erforderlich ist, die nach dem Meldegesetz dem Statistischen Landesamt übermittelt werden. In der dazu erlassenen Rechtsverordnung[88] wurden unsere Hinweise berücksichtigt.

Es zeigte sich jedoch, daß eine Reihe von Statistiken aus Dateien des Verwaltungsvollzuges erstellt werden, für deren Übermittlung an das Statistische Landesamt keine Anordnung durch Rechtsvorschrift erforderlich ist. In diesen Fällen haben wir die Grundlagen der Auftragsdatenverarbeitung nach § 3 BlnDSG überprüft. Hier ist die Verarbeitung durch das Statistische Landesamt nur aufgrund einer schriftlichen Anordnung der auftraggebenden Stelle und nach deren Weisungen zulässig. Auch die Zulässigkeit der Verarbeitung von Einzelangaben im Statistischen Informationssystem und damit der Verknüpfung mit anderen Einzelangaben hängt von der Weisung des Auftraggebers ab. Er bleibt datenschutzrechtlich für den Umgang mit den ihm zustehenden Daten im Statistischen Landesamt verantwortlich.

Auch zehn Jahre nach dem Volkszählungsurteil von 1983 ist dieses noch nicht in allen *Bundestatistikgesetzen* umgesetzt worden. Insbesondere kritisieren die Datenschutzbeauftragten von Bund und Ländern, daß zu erwarten steht, daß auch in dieser

83 Jahresbericht 1992 Ziff. 4.2.3 S. 73
84 vgl. Jahresbericht 1992, Ziff. 4.2.3
85 vgl. Jahresbericht 1992, 3.2

86 Drs. 12/5775 in der Fassung einer Beschlußempfehlung des Innenausschusses (Drs. 12/6100)
87 Sitzung des Bundesrates am 17. Dezember 1993
88 GVBl. 1993, S. 661

Legislaturperiode des Bundes das *Gesetz über die Bevölkerungsstatistik* noch nicht novelliert wird. Wir wandten uns an die Senatsinnenverwaltung und baten, über den Bundesrat auf eine Beschleunigung des Verfahrens zu drängen. Kritikwürdig ist bei der gegenwärtigen Verfahrensweise insbesondere die nicht klare Trennung von Statistik und Verwaltungsvollzug bei der primärstatistischen Datenerhebung, z. B. in Standesämtern, sowie die fehlende Definition der Hilfsmerkmale und die Nichtbeachtung des Trennungsgebotes von Hilfs- und Erhebungsmerkmalen.

Kampagnen

Auf der Grundlage des *Handelsstatistikgesetzes,* das ebenfalls dringend novellierungsbedürftig ist, fand eine Totalerhebung bei den Unternehmen des Handels- und Gastgewerbes statt. Dazu übermittelten die Finanzbehörden dem Statistischen Landesamt Daten der Handels- und Gastgewerbetreibenden. Es zeigte sich jedoch, daß diese Daten nicht selten veraltet oder sogar fehlerhaft waren. Ungeachtet vielfältiger Versuche des Statistischen Landesamtes, diese Daten zu bereinigen, wurde einer Vielzahl von Bürgern mitgeteilt, sie seien auskunftspflichtig, obwohl sie es nach dem Handelsstatistikgesetz nicht waren. Dies führte dazu, daß unnötigerweise zahlreiche unrichtige Erinnerungs- und Mahnschreiben vom Statistischen Landesamt versandt wurden.

In den letzten Monaten des Jahres 1993 riefen uns nicht wenige Bürger an, die zur Teilnahme an der 1-%-Gebäude- und Wohnungsstichprobe verpflichtet worden waren und sich über die Erhebung ihrer Einkommensdaten empörten.

Im Rahmen des Gesetzgebungsverfahrens zum *Wohnungsstatistikgesetz* vom 18. März 1993, das der Erhebung zugrunde lag, hatten wir insbesondere die Erforderlichkeit bezweifelt, das monatliche Netto-Einkommen nach Einkommensklassen in einer Staffelung von mindestens 200,– DM zu erheben. Diese ungeachtet unserer Hinweise in das Gesetz aufgenommene Regelung wurde von den betroffenen Bürgern als überzogener Eingriff in ihr informationelles Selbstbestimmungsrecht empfunden. Unserer Auffassung nach wäre auch hier eine gröbere Staffelung angemessener gewesen.

Die langfristigen Bemühungen des Statistischen Landesamtes, das statistische Informationsangebot zu verbessern, beinhalten auch, externen Nutzern einen On-line-Anschluß an den *Makrodatenbankrechner* zu ermöglichen. In einem Pilotverfahren ist ein solcher Anschluß durch die Industrie- und Handelskammer vorgesehen. Wir überprüften die technischen und organisatorischen Voraussetzungen. Durch vielfältige Sicherungsmaßnahmen - insbesondere durch den Einsatz eines isolierten, von der statistischen Aufbereitung abgekoppelten Rechners und einer zusätzlichen Prüfung der Daten auf die statistische Geheimhaltung - sind die datenschutzrechtlichen Voraussetzungen für ein derartiges kundenfreundliches System erfüllt.

4.5.5 Personalwesen

Noch immer kein datenschutzgerechtes Landesbeamtengesetz

Auch ein Jahr nach dem Inkrafttreten des 9. Dienstrechtsänderungsgesetz des Bundes[89] ist dem Abgeordnetenhaus noch kein Entwurf zur notwendigen Anpassung des Landesbeamtengesetzes vorgelegt worden. Zwar hat uns die Senatsverwaltung den Entwurf für ein 23. Landesbeamtenrechtsänderungsgesetz zugeleitet, der jedoch datenschutzrechtlich verbesserungsbedürftig ist. Wir haben dementsprechend eine ganze Reihe von detaillierten Vorschlägen zur datenschutzgerechten Formulierung des Gesetzentwurfes gemacht, die jedoch von der Senatsverwaltung für Inneres überwiegend nicht berücksichtigt worden sind.

Die Regeln des Beamtenrechtsrahmengesetzes bedürfen der Umsetzung durch den Landesgesetzgeber, weil es sich insofern nicht um unmittelbar in Berlin geltendes Bundesrecht, sondern um Rahmenrecht handelt. Bei der Umsetzung des Rahmenrechts hat der Landesgesetzgeber einen gewissen Spielraum, was auch die Senatsverwaltung nicht bestreitet. Diesen Spielraum sollte der Landesgesetzgeber nutzen, um die datenschutzrechtliche Position der Beamten des Landes Berlin weiter zu verbessern, wobei die Angestellten im öffentlichen Dienst den Beamten gleichzustellen wären.

Demgegenüber ist die Senatsinnenverwaltung der Meinung, aus Gründen der Rechtsvereinheitlichung sollte der Landesgesetzgeber die Vorgaben des Beamtenrechtsrahmengesetzes nahezu unverändert übernehmen. Damit verkennt sie die Eigenart der Rahmengesetzgebungskompetenz des Bundes, die überschritten würde, wenn die Länder zur Übernahme von Detailregelungen gezwungen würden.

Im einzelnen haben wir u.a. vorgeschlagen

- die organisatorische und personelle Trennung der Beihilfestellen von der Personalverwaltung wegen der Sensibilität der Beihilfeunterlagen zwingend vorzuschreiben;
- dem Beamten auch ein Recht auf Einsicht in seine Sicherheitsakte zu geben;
- die Beschwerden, Behauptungen und Bewertungen, die für den Beamten ungünstig sind, aber nicht zu disziplinarrechtlichen Maßnahmen geführt haben, nicht länger in der Personalakte des Betroffenen aufzubewahren, als entsprechende Disziplinarvorgänge aufbewahrt werden dürften.

Wir werden uns im Gesetzgebungsverfahren weiter für eine entsprechende Verbesserung des Entwurfs einsetzen.

Personalakte

Schon jetzt entstehen in der Praxis immer wieder Probleme im Zusammenhang mit der Führung von *Nebenakten.* Nach dem novellierten Beamtenrechtsrahmengesetz dürfen Nebenakten nur geführt werden, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist oder mehrere personalverwaltende Stellen für den Beschäftigten zuständig sind. Ihr Inhalt darf nur Unterlagen umfassen, die sich auch in der Grund- bzw. Teilakte befinden. Keinesfalls darf sie darüber hinausgehendes Aktenmaterial enthalten.

Die Rechtmäßigkeit der Datensammlung hat sich an dem Gebot der Erforderlichkeit zu orientieren. Daher darf die Nebenakte nur solche Unterlagen enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerledigung der betreffenden Stelle benötigt werden. Im übrigen ist gemäß § 56 Abs. 2 Satz 3 BRRG in die Grundakte ein vollständiges Verzeichnis aller Teil- und Nebenakten aufzunehmen.

Dies bedeutet, daß z.B. *dienstliche Beurteilungen* und *Bewertungen über die DDR-Vergangenheit* nicht Bestandteile der Nebenakte sein dürfen, da diese einerseits hochsensible Daten enthalten, andererseits eine Notwendigkeit der Speicherung bei der Beschäftigungsstelle nicht ersichtlich ist. Bei einer Abwägung der beiderseitigen Interessen müssen dabei Gesichtspunkte der möglichen Arbeitserleichterung für den Arbeitgeber zurückstehen.

Beim Inhalt von Nebenakten ist ferner zu beachten, daß er nach seiner Zweckbestimmung gegebenenfalls nur befristet erforderlich ist und vernichtet werden muß, sobald seine Notwendigkeit entfallen ist.

Verwaltungsinterner Schriftwechsel zu Arbeitsstreitverfahren ist nicht Bestandteil der Personalakte und kann daher auch nicht in die Nebenakte aufgenommen werden. Er ist in einer Sachakte zu führen und nach rechtskräftiger Entscheidung an das zuständige Rechtsreferat zurückzusenden. Enthält das Kündigungsschreiben Hinweise auf die DDR-Vergangenheit (Kündigung nach dem Einigungsvertrag), so ist dieses Schreiben in einem verschlossenen Umschlag aufzubewahren und seine Existenz in einem kurzen Vermerk in der Akte festzuhalten.

Gleiches gilt auch im übrigen bei anderen gerichtlichen Entscheidungen, da diese zumeist ebenfalls hochsensibles Datenmaterial enthalten.

Offenbarung von Personaldaten

Die Senatsinnenverwaltung hatte angefragt, ob nach unserer Auffassung dem unterlegenen Bewerber um eine Beamtenstelle im Absageschreiben automatisch der Name des erfolgreichen Bewerbers mitgeteilt werden dürfe.

89 BGBl. 1992 I. S. 1030 ff.

Da nicht jeder unterlegene Bewerber versuchen wird, seine Einstellung mit einer Konkurrentenklage zu erzwingen, ist die Bekanntgabe des Namens des erfolgreichen Bewerbers nicht in jedem Fall erforderlich. Eine *Namensnennung des erfolgreichen Bewerbers* sollte nur auf ausdrücklichen Wunsch des jeweils Unterlegenen und so rechtzeitig erfolgen, daß der unterlegene Bewerber etwaige Rechtsbehelfsfristen noch einhalten kann; auf diese Möglichkeit könnte im Ablehnungsschreiben hingewiesen werden.

Über die Auskunftserteilung ist der ausgewählte Bewerber sodann gemäß § 56 d Abs. 2 Satz 2 BRRG schriftlich zu informieren. Gründe für die ablehnende Auswahlentscheidung dürfen dem unterlegenen Bewerber nur insoweit mitgeteilt werden, als sie sich auf ihn (nicht auf den erfolgreichen Konkurrenten) beziehen.

Im Fall der *Aktenübersendung bei Konkurrentenklagen* an das Gericht ist die beklagte Dienstbehörde für die Rechtmäßigkeit der Datenübermittlung verantwortlich. Vor allem die unaufgeforderte Übermittlung vollständiger Personalakten (einschließlich Beihilfe-, Kindergeld-, Pfändungs- und Disziplinarakten, auch soweit diese nicht im Streit sind) an das Verwaltungsgericht ist in der Regel nicht erforderlich. Insofern hat die Behörde Aktenteile, die keinen Bezug zum Streitgegenstand haben, vor der Übermittlung selbst auszusondern. Durch die bundesgesetzlich vorgeschriebene Differenzierung der Personalaktenführung soll eine Aussonderung nicht erforderlicher Aktenteile durch die Verwaltung erleichtert werden. Allerdings kann das Verwaltungsgericht die Vorlage der vollständigen Personalakte des erfolgreichen Bewerbers verlangen. Die beklagte Dienstbehörde ist dann nach § 99 Verwaltungsgerichtsordnung verpflichtet, diesem Verlangen zu entsprechen, wenn und soweit die Personalakte nicht nach einem Gesetz oder ihrem Wesen nach geheimgehalten werden muß.

Zunehmend beschweren sich Beschäftigte des öffentlichen Dienstes über die Praxis der personalaktenführenden Stellen im Rahmen der *Vergleichsmitteilung* an den Arbeitgeber des Ehegatten bei der Festsetzung des Ortszuschlags.

Gemäß §§ 29 Abs. 5 Bundesangestelltentarifvertrag, 40 Abs. 5 Bundesbesoldungsgesetz (BBesG) werden dem öffentlichen Dienst Tätigkeiten in bestimmten Bereichen gleichgestellt, so daß zwischen den genannten Arbeitgebern Vergleichsmitteilungen auszutauschen sind. Offenbar prüfen jedoch die personalaktenführenden Stellen nicht immer hinreichend die Voraussetzungen für die Gleichstellung nach den Gesetzeskriterien, sondern versenden großzügig Vergleichsmitteilungen auch an andere Arbeitgeber.

Da eine Befugnis zum Austausch von Vergleichsmitteilungen mit sonstigen Arbeitgebern nicht besteht, kommt der Feststellung durch die Dienstbehörde - ob die gesetzlichen Voraussetzungen erfüllt sind, besondere Bedeutung zu.

Für die Prüfung der Voraussetzungen ist der Beamte, der den Ehegattenanteil bzw. Kinderanteil im Ortszuschlag begehrt, grundsätzlich nachweispflichtig. Falls der Nachweis auf Schwierigkeiten stößt, sind von Amts wegen weitere Ermittlungen zu führen.

Bevor nicht in dem gesetzlich vorgesehenen Verfahren abschließend geklärt ist, ob der Ehegatte des Betroffenen im öffentlichen Dienst oder bei einem gleichgestellten Arbeitgeber tätig ist, dürfen keine Vergleichsmitteilungen an den Arbeitgeber des Ehegatten versandt werden.

In der Verwaltungsstelle eines Bezirksamts wurden an allgemein zugänglicher Stelle die krankheitsbedingten Fehlzeiten eines Beschäftigten an einer Wandtafel ausgehängt. In einem Krankenhausbetrieb wurde ebenfalls geplant, Krankheitszeiten von Beschäftigten offen an einer Art Stecktafel auszuweisen.

Darin liegt ein besonders krasser Eingriff in das informationelle Selbstbestimmungsrecht der Beschäftigten.

Bei den Verwaltungen wurde verdeutlicht, daß Informationen über krankheitsbedingte Fehlzeiten höchst sensible Daten darstellen, die lediglich der personalaktenführenden Stelle oder der jeweiligen Einsatzstelle bekannt sein dürfen und von dieser vertraulich zu behandeln sind.

Überprüfung von Beschäftigten

Mit Beschluß vom 1. Dezember 1992 hat der Senat einer Vorlage der Senatsinnenverwaltung zugestimmt, die eine generelle Überprüfung von Bediensteten, die aus dem Westen Berlins bzw. den alten Bundesländern stammen, ohne deren Einverständnis vorsieht. Mit dieser Überprüfung soll festgestellt werden, wer früher mit dem Ministerium für Staatssicherheit zusammengearbeitet hat.

Während eine solche Überprüfung von Mitarbeitern und Bewerbern, die innerhalb der letzten zwei Jahre vor dem 3. Oktober 1990 ihren Wohnsitz oder gewöhnlichen Aufenthaltsort im Beitrittsgebiet hatten, ohne deren Einwilligung auf den Einigungsvertrag (Anlage I, Kapitel XIX, Sachgebiet A, Abschnitt III) gestützt werden kann, mangelt es bei Dienstkräften aus dem Westteil der Stadt dagegen an einer Rechtsgrundlage.

Dabei wird nicht verkannt, daß es politisch wünschenswert ist, aus Gründen der Gleichbehandlung die Überprüfung nicht auf Beschäftigte aus den östlichen Bezirken zu beschränken.

Das Stasi-Unterlagen-Gesetz (StUG) enthält jedoch lediglich Vorschriften darüber, für welche Zwecke Informationen aus den Stasi-Unterlagen verwendet und an wen sie weitergegeben werden dürfen. Fragen dienstrechtlicher Art, in welchen Fällen öffentlich Bedienstete durch eine Anfrage beim Bundesbeauftragten für die Stasi-Unterlagen überprüft werden dürfen, sind dagegen dort nicht geregelt. § 21 Abs. 1 Nr. 6 StUG sieht Überprüfungen der folgenden Personen nur nach Maßgabe „der dafür geltenden Vorschriften" vor und setzt daher Datenerhebungsbefugnisse voraus, die die Vorschrift selbst nicht enthält. Dies hat der Senat in seiner Stellungnahme zum Jahresbericht 1992[90] nicht berücksichtigt. Eine Bezugnahme auf die allgemeinen Grundsätze des Beamtenrechts ist ebenfalls nicht geeignet, eine normenklare Rechtsgrundlage für eine Datenerhebung bei anderen Stellen zu ersetzen. § 119 Abs. 2 Landesbeamtengesetz (LBG) gibt der Senatsverwaltung für Inneres die Befugnis, für den Bereich des Berliner Beamtenrechts Verwaltungsvorschriften zu erlassen. Die nach dem Bundesdatenschutzgesetz für eine Datenerhebung bei Dritten erforderliche Rechtsvorschrift ist auch hierin nicht zu sehen. Schließlich sind auch die in § 13 Abs. 2 Nr. 2 BDSG alternativ genannten Voraussetzungen nicht erfüllt. Das öffentliche Dienstrecht enthält keine gesetzliche Aufgabenzuweisung, Personen, die dem öffentlichen Dienst im Westteil der Stadt schon vor dem 3. Oktober 1990 angehörten, auf eine etwaige Zusammenarbeit mit dem Staatssicherheitsdienst zu überprüfen. Auch ist kein unverhältnismäßiger Aufwand damit verbunden, die Betroffenen selbst zu befragen oder an sie zu appellieren, sich freiwillig überprüfen zu lassen.

Da die Senatsvorlage der Senatsverwaltung für Inneres, die Grundlage für den späteren Senatsbeschluß vom 1. Dezember 1992 wurde, ein Überprüfungsverfahren gegenüber Westbediensteten vorsieht, das in deren Grundrechte eingreift und mangels Rechtsgrundlage gegen datenschutzrechtliche Vorschriften verstößt, wurde eine Beanstandung ausgesprochen. Die Senatsverwaltung für Inneres hat diese Beanstandung zurückgewiesen und erklärt, sie werde den Senatsbeschluß vollziehen. Unser Vorschlag zur Behebung der Schwierigkeiten, eine eigene Rechtsgrundlage zu schaffen, blieb unbeantwortet.

Die Senatsverwaltung für Inneres hat einen Leitfaden erstellt, wonach ab sofort jedem Antrag auf Einstellung oder Höhergruppierung für Bewerber/Dienstkräfte aus dem Beitrittsgebiet eine besonders gegliederte Begründung beizufügen ist.

Die Dienstbehörde muß vor Einstellung eines Angestellten bzw. Beamten gemäß den beamtenrechtlichen und tarifrechtlichen Bestimmungen ein Bild über die Verfassungstreue der Bewerber machen. Es ist daher aus datenschutzrechtlicher Sicht nicht zu beanstanden, wenn weitergehende, differenzierende Fragen zu Mitgliedschaft oder Funktionen in der SED, in gesellschaftlichen Organisationen oder sonstigen herausgehobenen Funktionen in diesem System in einem persönlichen Gespräch mit den Bewerbern erörtert werden. Bei Beförderungen/Höher-

90 Drs. 12/3081 (neu) S. 23

gruppierungen/Höherbewertungen von Dienstposten/Bewährungsaufstiegen ist dagegen eine solche Aktion, zumal sie bei solchen Anlässen stets zu wiederholen ist, unverhältnismäßig.

Der Schutz des Persönlichkeitsrechts des Arbeitnehmers läßt nur solche Fragen zu, an denen der Arbeitgeber zur Beurteilung der Eignung und Befähigung des Arbeitnehmers ein objektiv berechtigtes Interesse hat. Dem entspricht es, wenn in die Privatsphäre des Arbeitnehmers nicht tiefer eingedrungen werden darf, als es der Zweck des Arbeitsverhältnisses gemäß § 34 Abs. 2 BlnDSG in Verbindung mit § 28 BDSG erfordert. Maßgebend für die im Rahmen der Zweckbestimmung des Arbeitsverhältnisses vorzunehmende Interessenabwägung ist daher der Grundsatz der Verhältnismäßigkeit.

Ein Anhörungsverfahren in dem beschriebenen Umfang bei jeder Form der Höhergruppierung bzw. Beförderung ist jedoch nicht mehr erforderlich. Selbst wenn sich die Eignung nur auf ein konkretes Amt oder eine bestimmte Laufbahn bezieht, kann sie nicht bei jeder Bewerbung neu und insgesamt in Frage gestellt werden. Dies widerspräche dem Gleichheitsgrundsatz, da eine solche Verfahrensweise in diskriminierender Art für Bewerber aus dem Beitrittsgebiet zusätzlich Hürden bei Bewerbungen um Beförderungsstellen aufbaut.

Anhörungsverfahren sollten daher erst dann durchgeführt werden, wenn konkrete Hinweise vorliegen, die an der Geeignetheit des Bewerbers für die konkret angestrebte Position berechtigte Zweifel entstehen lassen.

Automation im Personalwesen

In der Berliner Verwaltung werden derzeit ADV-Verfahren geplant, mit denen verschiedene Aufgaben des Personalwesens integriert verarbeitet werden sollen.

Mit dem *Integrierten Personal-Verwaltungssystem (IPV)* ist die Einführung eines Systems vorgesehen, das einheitlich in den Personalstellen des Landes dezentral eingesetzt werden soll. Grundlage des IPV sollte zunächst ein Verfahren sein, das auf anderer technischer Plattform für das Personalwesen in den Berliner Krankenhäusern eingesetzt wird. Im Rahmen der Hauptuntersuchung stellte sich jedoch die mangelnde Eignung des zugrunde gelegten Verfahrens für die Zwecke der Verwaltung heraus. Dies führte zu einer Verzögerung des Projektes IPV.

Ein anderes Projekt der integrierten Personaldatenverarbeitung ist jedoch in eine entscheidende Phase getreten: Mit dem *Lehrer-Informations- und Verwaltungssystem (LIV)* wird im Bereich der Berliner Verwaltung erstmalig ein System zur Verarbeitung von Personaldaten geplant, welches administrierende Aufgaben der Personal- und Stellenverwaltung durch die Einbindung der Schulaufsicht mit Aufgaben der Personalsteuerung, -aufsicht und -kontrolle verbindet[91].

Das *Landesamt für Informationstechnik (LIT)* bietet seine Dienstleistungen als Großrechenzentrum und IuK-Beratungsinstanz der mittelbaren und unmittelbaren Verwaltung an. Die Kosten dafür werden mit der mittelbaren Verwaltung direkt abgerechnet, bei der unmittelbaren Verwaltung, die dafür nicht bezahlen muß, gehen jedoch Kostengesichtspunkte in die Abschätzung von Projektkosten ein, die u.a. zur Bewertung der Wirtschaftlichkeit von IuK-Projekten herangezogen werden müssen. Das LIT führt daher eine *Kostenrechnung* durch, die auch seinen Personaleinsatz für andere Verwaltungen einbezieht.

Der Wunsch des LIT, dafür wie andere IuK-Dienstleister in der Privatwirtschaft, die konkreten Gehaltsdaten der eigenen Mitarbeiter heranziehen zu können, stieß jedoch auf datenschutzrechtliche Hindernisse. Es verfügt nämlich nicht selbst über seine Daten. Aufgrund des Allgemeinen Zuständigkeitsgesetzes in Berlin ist die Zahlbarmachung der Löhne und Gehälter für Mitarbeiter der Hauptverwaltung und der ihr untergeordneten Landesbehörden dem Landesverwaltungsamt (LVwA) zugeordnet, welches damit datenverarbeitende Stelle für die Zahlungsverfahren Lohn, Vergütung und Besoldung ist.

Die Verwendung von Personaldaten von Mitarbeitern des LIT aus dem Besoldungs- bzw. Vergütungsverfahren durch das LIT setzt eine Übermittlung dieser Daten aus dem Landesverwaltungsamt voraus. Da es sich dabei um Daten handelt, die bestehende dienst- oder arbeitsrechtliche Rechtsverhältnisse betreffen, ist für die Beurteilung der Zulässigkeit dieser Übermittlung wegen des Verweises in § 34 Abs. 2 BlnDSG § 28 BDSG hinzuzuziehen. Hier war nur zu prüfen, ob die Voraussetzung von § 28 Abs. 1 Nr. 1 oder Nr. 2 BDSG gegeben sind. Beides ist zu verneinen, denn es entspricht nicht der Zweckbestimmung der dienst- oder arbeitsrechtlichen Vereinbarungen, daß die Daten für eine Kostenrechnung, die für Behörden wie das LIT rechtlich nicht vorgesehen ist, an das LIT übermittelt werden. Wohl kann das LIT berechtigte Interessen geltend machen, eine solche Kostenrechnung durchzuführen. Jedoch stützt der Widerspruch des Personalrates ebenso wie die ständige Rechtsprechung der Arbeitsgerichte die Annahme, daß das schutzwürdige Interesse an dem Ausschluß der Verarbeitung oder Nutzung überwiegt.

Eine gesetzliche Regelung, die der besonderen Aufgabenstellung des LIT als verwaltungsinternem Dienstleister Rechnung trägt und eine Zuordnung der Leistungen und Kosten auf die öffentlichen Stellen, die die Dienstleistungen in Anspruch nehmen, durch eine Kostenrechnung vorschreibt, wäre im Rahmen eines IuK- oder LIT-Gesetzes anzustreben. Sie liegt jedoch noch nicht vor.

Es mußte daher bei folgender Lösung bleiben:

Das LVwA liefert dem LIT aggregierte Daten über die Durchschnittspersonalkosten ausreichend großer, gemeinsam abzurechnender Gruppen aus dem LIT. Diese Durchschnittskosten werden dann der Kostenrechnung für den Einsatz von Mitarbeitern aus diesen Gruppen zugrundegelegt. Da es sich bei diesen aggregierten Daten um nicht mehr personenbezogene Daten handelt, entfällt die Notwendigkeit einer datenschutzrechtlichen Rechtsgrundlage.

Wenn im Einzelfall eine personenbezogene Kostenrechnung erforderlich ist, ist vorab sicherzustellen, daß eine schriftliche Einwilligung des Betroffenen vorliegt, die den Voraussetzungen des § 6 Abs. 2 bis 4 BlnDSG genügt.

4.6 Jugend und Familie

Gesetzgebung

Zum 1. April 1993 ist eine *Änderung* des 8. Buchs des Sozialgesetzbuchs (SGB VIII) in Kraft getreten[92]. Darin werden die Beziehungen zwischen Jugendamt, Jugendgerichtshilfe und Jugendgericht nur festgelegt. Ungeregelt ist weiterhin ob hierzu ein Informationsfluß ohne Zustimmung des Betroffenen zulässig ist. Es bleibt daher bei der grundsätzlichen Mitwirkungsbedürftigkeit des Jugendlichen nach § 60 ff. SGB I, da besondere Übermittlungsbefugnisse im SGB VIII für den Bereich der Jugendgerichtshilfe nicht enthalten sind. Dies führt dazu, daß die Jugendgerichtshilfe in besonderem Maß auf die Kooperation eines straffälligen Jugendlichen setzen muß. Verweigert dieser die Kooperation mit der Jugendgerichtshilfe, kann diese auch nur beschränkt zum Wohle des Jugendlichen in das gerichtliche Verfahren eingreifen. Ziel der Betreuungsarbeit der Gerichtshilfe muß es daher sein, dem Jugendlichen deutlich zu machen, daß es um eine zu seinen Gunsten wirkende Leistung des Staates geht.

Unterhaltspflicht: Anfrage beim Arbeitgeber?

Ein unterhaltspflichtiger Vater verweigerte trotz Mahnung die Auskunft über die Veränderung seiner Vermögensverhältnisse. Das Jugendamt hatte die Unterhaltsbeistandsschaft für die geschiedene Ehefrau und ihre Kinder übernommen. Nach wiederholter Mahnung nahm es eine Anfrage beim Arbeitgeber des Unterhaltsverpflichteten vor, der vorher allerdings auf diesen Schritt hingewiesen worden war. Der Unterhaltsverpflichtete verbot seinem Arbeitgeber jegliche Auskunft, so daß der zuständige Stadtvormund durch seine Anfrage keine neuen Erkenntnisse erzielen konnte.

91 vgl. unten 4.8

92 BGBl. I, S. 239

Der Unterhaltsverpflichtete ist nach § 1605 BGB zur Auskunft verpflichtet, die dieser jedoch verweigerte. Bei der Beurteilung der Frage, ob die Datenerhebung beim Arbeitgeber nach § 68 Abs. 1 SGB VIII zulässig ist, kommt es auf die Verhältnismäßigkeit der Anfrage an. Der Verhältnismäßigkeitsgrundsatz erfordert zumindest die Geeignetheit einer Maßnahme. Nach § 68 SGB VIII darf eine Datenerhebung beim Arbeitgeber nur dann vorgenommen werden, wenn dies zur Durchführung der Unterhaltsbeistandsschaft erforderlich ist. Dies ist nur der Fall, wenn damit der Rechtsanspruch des Unterhaltsberechtigten auch durchgesetzt werden kann.

Da Unterhaltsansprüche in der Regel nur dann für die Vergangenheit geltend gemacht werden können, wenn sie rechtshängig geworden sind, bedeutet die Anfrage beim Arbeitgeber nur unnötigen Zeitverlust, da dieser rechtlich nicht verpflichtet ist, dem Amtsvormund oder Unterhaltsbeistand darüber Auskunft zu erteilen. Die Anfrage ist deshalb nicht geeignet, den Unterhalt zu sichern, weil die erforderliche Auskunft nicht erlangt werden kann. Im Gegenteil ist es dem Arbeitgeber aus Gründen des Personaldatenschutzes verboten, ohne Zustimmung des Betroffenen Auskunft über die Einkommensverhältnisse zu erteilen. Die Rechtspflicht des Unterhaltsverpflichteten kann keine Rechtfertigung für einen Verstoß gegen datenschutzrechtliche Bestimmungen durch den Arbeitgeber darstellen.

Die Anfrage kann darüber hinaus auch dem Unterhaltsberechtigten mittelbar schaden, wenn dem Arbeitgeber der zugrunde liegende Sachverhalt bislang unbekannt war und er die Mitteilungen des Unterhaltsbeistands zum Anlaß für arbeitsrechtliche Maßnahmen nimmt. Dies stellt gerade bei mittleren und kleinen Betrieben möglicherweise ein erhebliches Risiko dar. Die datenschutzwidrige Anfrage des Amtsvormunds beim Arbeitgeber gefährdet daher zusätzlich die Realisierung des Unterhaltsanspruchs.

Wir haben deshalb empfohlen, im Falle der Auskunftsverweigerung die notwendigen rechtlichen Schritte gegen den Unterhaltsschuldner selbst einzuleiten, die erforderlich sind, den Anspruch der Höhe und dem Grunde nach zu sichern, nämlich die zivilrechtliche Stufenklage auf Auskunftserteilung mit anschließender Bezifferung des geltend gemachten Unterhaltsanspruchs.

Aktenführung

Wir hatten schon mehrere Jahre vor dem Inkrafttreten des SGB VIII Vorschläge unterbreitet, die Aktenführung der Jugendverwaltung neu zu strukturieren und von der auf eine Bedarfsgemeinschaft bezogenen Aktenführung weg zu einer *vorgangsbezogenen Differenzierung* zu kommen. Unsere Vorschläge, die seinerzeit auf nur verhaltene Zustimmung gestoßen waren, teilweise sogar abgelehnt wurden, werden nunmehr in einigen Berliner Bezirken erfolgreich praktiziert.

Die Neustrukturierung der Aktenführung wurde begünstigt durch die Novellierung des Jugendhilferechts und insbesondere dort durch die Vorschriften zur Dokumentation (§ 63 SGB VIII). Die Mitarbeiter der Ämter berichteten übereinstimmend, daß die Verwaltungstätigkeit näher an die hilfebedürftigen Menschen herangerückt und entbürokratisiert worden sei. Insbesondere das Risiko der Betroffenen, durch stigmatisierende Erfahrungsberichte in ein möglicherweise unzutreffendes Licht gerückt zu werden, ist weitgehend abgemildert worden. Wir hoffen, daß diese Erfahrungen auch bei anderen Bezirken gemacht werden. In einer Empfehlung der Senatsverwaltung für Jugend und Familie[93] wurden diese Grundsätze als allgemeine Leitlinie für die bezirkliche Jugendverwaltung empfohlen.

93 Rundschreiben vom 19. März 1993 „über Grundsätze der Aktenführung in den Ämtern für sozialpädagogische Dienste (Familienfürsorge) sowie zum Umfang der Aktenweitergabe und -aufbewahrung"

4.7 Justiz

Gesetzgebung

Noch immer ist das *Justizmitteilungsgesetz*[94] nicht in Kraft; der Bundesrat hatte 1992 zu einem Entwurf der Bundesregierung eine ablehnende Stellungnahme abgegeben. Dies ist bedauerlich, da in diesem Bereich klare und datenschutzfreundliche Rechtsgrundlagen erforderlich sind.

In Berlin gibt es seit dem Inkrafttreten des Ausführungsgesetzes zum Gerichtsverfassungsgesetz (AGGVG)[95] eine Übergangsregelung in § 29 Abs. 2 AGGVG. Den Verwaltungsvorschriften „Mitteilungen in Zivilsachen" (MiZi) und „Mitteilungen in Strafsachen" (MiStra) ist bis zur Verabschiedung des Justizmitteilungsgesetzes Gesetzeskraft verliehen worden.

Das Gesetzgebungsverfahren im Bereich des *Strafvollzuges* macht ebenfalls keine Fortschritte, obwohl auch hier - angesichts der vielfältigen und umfangreichen Datenverarbeitung - die Schaffung klarer gesetzlicher Grundlagen besonders dringend ist.

Auch der bereits 1989 vorgelegte Entwurf für ein *Strafverfahrensänderungsgesetz (StVÄG)* ist immer noch nicht in den Bundestag eingebracht worden[96]. Nur das Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG), das am 15. September 1992 in Kraft getreten ist[97], nahm einige - besonders gravierende - Regelungen vorweg.

Kürzlich ist von den Ländern ein neuer Entwurf unter dem Titel *„Dateienregelungen in Strafverfahren"* erarbeitet worden. Dieser Entwurf ist datenschutzrechtlich nicht akzeptabel. Die vorgesehenen Regelungen bleiben noch hinter dem STVÄG[98] zurück. Der Gesetzentwurf bedarf, wenn er weiterverfolgt werden soll, dringend einer Überarbeitung, die eine sorgfältige Abwägung zwischen den Interessen des Staates an der Strafverfolgung und dem informationellen Selbstbestimmungsrecht der Bürger erkennen lassen.

So soll eine Generalermächtigung für spontane Datenübermittlungen anderer öffentlicher Stellen an die Staatsanwaltschaft eingefügt werden, die in ihrer Pauschalität höchst bedenklich ist. Abzulehnen ist auch das vorgesehene Akteneinsichtsrecht für die Gerichte, Staatsanwaltschaften und andere Justizbehörden zum Zwecke der „Rechtspflege". Ein Akteneinsichtsrecht sollte die Ausnahme bleiben und nur erfolgen, wenn Auskünfte aus Strafakten nicht genügen. Dies ist unerläßlich, da in den Strafakten unterschiedlichste Daten enthalten sein können, die nicht immer in vollem Umfang für die jeweilige Aufgabe der anfragenden Stelle erforderlich sein müssen. Außerdem sollten Auskunfts- und Akteneinsichtsrechte auf den Zweck der Strafrechtspflege beschränkt sein. Die Zweckbestimmung „Rechtspflege" ist viel zu unbestimmt.

Ferner enthält der Entwurf eine Regelung, nach der Auskünfte aus Akten an öffentliche Stellen zulässig sein sollen, wenn dies zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben erforderlich ist. Akteneinsicht soll in diesen Fällen schon dann gewährt werden können, wenn die Erteilung von Auskünften einen unverhältnismäßigen Aufwand erfordert. Diese Regelung steht nicht im Einklang mit den im Volkszählungsurteil aufgestellten Anforderungen an eine normenklare Eingriffsbefugnis. Hiermit ist ein nahezu ungehinderter Zugriff öffentlicher Stellen auf sämtliche in Strafverfahren gesammelten Daten möglich. Die Möglichkeit zur Akteneinsicht, wenn eine Auskunft mit einem „unverhältnismäßig großen Aufwand" verbunden ist, dürfte sich durch die Überlastung der Strafverfolgungsbehörden in der Praxis als ein allgemeines Akteneinsichtsrecht aller öffentlichen Stellen in Strafakten auswirken. Wir haben in unserer Stellungnahme betont, daß klare, differenzierte Kriterien, in welchen Fällen und zu welchem Zweck Auskünfte aus Strafakten an andere öffentliche Stellen erteilt werden dürfen, unerläßlich sind.

94 BT-Drs. 12/3199
95 Jahresbericht 1991, 3.6 und Jahresbericht 1992, 4.3
96 Jahresbericht 1991, 3.6 und Jahresbericht 1992, 4.3
97 Jahresbericht 1992, 4.3; BGBl. I 1992, S. 1302
98 Jahresbericht 1990, 3.6, Jahresbericht 1991, 3.6, Jahresbericht 1992, 4.3

Mit § 482 des Entwurfs soll eine Rechtsgrundlage zur automatisierten Datenverarbeitung geschaffen werden. Gerichte, Staatsanwaltschaften und andere Justizbehörden dürfen danach personenbezogene Daten in Dateien speichern, verändern und nutzen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Dies ist eine Generalklausel ohne jede Aussage darüber, welche Daten zu welchem Zweck gespeichert werden dürfen. Diese Vorschrift ermöglicht ein uneingeschränktes Sammeln von Informationen über jeden, wenn es von den Strafverfolgungsbehörden für erforderlich gehalten wird.

Weiterhin soll eine Regelung für gemeinsame und verbundene Dateien geschaffen werden. Diese Regelung ist ebenfalls so allgemein gefaßt, daß sie eine Befugnis zu einer unüberschaubaren, nicht mehr nachvollziehbaren Verflechtung verschiedenster Datensammlungen nicht nur der Strafverfolgungsbehörden schafft. Aufgrund der fehlenden Präzisierung wären sogar gemeinsame Datenbestände von Polizei und Justiz zulässig.

Genetischer Fingerabdruck

In der Vergangenheit hatten wir mehrfach darauf hingewiesen, daß die Nutzung des genetischen Fingerabdrucks für Zwecke der Identifizierung oder Entlastung von Tatverdächtigen möglichst eindeutig in der Strafprozeßordnung geregelt werden sollte[99]. Inzwischen hat die Bundesregierung den Entwurf eines *Strafverfahrensänderungsgesetzes zur DNA-Analyse („genetischer Fingerabdruck")* beschlossen[100], zu dem der Bundesrat im November 1993 Stellung genommen hat. Diese Stellungnahme enthält nur in einem Punkt eine Verbesserung des Regierungsentwurfs. So ist die vom Bundesrat geforderte Klarstellung zu begrüßen, daß molekulargenetische Untersuchungen sich nicht auf Bereiche des menschlichen Genoms erstrecken dürfen, die Aufschluß über Erbanlagen des Betroffenen geben können.

In allen anderen Punkten würde eine Berücksichtigung der Stellungnahme des Bundesrates den Gesetzentwurf der Bundesregierung, der selbst in einer Reihe von Punkten unbefriedigend ist, aus datenschutzrechtlicher Sicht noch weiter verschlechtern.

Zwar sieht der Regierungsentwurf vor, daß molekulargenetische Untersuchungen nur durchgeführt werden dürfen, soweit sie zur Feststellung der Abstammung oder der Tatsache, ob aufgefundenes Spurenmaterial von dem Beschuldigten oder dem Verletzten stammt, erforderlich sind. Für den Fall, daß entgegen dieser Vorschrift dennoch *Überschußinformationen* z.B. über Erbanlagen der untersuchten Person erhoben werden, müßte die Verwertung dieser Informationen gesetzlich verboten werden. Eine entsprechende Regelung enthält der von der SPD-Bundestagsfraktion im Dezember 1992 eingebrachte Gesetzentwurf zum selben Problemkreis[101]. Dagegen ist nach dem Regierungsentwurf die Verwertung rechtswidrig erhobener Informationen über Erbanlagen im Prozeß zulässig. Damit kann das Verbot der Erhebung von Überschußinformationen jederzeit unterlaufen werden.

Die Bundesregierung sieht in ihrem Gesetzentwurf mit Recht kein Bedürfnis für eine *Eilzuständigkeit der Staatsanwaltschaft* zur Anordnung von molekulargenetischen Untersuchungen als gegeben an. Dies gilt insbesondere angesichts der langen Haltbarkeit von Zellresten im Spurenmaterial, die es ausgeschlossen erscheinen lassen, daß die Entscheidung eines Richters für diesen weitreichenden Eingriff nicht abgewartet werden kann. Soweit einem Beschuldigten Blutproben oder sonstige Körperzellen entnommen werden sollen, kann dies auch geschehen, ohne daß sofort eine molekulargenetische Untersuchung angeordnet werden muß. Insofern ist es unverständlich, daß der Bundesrat dennoch die Begründung einer Eilzuständigkeit der Staatsanwaltschaft für erforderlich hält.

Der Gesetzentwurf der Bundesregierung läßt die Verwendung von Blutproben oder sonstigen Körperzellen für Zwecke jedes beliebigen anhängigen Strafverfahrens zu. Molekulargenetische Untersuchungen sollten jedoch auf einen begrenzten Katalog von *besonders schweren Straftaten* beschränkt werden. Dies halten allerdings weder die Bundesregierung noch der Bundesrat für erforderlich. Sie wollen im Gegenteil den Einsatz derartiger Untersuchungsmethoden in jedem Strafverfahren ermöglichen. Es ist zwar richtig, daß der Regierungsentwurf mit der Beschränkung der Untersuchungsmethoden auf Feststellungen zur Abstammung und zur Zuordnung von Tatspuren zu Beschuldigten oder Verletzten den Kreis der in Frage kommenden Delikte praktisch von vornherein begrenzt. Es wäre jedoch wünschenswert, wenn der Gesetzgeber selbst eine entsprechende ausdrückliche Begrenzung in die Strafprozeßordnung aufnehmen würde. Dann muß auch sichergestellt werden, daß eine Verwendung der Ergebnisse aus dem Ursprungsverfahren in anderen Verfahren (z.B. bei der Verfolgung von Bagatelldelikten) ausgeschlossen ist.

Nach den Vorschlägen der Bundesregierung können mit der Durchführung der Untersuchung *Sachverständige* beauftragt werden, die öffentlich bestellt oder nach dem Verpflichtungsgesetz verpflichtet oder Amtsträger sind, die der ermittlungsführenden Behörde nicht angehören oder einer Organisationseinheit dieser Behörde angehören, die von der ermittlungsführenden Dienststelle organisatorisch und sachlich getrennt ist. Diese Beschränkung des Personenkreises bleibt hinter dem zurück, was wir in der Vergangenheit für erforderlich gehalten haben, um eine unvoreingenommene Durchführung der molekulargenetischen Untersuchung sicherzustellen. Der Bundesrat allerdings hat eine weitere Lockerung der Beschränkung des Personenkreises befürwortet, die dazu führen würde, daß letztlich jeder Polizeibeamte im Eilfall auf Anordnung des ermittelnden Staatsanwalts mit einem auf dem Markt erhältlichen „Test-Kit" (Untersuchungskoffer) die molekulargenetische Untersuchung, die er für seine Ermittlungen zu benötigen glaubt, selbst durchführen dürfte.

Außerdem hat der Bundesrat vorgeschlagen, die von der Bundesregierung mit Recht für notwendig gehaltene *Anonymisierung des Untersuchungsmaterials* vor Übergabe an den Sachverständigen zu lockern. Demgegenüber darf dem Sachverständigen die Zuordnung des Untersuchungsmaterials zum Betroffenen selbst nicht möglich sein. Dies ist nur bei Verwendung eines Codes gewährleistet, den ausschließlich das anordnende Gericht entschlüsseln kann.

Schließlich hat der Bundesrat dem Vorschlag der Bundesregierung widersprochen, den Datenschutzbeauftragten des Bundes und der Länder eine *Kontrollkompetenz* für die mit molekulargenetischen Untersuchungen beauftragten Sachverständigen einzuräumen. Dabei verkennt der Bundesrat, daß auch private Sachverständige mit der Untersuchung beauftragt werden können. Dann aber ergibt sich ein erhebliches Kontrolldefizit, weil die Aufsichtsbehörden auf die bloße Anlaßkontrolle bei Dateiverarbeitung beschränkt sind. Es ist daher unabdingbar, daß entsprechend dem Regierungsentwurf die Datenschutzbeauftragten des Bundes und der Länder eine ausdrückliche Kontrollkompetenz unabhängig von der Verarbeitung in Dateien bei allen (auch privaten) Sachverständigen erhalten, die molekulargenetische Untersuchungen nach der Strafprozeßordnung durchführen.

Datenschutzrechtliche Strafvorschriften

Seit der Novellierung des Berliner Datenschutzgesetzes hat der Berliner Datenschutzbeauftragte - neben der/dem Betroffenen - das Recht, Strafantrag zu stellen, wenn der Verdacht besteht, daß die Strafvorschrift des § 32 BlnDSG erfüllt ist. Danach wird bestraft, wer unbefugt personenbezogene Daten, die nicht offenkundig sind, übermittelt oder verändert oder abruft oder sich aus in Behältnissen verschlossenen Dateien verschafft.

Das *Antragsrecht des Berliner Datenschutzbeauftragten* ist aufgenommen worden, um auch in Fällen eine Strafverfolgung zu ermöglichen, in denen ein Strafantrag des Betroffenen nicht vorliegt, die Verletzung der informationellen Selbstbestimmung aber gleichwohl eine Strafsanktion erfordert.

Hieraus ergibt sich, daß in erster Linie der Betroffene (der Verletzte) darüber entscheiden sollte, ob ein Strafantrag nach § 32 BlnDSG gestellt wird oder nicht. Soweit möglich, sollte der Betroffene als erster von der Staatsanwaltschaft befragt werden, ob er Strafantrag stellen will oder nicht.

99 vgl. dazu JB 1989, 2.3; 1990, 3.6 und 1992, 4.3
100 BR-Drs. 729/93
101 BT-Drs. 12/3981

Der Berliner Datenschutzbeauftragte ist bis Ende 1993 in 16 Fällen gefragt worden, ob er von seinem Strafantragsrecht Gebrauch machen will. In drei Fällen wurde Strafantrag gestellt, in den übrigen Fällen von der Stellung eines Strafantrages abgesehen. Dabei wurde von folgenden Kriterien ausgegangen:

Ein Strafantrag ist nur dann zu stellen, wenn der *objektive Tatbestand* des § 32 BlnDSG vorliegt. Bei Zweifeln über den tatsächlichen Geschehensablauf muß die Strafbarkeit des vermuteten Verhaltens feststehen.

Im Hinblick auf die Wahrung der informationellen Selbstbestimmung muß ein öffentliches Interesse an der Strafverfolgung bestehen. Unsere Aufgabe erschöpft sich nicht darin, dem Bürger zu seinem Recht zu verhelfen. Vielmehr ist die Sicherstellung und Verbesserung des Datenschutzes eine öffentliche Aufgabe, die auch abgelöst von Individualinteressen zu vertreten ist. Für das Vorliegen eines öffentlichen Interesses bietet Ziffer 86 Abs. 2 der Richtlinien für das Straf- und Bußgeldverfahren eine Orientierung. Danach wird ein öffentliches Interesse in der Regel vorliegen, wenn der Rechtsfrieden über den Lebenskreis des Verletzten hinaus gestört und die Strafverfolgung ein gegenwärtiges Anliegen der Allgemeinheit ist. Wichtige Aspekte sind hierfür die Intensität der Straftat, die Frage, ob Wiederholungsgefahr besteht, der Schadensumfang, die Kommerzialisierung und die Frage, ob bewußt Systemschwächen ausgenutzt oder auch geschaffen wurden.

Ist ein öffentliches Interesse zu bejahen, muß die subjektive Betroffenheit Einzelner nicht mehr berücksichtigt werden. Allerdings erübrigt sich auch in diesen Fällen ein Strafantrag, wenn die Straftat ohnehin von Amts wegen verfolgt wird, also wenn konkurrierende Delikte in ihrem Unrechtsgehalt gegenüber dem Unrechtsgehalt der datenschutzrechtlichen Verstöße überwiegen. Auch bei Antragsdelikten außerhalb des Datenschutzgesetzes (z.B. § 203 StGB) erübrigt sich ein Antrag, wenn bereits Strafanträge von dritter Seite vorliegen und nicht die Gefahr besteht, daß diese Strafanträge zurückgenommen werden.

Unabhängig vom öffentlichen Interesse ist zu prüfen, ob die *Interessen des Betroffenen* einen Strafantrag erforderlich machen. Handelt es sich um einen verhältnismäßig geringfügigen Verstoß und liegt ein Strafantrag des Betroffenen vor, wird kein Strafantrag gestellt. Dasselbe gilt, wenn der Betroffene ausdrücklich auf einen Strafantrag verzichtet hat. Hingegen soll dann ein Strafantrag gestellt werden, wenn der Betroffene den Strafantrag nicht stellen kann oder wegen einer Zwangslage nicht freiwillig stellen will.

Durch mehrere Bürgereingaben sind wir darauf aufmerksam gemacht worden, daß die Staatsanwaltschaft Strafverfahren einstellte, die auf Strafanträge von Betroffenen wegen des Verdachtes einer unbefugten Offenbarung von Schriftstücken oder Aktenbestandteilen eingeleitet werden, weil sie die Auffassung vertritt, daß § 32 BlnDSG nur die Weitergabe von elektronisch gespeicherten Daten, nicht aber von Schriftstücken oder Aktenbestandteilen unter Strafe stellt.

Zur Begründung dieser Auslegung wurde auf die gesetzliche Definition des Begriffs des Übermittelns in § 4 Abs. 2 Nr. 4 BlnDSG Bezug genommen, wo das Übermitteln als das Bekanntgeben *gespeicherter oder durch Datenverarbeitung gewonnener Daten* an Dritte bestimmt ist. Aus der Gesetzesdefinition des § 4 Abs. 2 Nr. 2 BlnDSG, in der das Speichern als das Erfassen, Aufnehmen oder Aufbewahren von Daten *auf einem Datenträger* gesetzlich bestimmt wird, wurde hergeleitet, daß Papier, Akten und Aktenbestandteile keine Datenträger seien.

Diese Auslegung ist unzutreffend. Der Anwendungsbereich des neuen Berliner Datenschutzgesetzes ist nicht mehr auf Dateien beschränkt. Alle Bestimmungen dieses Gesetzes gelten auch für die Datenverarbeitung in Akten, es sei denn, es sind ausdrücklich besondere Regelungen für die Datenverarbeitung auf bestimmten Datenträgern vorhanden. So hat der Gesetzgeber wegen der besonderen Gefahren, die mit den technischen Möglichkeiten der automatisierten Datenverarbeitung verbunden sind, besondere Bestimmungen für diese Art der Datenverarbeitung vorgesehen (vgl. §§ 15, 16 Abs. 2 BlnDSG). § 32 BlnDSG entspricht dieser Gesetzessystematik.

Datenträger ist jedes Medium, auf dem Daten lesbar festgehalten werden können. Jedes Material, das beschriftet werden und auf andere Weise Informationen aufnehmen kann, genügt. Papier, Akten und Aktenbestandteile, ja auch Audio- oder Videobänder (wichtig beim Schutz von Daten aus Überwachungsmaßnahmen!), sind Datenträger. § 32 Abs. 1 Nr. 1 BlnDSG erfaßt das Übermitteln oder Verändern personenbezogener Daten unabhängig davon, ob diese Daten in Dateien, Akten oder auf sonstigen Datenträgern gespeichert sind. Die Staatsanwaltschaft wird dies künftig berücksichtigen.

Speicherung im staatsanwaltschaftlichen Informationssystem ASTA

Eine Petentin wurde am Schalter eines Postgiroamtes beschuldigt, gefälschte Geldscheine zu benutzen. Die Kriminalpolizei stellte nach kurzer Zeit fest, daß die Scheine echt waren. Das gegen sie eingeleitete Ermittlungsverfahren wurde von der Staatsanwaltschaft mangels hinreichenden Tatverdachts nach § 170 Abs. 2 Strafprozeßordnung (StPO) eingestellt. Sie hat sich darüber beschwert, daß ihre Daten im Informationssystem ASTA der Amts- und Staatsanwaltschaften nicht gelöscht wurden, obwohl eine Straftat eindeutig nicht vorlag.

Die Staatsanwaltschaft hat der Petentin mitgeteilt, daß sich zwar bereits bei der Erörterung bei der Polizei herausgestellt hatte, daß eine Straftat nicht vorlag, aber eine Aufbewahrung und Registrierung des Vorganges für fünf Jahre erfolgen müsse. Die Akten würden nur dann zur Einsichtnahme herangezogen werden, wenn gegen die Petentin wider Erwarten erneut der Verdacht einer Straftat entstünde.

Die Staatsanwaltschaft betreibt zur Aktenverwaltung das Informationssystem ASTA. Hier werden unterschiedslos *alle* Ermittlungsverfahren registriert und nach Ablauf von fünf Jahren, den bundeseinheitlichen Aufbewahrungsbestimmungen für die Akten, gelöscht.

Die Aufbewahrung der Strafermittlungsakten kann allenfalls zu Zwecken der Dokumentation des Vorganges erfolgen, aber nicht - wie in der Antwort der Staatsanwaltschaft gegenüber der Petentin angegeben - für die künftige Straftatenverfolgung. Bei Fällen, in denen keine Straftat vorgelegen hat, ist die Aufbewahrungsdauer der Akten und damit die Speicherung in ASTA auf das unbedingt notwendige Maß zu reduzieren. Die Dauer der Speicherung sollte in diesen Fällen ein Jahr nicht überschreiten. Dies wurde von der Generalstaatsanwaltschaft unter Hinweis auf die bundeseinheitlichen Aktenaufbewahrungsbestimmungen abgelehnt. Wir empfehlen, daß die Senatsverwaltung für Justiz eine Initiative zur Änderung dieser Aufbewahrungsbestimmungen ergreift.

Ungeachtet dessen ist dafür zu sorgen, daß der Betroffene keine Nachteile durch die Datenspeicherung erleiden kann. Wir haben deshalb bei der Staatsanwaltschaft angeregt, in derartigen Fällen, in denen sich nach Einleitung eines strafrechtlichen Ermittlungsverfahrens herausstellt, daß eine Straftat objektiv nicht vorgelegen haben kann, im ASTA-System einen Hinweis aufzunehmen, daß ein Anfangsverdacht nicht vorgelegen hat.

Auch wenn das ASTA-System vornehmlich ein der Aktenverwaltung dienendes, internes Register ist und hierzu strenge Zugangsbeschränkungen bestehen, ist die Speicherung personenbezogener Daten ein Eingriff in das informationelle Selbstbestimmungsrecht des jeweils Betroffenen. Es ist ein schutzwürdiges Interesse der Betroffenen, daß die fehlende strafrechtliche Relevanz eines gegen sie eingeleiteten und nach § 170 Abs. 2 StPO eingestellten Ermittlungsverfahrens im ASTA-System hervorgehoben wird, wenn sich herausstellt, daß sie objektiv keine Straftat begangen haben.

Nachdem sich die Staatsanwaltschaft beharrlich geweigert hatte, einen entsprechenden Hinweis in ASTA aufzunehmen, wurde diese schließlich von der Senatorin für Justiz gebeten, in den Fällen des § 170 Abs. 2 StPO, in denen sich herausstellt, daß eine Straftat objektiv nicht vorgelegen haben kann, einen Hinweis „objektiv keine Straftat" im Feld „Bemerkungen" aufzunehmen.

Mängel beim Zentralen Schuldnerverzeichnis

Ein Rechtsanwalt wunderte sich, daß ein Versandhaus ihm eine Lieferung nicht zukommen lassen wollte. Überraschend wurde ihm auch ein Kreditkartenantrag abgelehnt aus Gründen, die ihm nicht mitgeteilt wurden. Eine Auskunft bei der SCHUFA hat dann die ganze Angelegenheit erhellt: Er war mit zwei Haftbefehlen im Zentralen Schuldnerverzeichnis beim Amtsgericht Schöneberg eingetragen. Der Anwalt war in zwei Vollstreckungsverfahren fälschlicherweise statt des von ihm vertretenen Schuldners eingetragen worden.

Beim Amtsgericht Schöneberg wird zentral ein Verzeichnis geführt über Personen, die eine eidesstattliche Versicherung nach § 807 Zivilprozeßordnung (ZPO) abgegeben haben oder gegen die nach § 901 ZPO die Haft angeordnet ist. Auch wer eine eidesstattliche Versicherung nach § 284 der Abgabenordnung (AO) abgegeben hat, wird in das Schuldnerverzeichnis eingetragen.

Da nach § 915 ZPO jedem auf Antrag Auskunft über das Bestehen oder Nichtbestehen von Eintragungen in das Schuldnerverzeichnis erteilt wird oder Einsicht in das Verzeichnis gewährt wird, können fehlerhafte Eintragungen sich für den Betroffenen sehr unangenehm auswirken, wie der Fall unseres Petenten zeigte.

In seiner Stellungnahme hat das Amtsgericht ausgeführt, daß die Eintragung im *Zentralen* Schuldnerverzeichnis auf der Eintragung im *örtlichen* Schuldnerverzeichnis beruht. Der Fehler im Fall unseres Petenten hat das Amtsgericht Schöneberg dazu veranlaßt, in seinem Zuständigkeitsbereich eine geänderte Fassung der Eintragungsverfügung zu erproben, um Falscheintragungen mit noch größerer Sicherheit auszuschließen. Die Protokolle der nichtöffentlichen Sitzungen des Amtsgerichtes in einer Zwangsvollstreckungsangelegenheit werden ergänzt um einen Hinweis auf den Schuldner, der in das Schuldnerverzeichnis eingetragen wird. Auch der Präsident des Amtsgerichtes Tiergarten ist inzwischen an die Direktoren der Amtsgerichte herangetreten und hat die probeweise Einführung des in Zwangsvollstreckungssachen ergänzten Protokollvordruckes empfohlen.

Übersendung vollständiger Ehescheidungsakten durch das Familiengericht an die Ausländerbehörde

Ein Rechtsanwalt machte darauf aufmerksam, daß die Eheschließungsakte seines Mandanten vom Familiengericht an die Ausländerbehörde übersandt worden sei. Die Überprüfung ergab, daß im Jahr 1992 die Ausländerbehörde in insgesamt elf Fällen eine Übersendung der gesamten Ehescheidungsakte oder der Kopie des Scheidungsurteils gestellt wurden. Zur Begründung wurde angeführt, die Aufenthaltserlaubnis sei ausschließlich im Hinblick auf die Eheschließung mit einem deutschen Ehepartner erteilt worden und nunmehr müsse überprüft werden, ob nicht eine Scheinehe vorliege.

In fünf Fällen übersandte das Familiengericht die gesamten Verfahrensakten. In einem Fall wurde das Scheidungsurteil und in einem anderen Fall das Verhandlungsprotokoll übersandt. In zwei Fällen wurde schriftlich, in einem Fall telefonisch Auskunft über den im Scheidungsurteil festgehaltenen Trennungszeitpunkt gegeben.

Durch die Übersendung der Scheidungsakten wurden u. a. Angaben über das Einkommen und Beschäftigungszeiten der Ehepartner, Unterlagen zur Durchführung des Versorgungsausgleiches, Akten zum Prozeßkostenhilfeantrag, Listen über Haushaltsgegenstände der Eheleute offenbart. Hinzu kommen äußerst sensible Daten wie Angaben über den Gesundheitszustand des deutschen Ehegatten, Name und Anschrift der betroffenen Person, zu der ein Ehegatte außereheliche Beziehungen hatte, Name und Anschrift der Zeugen von tätlichen Auseinandersetzungen der Ehegatten.

Rechtsgrundlagen für die Datenübermittlungen vom Familiengericht an die Ausländerbehörde sind sowohl im Ausländergesetz (AuslG) als auch im Ausführungsgesetz zum Gerichtsverfassungsgesetz (AGGVG) enthalten. Beide Vorschriften sind an dieselben Voraussetzungen geknüpft. Nach § 76 Abs. 1 i.V.m. § 75 Abs. 1 AuslG haben öffentliche Stellen der Ausländerbehörde auf Ersuchen die bekanntgewordenen Umstände mitzuteilen, die für die Aufgabenerfüllung nach dem Ausländergesetz erforderlich sind. Gerichte haben nach § 21 Abs. 5 Nr. 2 AGGVG Verwaltungsbehörden Einsicht in Akten zu gewähren oder Auskünfte zu erteilen, soweit dies zur Erfüllung der ihnen gesetzlich zugewiesenen Aufgaben erforderlich ist.

Für die Aufgabenerfüllung der Ausländerbehörde sind die Informationen, ob eine sogenannte *Scheinehe* eingegangen wurde und der Trennungszeitpunkt für aufenthaltsrechtliche Entscheidungen von Bedeutung. Nach § 23 AuslG wird dem ausländischen Ehegatten eines Deutschen eine Aufenthaltserlaubnis erteilt für drei Jahre im Hinblick auf die Ehe. Die Aufenthaltserlaubnis wird nur dann verlängert, wenn nach drei Jahren die eheliche Lebensgemeinschaft noch besteht. Ein eigenständiges Aufenthaltsrecht erwirkt der ausländische Ehegatte nach der Trennung erst dann, wenn die eheliche Lebensgemeinschaft mindestens drei Jahre angedauert hat.

Vom Landeseinwohneramt - Melderegister - wird die Ausländerbehörde regelmäßig ohne Ersuchen über Ehescheidungen informiert. Erhält die Ausländerbehörde die Mitteilung, daß die Ehe nach Ablauf von drei Jahren geschieden wurde, ist für sie von Bedeutung, wie lange die tatsächliche eheliche Lebensgemeinschaft gedauert hat, insbesondere dann, wenn die Ehezeit nicht viel länger als drei Jahre betragen hat. Sie benötigt in diesen Fällen eine Auskunft vom Familiengericht, wann die Eheleute sich getrennt haben.

Hierfür ist der im Scheidungsurteil angegebene *Trennungszeitpunkt* maßgeblich. Hierüber genügt eine Auskunft des Familiengerichtes.

Bei begründetem Verdacht einer Scheinehe darf die Ausländerbehörde bei Scheidungen nach über dreijähriger Ehezeit oder vor Ergehen eines Scheidungsurteils um Übersendung der Schriftstücke aus der Scheidungsakte bitten, die diesen Verdacht belegen, wenn eine Auskunft - meist dürfte der Trennungszeitpunkt ausreichen - nicht bereits diesen Zweck erfüllt. Vorab ist jedoch grundsätzlich beim Betroffenen Auskunft einzuholen. Erst wenn dies nicht gelingt bzw. begründeter Verdacht besteht, daß Angaben nicht zutreffen, können im Weg der Auskunft beim Familiengericht personenbezogene Daten erfragt werden. Die Übersendung gesamter Akten ist dazu jedenfalls nicht erforderlich.

Schon 1986 haben wir gefordert, Anforderungen von Ehescheidungsunterlagen auf diejenigen Teile zu beschränken, aus denen sich die Umstände des Getrenntlebens ergeben. Die Einhaltung dieses Verfahrens wurde uns damals von der Ausländerbehörde zugesagt. Nach den Feststellungen, die wir nun bei unseren Überprüfungen getroffen haben, ist das damals vereinbarte Verfahren nicht umgesetzt worden. Wir haben das Landeseinwohneramt und Familiengericht aufgefordert sicherzustellen, daß nur die erforderlichen Daten übermittelt werden. Das Familiengericht wird die betroffenen Ehegatten vor der Datenübermittlung hören. Keine Einigung konnte bisher hinsichtlich der Verpflichtung des Familiengerichts zur Prüfung der Übermittlungsvoraussetzungen erzielt werden. Eine abschließende Stellungnahme des Landeseinwohneramtes zu unseren Empfehlungen steht noch aus.

Prozeßakten auf der Straße

Beim abendlichen Spaziergang staunte ein Berliner Bürger nicht schlecht, als er am Straßenrand ein Bündel mit 146 Akten der Berliner Amtsanwaltschaft zu Strafverfahren auffand. Er unterrichtete davon sofort einen Reporter einer Berliner Tageszeitung, der die Akten dann an sich nahm, um sie letztenendes der Amtsanwaltschaft zurückzugeben - allerdings nicht ohne ausführlich in seiner Zeitung über den Fall zu berichten.

Die Amtsanwaltschaft wie auch die vorgesetzte Staatsanwaltschaft beim Landgericht hatten die ausgesonderten und zur Vernichtung bestimmten Akten von einem privaten Papier-Recycling-Unternehmen im Auftrag vernichten lassen. Dazu wurde das Vernichtungsgut zu dem Unternehmen transportiert und dort eingeschlämmt. Dieser ganze Prozeß wird von einem Justizwachtmeister überwacht.

Gegen dieses Verfahren zur Aktenvernichtung ist nichts einzuwenden, wenn wie vorgesehen verfahren wird, die Zusammenarbeit zwischen Justizbehörden und Unternehmen wie verabredet abläuft und der Transport des Vernichtungsgutes so erfolgt, daß unterwegs nichts verlorengehen kann.

Wie die fraglichen Akten nun an dem Tag des Fundes unvernichtet auf öffentliches Straßenland in unmittelbarer Umgebung des Recycling-Unternehmens geraten waren, konnte auch in einem staatsanwaltschaftlichen Untersuchungsverfahren nicht geklärt werden. Der Vermutung, die Akten seien vom Lastkraftwagen heruntergeweht worden, wurde von der Fahrbereitschaft widersprochen, denn der Wagen sei sorgfältig abgedeckt worden und ein vollständiges Bündel sei auch zu schwer, um ohne weiteres vom Wagen heruntergeweht werden zu können. Eine weitere Möglichkeit bestand darin, daß die Akten vor der Vernichtung vom Betriebshof der Recyclingfirma entwendet worden sein konnten und dann auf der Straße abgelegt wurden, um dem Ruf der Firma Schaden zuzufügen.

Dieser Diebstahl hätte durch den Justizwachtmeister, der den Vernichtungsvorgang eigentlich überwachen sollte, verhindert werden müssen. Jedoch war bei diesem Transport entgegen der Weisung kein Justizwachtmeister mitgefahren.

Ein solches Fehlverhalten einzelner Mitarbeiter kann natürlich nie ganz ausgeschlossen werden. Zu beanstanden war jedoch die Tatsache, daß die Zusammenarbeit zwischen den Staatsanwaltschaften und der Recycling-Firma, insbesondere die Verabredungen zu den Abläufen bei der Vernichtung nicht schriftlich und damit revisionsfähig niedergelegt worden waren.

Die *Vernichtung der Akten bei der Recyclingfirma* ist datenschutzrechtlich als *Datenverarbeitung im Auftrag* anzusehen, für die vertragliche Vereinbarungen (Weisungen) u. a. über die Behandlung der Akten und der Abläufe bei der Vernichtung, aber neuerdings auch nach § 3 Abs. 4 BlnDSG die Unterwerfung des privaten Auftragnehmers unter das Berliner Datenschutzgesetz und die Kontrolle durch den Berliner Datenschutzbeauftragten, zu treffen sind. Dieser Verstoß gegen § 3 BlnDSG wurde beanstandet. Der Generalstaatsanwalt beim Landgericht hat dazu geltend gemacht, daß das Verfahren zur Aktenvernichtung nicht als Datenverarbeitung im Auftrag anzusehen sei, weil es von seinen Bediensteten selbst durchgeführt werde. Dies berücksichtigt nicht, daß die verwendeten Geräte und technischen Verfahren bei der Vernichtung in der Verantwortung des Auftragnehmers arbeiten, gewartet und instandgehalten werden. Darüber hinaus zeigte der oben beschriebene Vorfall, daß der Vernichtungsvorgang auch stattfand, wenn der Wachtmeister nicht für die Justizverwaltung zugegen war.

Diese rechtliche Debatte hatte allerdings für das weitere Vorgehen keine Bedeutung. Die Senatsverwaltung für Justiz hat den Aktenfund zum Anlaß genommen, die Geschäftsbeziehungen mit der Recyclingfirma zu beenden. Bereits vor dem Vorfall war im Gebäude des Amtsgerichtes Moabit eine neue leistungsfähige und allen Anforderungen des Datenschutzes entsprechende Aktenvernichtungsanlage installiert worden, die allerdings damals aus bautechnischen Gründen noch nicht in Betrieb genommen worden war. Die Aktenvernichtung erfolgt jetzt also mit dieser neuen Anlage.

Die Präsidentin des Kammergerichtes hat in der Zwischenzeit für ihren Zuständigkeitsbereich einen Datenträgervernichtungsvertrag mit einer anderen Papierrecyclingfirma abgeschlossen, zu dem sie uns Gelegenheit zur Stellungnahme gab, damit er den datenschutzrechtlichen Bestimmungen voll genügt.

4.8 Schule, Berufsbildung und Sport

Erste Erfahrungen mit den Datenschutzregelungen im Berliner Schulgesetz

Die mit dem Artikelgesetz in das Berliner Schulgesetz aufgenommenen Regelungen zum Datenschutz waren bis zum 31. Dezember 1993 durch eine Rechtsverordnung zu untersetzen.

Mit der *Schuldatenverordnung*, die allerdings nicht zum vorgegebenen Zeitpunkt in Kraft gesetzt wurde, wird die Verarbeitung schülerbezogener Daten an Berliner Schulen auf eine rechtliche Grundlage gehoben. Dabei sollen die Grundsätze und die wesentlichen Punkte der bislang geltenden Ausführungsvorschriften über die Führung schriftlicher Unterlagen über Schüler *(AV-Schülerunterlagen)* im wesentlichen übernommen und ergänzt werden. Ausgehend von dem Grundsatz, daß die Schulen datenverarbeitende Stellen sind, werden die Unterlagen, die in den Schulen geführt werden, im einzelnen aufgeführt und die zulässigerweise in diesen Unterlagen zu erhebenden Daten genannt. Diese Unterlagen sind durch den Klassenlehrer zu führen. Die Tätigkeit von Förderausschüssen wird aus datenschutzrechtlicher Sicht legitimiert. Darüber hinaus enthält der Entwurf Regelungen zur Einsichtnahme in Schülerunterlagen, Übermittlungsregelungen und Festlegungen über Aufbewahrungsfristen.

Mehrfach gingen wir in der Vergangenheit auf die Frage der Zulässigkeit der Verarbeitung von Schülerdaten auf *privaten Computern der Lehrer* ein. Die jetzt vorgeschlagene Regelung wird unserer Auffassung nach sowohl den Anforderungen des Datenschutzes als auch den Wünschen der Lehrer gerecht. Danach bedarf die Verarbeitung von Schülerdaten auf privaten Datenverarbeitungsgeräten der Zustimmung des Schulleiters. Der Schuldatenschutzbeauftragte ist zuvor zu hören. Der Lehrer hat schriftlich zuzusichern, dem Berliner Datenschutzbeauftragten die Wahrnehmung seiner Kontrollaufgaben in seiner Privatwohnung zu ermöglichen. Bisher galt für Leistungsdaten (Zeugnisse, Zensurenlisten) der Grundsatz, daß sie zwar im Rahmen der Textverarbeitung erstellt werden dürfen, nach Fertigstellung des Textes jedoch zu löschen sind. Die neue Regelung geht hier von dem realistischen Ansatz aus, daß auch auf privaten Datenverarbeitungsanlagen Leistungsdaten von Schülern über die Dauer eines Schuljahres, Kurses oder Semesters vorgehalten werden dürfen. Sie sind jedoch unmittelbar nach Zeugnisausdruck zu löschen. Verhaltensdaten von Schülern hingegen dürfen nur vorübergehend zum Ausdruck von Zeugnissen gespeichert werden. Die Verarbeitung besonders sensibler Daten wie Gesundheitsdaten auf privaten Datenverarbeitungsgeräten bleibt verboten.

Bei verschiedenen Gesprächen und Überprüfungen an Schulen mußten wir feststellen, daß die Ergänzung des Berliner Schulgesetzes um Datenschutzregelungen erst wenigen Schulleitern und Lehrern bekannt war. Häufig wurden die Lehrer erst durch unsere Broschüre „Datenschutz in der Schule - ein Leitfaden für Schuldatenschutzbeauftragte", von der wir jeder Schule fünf Exemplare übergeben haben, auf diese Ergänzung aufmerksam gemacht. Verschiedene Anfragen von Schulleitern, Schuldatenschutzbeauftragten und Lehrern zeigten uns jedoch, daß die Sensibilität für Fragen des Datenschutzes im Bereich der Schule gewachsen ist.

Statistik in der Schule

Ohne entsprechende Rechtsgrundlage wurde in der Vergangenheit durch die Senatsschulverwaltung die *Schulstatistik* durchgeführt.

Auf der Grundlage des Landesstatistikgesetzes und des geänderten Schulgesetzes wird die Übermittlung von Einzelangaben durch die Schulen an die Senatsschulverwaltung als Träger der Schulstatistik nunmehr als Landesstatistik legitimiert. Die Daten werden in schwach anonymisierter Form übermittelt. An die die Schulstatistik durchführende Organisationseinheit der Senatsschulverwaltung werden die gleichen Anforderungen hinsichtlich der Abschottung gestellt, wie an statistische Landesämter oder kommunalstatistische Ämter. Jegliches Zusammenführen von Einzelangaben der Schulstatistik mit anderen Angaben zur Herstellung eines Personenbezuges wird unter Strafe gestellt.

Die Umfrage zu *Winterferien ab dem Jahr 1995* war sicherlich dem Bemühen um elterliche Akzeptanz für Entscheidungen der Senatsschulverwaltung geschuldet. Die datenschutzrechtlichen Mängel dieser Erhebung wären durch eine frühzeitige Konsultation des Berliner Datenschutzbeauftragten vermeidbar gewesen. Auch bei einer - wie im vorliegenden Fall - auf Freiwilligkeit und Einwilligung gestützten Umfrage dürfen nur die Daten erhoben werden, die unmittelbar dem Zweck der anonymisierten zusammengefaßten Auswertung dienen. So wurden als Hilfsmerkmale die Angaben „Klasse" und „Name des Schülers" über alle Erhebungsstufen (Schule, Abteilung Volksbildung des Bezirksamts, Senatsschulverwaltung) weitergegeben. Daher wandten wir uns

im Mai an die Senatsschulverwaltung und wiesen darauf hin, daß die Einzelbögen der Eltern nach Zusammenzählen und Übertragen auf die Summierungsbögen je Schule zu vernichten sind. Auch die vielfältigen Hinweise der Eltern machten es im Regelfall nicht erforderlich, Name und Klasse zu erheben und diese Daten über einen längeren Zeitraum vorzuhalten. Ende Oktober mußten wir feststellen, daß die uns von der Senatsschulverwaltung zugesagte Vernichtung der einzelnen Erhebungsbögen darin bestand, sie nach und nach in den normalen Hausmüll zu geben.

Eine Reihe von Anfragen erreichte uns zur *Schülerstatistik 1993*. Erstmals wurde die Anzahl der Asylbewerberkinder je Klasse erfragt. Diese Frage wurde auf die mit Rundschreiben von 1988 bzw. 1992 erfolgte Aufforderung gestützt, auf Schülerbogen und Schülerkartei entsprechende Vermerke anzubringen. In den AV-Schülerunterlagen ist jedoch der Umfang der Angaben im Schülerbogen und in der Schülerkartei verbindlich geregelt. Dabei wird die Erhebung eines Merkmales, das die Kinder als Asylbewerber ausweist, nicht zugelassen.

Lehrer-Informations- und Verwaltungssystem (LIV)

Mit dem LIV wird im Bereich der Berliner Verwaltung erstmalig ein System zur Verarbeitung von Personaldaten geplant, welches administrierende Aufgaben der Personal- und Stellenverwaltung durch die Einbindung der Schulaufsicht mit Aufgaben der Personalsteuerung, -aufsicht und -kontrolle verbindet.

Die Trennung der verschiedenen Aufgabenbereiche erfolgt durch die Definition grober *Benutzerprofile*. Während sich für die Personal- und Stellenverwaltung wegen der relativ strikten personalrechtlichen Vorgaben noch recht einfach festlegen läßt, welche Funktionen mit welchen Daten dort bereitgestellt werden müssen, ist dies für die Schulaufsicht nicht so einfach möglich. Auch hier gibt es zwar rechtliche Vorgaben, die einen Mindestbedarf an Daten und Funktionen begründen, jedoch liegt es im Ermessen der Schulaufsichtsbeamten, mit welchen Daten und Methoden sie ihre Aufgaben wahrnehmen. Gleiches gilt für die Planungs- und Steuerungsaufgaben der Senatsverwaltung für Schulwesen, Berufsbildung und Sport.

Im Pflichtenheft werden die einzelnen Datenbereiche ausführlich dargestellt, die den verschiedenen Fachbenutzern für den lesenden oder schreibenden Zugriff zur Verfügung gestellt werden sollen.

Allerdings war zu bemängeln, daß eine *Analyse des Daten- und Funktionsbedarfs* der Schulaufsicht ebenso fehlte wie eine Analyse des Datenbedarfs der Senatsschulverwaltung, die für planerische und statistische Aufgaben der Hauptverwaltung im Rahmen der (anonymisierten) Lehrerindividualdatei (LID) eine regelmäßige Übermittlung von Daten aus dem LIV beansprucht. Wegen des Pilotcharakters des Verfahrens, der Dispositionsmöglichkeiten von Schulaufsicht und Senatsverwaltung hinsichtlich des Daten- und Funktionsbedarfs und des gegenüber reinen Personal- und Stellenverwaltungssystemen stärkeren Eingriffs in das informationelle Selbstbestimmungsrecht der betroffenen Mitarbeiter wäre eine solche Analyse notwendig gewesen. In ihr hätte durch einen Vergleich der bisherigen (nicht automationsgestützten) mit den künftigen (mit LIV zu unterstützenden) Verfahren der Daten- und Funktionsbedarf präziser und wohl auch maßvoller ermittelt werden können.

Diese Gegenüberstellung von Ist-Abläufen und Soll-Konzepten gehört zwar zum Standard der Vor- und Hauptuntersuchungen, die bei der Entwicklung eines IT-Anwendungsverfahrens erfolgen müssen, ist jedoch für das LIV nicht durchgeführt worden. Vielmehr ist der Datenbedarf in Abstimmungen mit den Vertretern der Bezirke ohne nachvollziehbare Analysen ermittelt worden. Dies hat zu einer Maximierung des Datenmodells geführt.

Das Fehlen einer überzeugenden Analyse ist ursächlich dafür, daß zur Erforderlichkeit der Daten, Zugriffsberechtigungen und Funktionen eine Vielzahl von Fragen zu stellen war. Die Antworten auf diese Fragen konnten aber Zweifel nicht immer ausräumen, ob die Daten, Zugriffsberechtigungen und Funktionen für die Aufgabenerfüllung objektiv erforderlich sind oder nur subjektiv als nützlich angesehen werden. Dies gilt sowohl für die Nutzung des LIV durch die Schulaufsicht als auch für den Umfang der regelmäßigen Übermittlung von anonymisierten Einzeldaten für die Lehrerindividualdatei bei der Senatsverwaltung für Schulwesen, Berufsbildung und Sport.

Ein Teildatenbestand aus dem LIV soll jährlich selektiert und auf Disketten geschrieben werden, die an die Senatsschulverwaltung zur Führung der *Lehrerindividualdatei* übersandt werden. Dabei handelt es sich um eine Datenübermittlung, für die nur dann eine Rechtsgrundlage entbehrlich ist, wenn für den Empfänger ein Personenbezug ausgeschlossen ist, eine ausreichende Anonymisierung also vorliegt. Im Verlaufe der Diskussionen um das Pflichtenheft wurde der zu übermittelnde Datenbestand soweit modifiziert, daß wir die zur Übermittlung vorgesehenen Daten als ausreichend anonymisiert ansehen konnten.

Gerade bei Systemen der Personaldatenverarbeitung sind an die Revisionsfähigkeit besondere Anforderungen zu stellen, da neben den Prüfinteressen des Rechnungshofs und des behördlichen sowie des Berliner Datenschutzbeauftragten ein Interesse der Personalvertretungen an einer Kontrolle der Einhaltung von Dienstvereinbarungen besteht. Das Landesamt für Informationstechnik (LIT) hatte daher einen *Protokollierungsstandard (PROVER)* entwickelt, der generell bei Pflichtenheften für Ausschreibungen zu IuK-Verfahren der Berliner Verwaltung Berücksichtigung finden soll. Dieser Standard findet erstmalig im LIV Anwendung. Er sieht u.a. vor, daß die Auswertung der Protokolldateien nur unter Verwendung von zwei Paßwörtern, also nach dem Vier-Augen-Prinzip, möglich sein soll. Die Zuteilung der beiden Paßwörter für den Zugriff auf die Protokolle wird den Bezirksämtern als den Anwendern überlassen. Von der Projektgruppe wurde dem Wunsch der Personalräte nach einer Empfehlung entsprochen, daß neben dem Protokoll-Auswerter der Verwaltung ein Vertreter des Lehrerpersonalrats über ein Paßwort verfügen soll. Aufgrund unserer Vorbehalte, daß die zu Datenschutzzwecken erfolgende Auswertung der Protokolldateien eigentlich dem behördlichen Datenschutzbeauftragten des jeweiligen Bezirksamtes zukommen sollte, wurde zugesichert, daß die Kontrollmöglichkeiten für den behördlichen Datenschutzbeauftragten und den Berliner Datenschutzbeauftragten uneingeschränkt bleiben würden.

4.9 Soziales

Zum Spannungsverhältnis zwischen Sozialverwaltung und Datenschutz

Private Leistungsträger fragten uns, ob es zulässig sei, daß bei drohendem Wohnungsverlust Mieterdaten aus der bezirklichen Verwaltung an Beratungseinrichtungen der freien Wohlfahrtspflege übermittelt werden dürfen. Die Erfahrungen hätten gezeigt, daß sich gerade ehemalige DDR-Bürger und -Bürgerinnen, aber auch andere Menschen, die sich in einer persönlichen Krise befinden, über die negativen Folgen der Wohnungslosigkeit nicht bewußt sind und den drohenden Wohnungsverlust als scheinbar unveränderliche Tatsache hinnehmen. Die „aufsuchende Sozialarbeit" sei gegenüber diesen Menschen unumgänglich. In Hausbesuchen könnten Unterstützungsmöglichkeiten aufgezeigt und persönliche Beratung angeboten werden, Ängste über Behördenkontakte und Scham könnten abgebaut werden. Deshalb sei die Übermittlung von Mieterdaten notwendig, ohne daß die Zustimmung der Mieter vorausgesetzt werden könne. Es handele sich hier um einen Fall der Rechtsgüterabwägung zwischen dem informationellen Selbstbestimmungsrecht und der drohenden Wohnungslosigkeit.

Nach § 20 Sozialgesetzbuch X (SGB X) haben die Behörden einen Leistungssachverhalt auch von Amts wegen zu ermitteln. Sie bestimmen Art und Umfang der Ermittlungen. Ferner ist nach § 17 Abs. 1 SGB I darauf hinzuwirken, daß jeder Berechtigte die ihm zustehenden Sozialleistungen in zeitgemäßer Weise umfassend und schnell erhält. Bei einer Person, bei der von einer Fähigkeit zur Selbsthilfe und Mitwirkung (§ 60 SGB I) nicht mehr ausgegangen werden kann, müssen daher die notwendigen Hilfsmaßnahmen von Amts wegen eingeleitet werden. Dies kann gemäß § 69 SGB X auch zur Übermittlung der erforderlichen

Daten an Dritte führen, die dann eine entsprechende Hilfe gewähren. Dabei ist jedoch immer der Grundsatz der Verhältnismäßigkeit zu beachten und die Offenbarung auf das unerläßliche Minimum zu reduzieren.

Das Problem des knappen Geldes führte bei einer Berliner Krankenkasse zu folgendem Datenschutzproblem: Sie richtete nämlich an die Hochschule der Künste (HdK) Auskunftsersuchen und bat um Mitteilung der Immatrikulationszeiten von Studenten.

In gewissem Umfang werden auch Sozialdaten versicherter Studenten übermittelt. Die HdK unterliegt nicht dem Sozialgesetzbuch, vielmehr ist auf sie das Berliner Hochschulgesetz anzuwenden, welches seit dem 31. Januar 1993 eine bereichsspezifische Befugnis zur Verarbeitung, also auch Übermittlung von Studentendaten enthält. Eine Befugnis zur Übermittlung solcher Daten an Krankenkassen erlaubt diese Vorschrift jedoch nicht; auch die Einwilligung der Betroffenen lag nicht vor. Eine Krankenversicherung darf zwar nach § 284 Abs. 1 SGB V personenbeziehbare Daten für Zwecke der Krankenversicherung erheben und erfassen, soweit diese für die Feststellung des Versicherungsverhältnisses (§§ 5 bis 10 SGB V) und der Mitgliedschaft (§§ 186 bis 193 SGB V) erforderlich sind. Diese Erhebungsbefugnis läßt sich jedoch nicht in die Übermittlungsbefugnis einer anderen öffentlichen Körperschaft uminterpretieren.

Maßgeblich sind vielmehr die Vorschriften des Sozialgesetzbuchs, die im Verhältnis zum Versicherungsträger in § 206 SGB V eine Auskunfts- und Mitteilungspflicht des Versicherten selbst vorsehen.

Wer versichert ist oder als Versicherter in Betracht kommt, hat, soweit er nicht nach § 280 SGB IV auskunftspflichtig ist, der Krankenkasse alle erforderlichen Daten zur Feststellung des Versicherungsverhältnisses und der Beitragspflicht und etwaiger Änderungen der Verhältnisse mitzuteilen. Entstehen der Krankenkasse durch eine Verletzung dieser Pflichten (§ 206 Abs. 1 SGB V) zusätzliche Aufwendungen, kann sie von den Verpflichteten deren Erstattung verlangen (§ 206 Abs. 2 SGB V). Aus dieser eindeutigen Regelung der Datenquellen, derer sich die Krankenkasse bedienen darf, geht hervor, daß nur der Versicherte selbst hinsichtlich seiner personenbezogenen Daten in Anspruch genommen werden darf. Die Abfrage bei der HdK war datenschutzrechtlich somit unzulässig. Der Versicherungsträger hat sich unserer Auffassung angeschlossen.

Berliner Automatisiertes Sozialhilfe-Interaktions-System (BASIS)

Das Projekt BASIS zur Automationsunterstützung der Sachbearbeitung bei der Gewährung von Sozialhilfe und wirtschaftlicher Hilfe für Jugendliche, über das wir bereits in früheren Jahresberichten berichtet hatten, ist weiter mit Nachdruck vorangetrieben worden. In verschiedenen Erprobungsbezirksämtern sind zum Jahresende die Hardware-Installationen erfolgt, im Modellbezirksamt Weißensee wird das Verfahren bereits im Echteinsatz erprobt.

Eine Untergruppe der BASIS-Projektgruppe befaßt sich mit der Entwicklung eines Datenschutz- und Datensicherheitskonzeptes für BASIS, das sich allerdings bisher nur mit den lokalen Bedingungen in den Bezirksämtern befaßt und den geplanten bezirksübergreifenden Datenverkehr ebenso nicht in Betracht zieht wie die geplante Fernadministration durch das Landesamt für Informationstechnik. Eine abschließende Bewertung des Datenschutz- und Datensicherheitskonzeptes für BASIS ist noch nicht möglich.

Zu dem fertiggestellten Hauptuntersuchungsbericht für BASIS konnte jedoch eine Stellungnahme abgegeben werden.

Dabei ging es aus rechtlicher Sicht insbesondere um die Zulässigkeit der verschiedenen Datenübermittlungen zwischen den Bezirksämtern untereinander und der Bezirksämter mit anderen Behörden:

Der Datenaustausch zwischen den Bezirksämtern und der *Zentralen Sozialhilfestelle (ZSA)* mit dem LIT zur Durchführung zentraler Aufgaben (z.B. für die Zahlbarmachung und die zentrale Datensicherung) soll auch den zentralen Datenabgleich zur Aufdeckung des mehrfachen und damit unter Umständen betrügerischen Sozialhilfebezuges umfassen, der bereits in der Vergangenheit im Zentrum der datenschutzrechtlichen Debatten um BASIS stand.

Das LIT tritt bei dem Datenaustausch als Auftragnehmer für die Datenverarbeitung im Sinne von § 80 SGB X auf. Die Bereitstellung und damit die Offenbarung der Daten an das LIT zu Zwecken der Auftragsdatenverarbeitung ist durch § 69 Abs. 1 Nr. 2 SGB X gedeckt. Auftraggeber für die zentrale Datenverarbeitung durch das LIT sind die Abteilungen für Sozialwesen und für Jugend und Sport der Bezirksämter, da den Bezirken nach dem Allgemeinen Zuständigkeitsgesetz die Durchführung der Aufgaben der Sozial- und Jugendhilfe als bezirkseigene Aufgaben obliegt. Die Zahlbarmachung und zentrale Datensicherung durch das LIT bedarf keiner Verquickung der zumindest logisch zu trennenden Daten der verschiedenen speichernden Stellen. Eine Datenübermittlung im Sinne von § 3 Abs. 5 Nr. 3 BDSG ist dabei nicht erforderlich und findet auch nicht statt.

Anders ist es im Fall des zentralen Abgleichs. Bei diesem Abgleich werden im Einzelfall personenbezogene Daten durch eine speichernde Stelle eingegeben und mit den Daten der anderen speichernden Stellen abgeglichen. Bei diesem Abgleich handelt es sich um einen automatisierten Abgleich im Sinne der Neufassung des § 117 BSHG.

Die Prüfung, ob § 117 BSHG als Rechtsgrundlage für den Abgleich herangezogen werden kann, ergab, daß dies ohne eine Änderung Berliner Landesrechts nicht zutrifft.

§ 117 Abs. 2 BSHG ermächtigt die Träger der Sozialhilfe untereinander zu dem dort beschriebenen Abgleich. Nach § 1 des Ausführungsgesetzes zum BSHG (AGBSHG) ist das Land Berlin Träger der Sozialhilfe, nicht jedoch die Bezirksämter. Allerdings sind - wie schon erwähnt - die Bezirksämter nach dem allgemeinen Zuständigkeitsgesetz Berlin mit der Durchführung der Sozial- und Jugendhilfe als bezirkseigene Angelegenheit betraut. Damit sind die Bezirke speichernde Stellen im Sinne von § 3 Abs. 5 Nr. 8 BDSG bzw. die Organisationseinheiten der Bezirke, denen Aufgaben nach dem BSHG zugewiesen sind (§ 4 Abs. 3 Ziff. 1 BlnDSG). Datenübermittlungen - und dazu zählen auch die Datenabgleiche - bedürfen daher einer Rechtsgrundlage. Da die Bezirke also keine Träger der Sozialhilfe sind, kann § 117 Abs. 2 BSHG nicht als Rechtsgrundlage für den Datenabgleich angesehen werden.

Dieses Ergebnis wird auch von uns als unbefriedigend angesehen, denn es ist nicht erkennbar, daß ein Datenabgleich mit anderen Kommunen möglich sein soll, aber innerhalb der Berliner Bezirke nicht. Diese Situation sollte durch eine geeignete Änderung des Landesrechts verändert werden; wir empfehlen, § 1 Ausführungsgesetz zum Bundessozialhilfegesetz durch eine Vorschrift zu ergänzen, die die Bezirke in Bezug auf den automatisierten Datenabgleich den Trägern der Sozialhilfe nach § 117 BSHG gleichstellt.

Der *Datenaustausch zwischen dem Landeseinwohneramt Berlin (LEA) und den Bezirksämtern* dient lediglich der Prüfung der Zuständigkeit des jeweiligen Bezirksamtes. Eine Prüfung auf mögliche Doppelbeantragungen durch Kontrolle der Meldeverhältnisse erfolgt auf diesem Weg nicht, da dies mit dem oben beschriebenen Datenabgleich nach § 117 BSHG erfolgen soll.

Da eine Überprüfung der Zuständigkeit auch durch Vorlage des Personalausweises erreicht werden kann und nur in vereinzelten Zweifelsfällen eine Auskunft aus dem LEA erforderlich ist, halten wir die Einrichtung eines automatisierten Abrufverfahrens an das Melderegister und damit die Aufnahme der bezirklichen Sozial- und Jugendämter in die Anlage 5 zu § 3 Nr. 2 DVO-Meldegesetz für unverhältnismäßig.

Gegen die *Einbeziehung der Ämter VIII der Abteilung Jugend und Sport der Bezirke* in das Verfahren BASIS bestehen keine Bedenken, sofern die oben beschriebene Gesetzesanpassung für die Anwendbarkeit des § 117 BSHG in Berlin realisiert wird.

Aus *technischer und organisatorischer Sicht* haben wir der Projektgruppe die von uns für nötig gehaltenen differenzierten Anforderungen mitgeteilt und hatten uns darüber hinaus kritisch mit dem Datenschutz- und Datensicherheitskonzept im Hauptuntersuchungsbericht auseinanderzusetzen.

Positiv war zu würdigen, daß

- bei der Planung der gebäudeinternen Kommunikation die Option freigehalten wird, für BASIS ein eigenes virtuelles Netz realisieren zu können. Es wird erkannt, daß eine Trennung des BASIS-Verfahrens von anderen Großverfahren der Bezirke einfach realisierbar sein muß;
- eine Datenverschlüsselung bei der Datenübermittlung im berlinweiten Verwaltungsnetz über sogenannte „black boxes" und beim Datenträgeraustausch mittels geeigneter Software erfolgen soll;
- die Client-APC ohne Diskettenlaufwerk oder mit Diskettenlaufwerk mit mechanischem Schließsystem ausgestattet sein sollen;
- das UNIX-System höheren amtlichen Sicherheitskriterien genügen soll, als normale UNIX-Derivate erfüllen können.

Zu kritisieren war, daß die Paßwortverwaltung durch den Projektkoordinator erst in einer späteren BASIS-Version durch die Paßwortverwaltung durch die Anwender selbst abgelöst werden sollte. Wir haben empfohlen, daß dies mit Beginn des Echtbetriebes realisiert sein sollte. Eine Paßwortverwaltung durch Dritte stellt die Verbindlichkeit der an die Person der Anwender gebundenen Sicherheits- und Kontrollverfahren grundsätzlich in Frage. Da im übrigen die Paßwortverwaltung durch die Anwender mittlerweile von fast allen Systemen ermöglicht wird, wäre BASIS insoweit nicht auf dem Stand der Technik.

Im Zusammenhang mit der Konzeption des Datenschutz- und Datensicherheitskonzeptes wurde eine Risikoabschätzung durchgeführt, die leider zu unrealistischen Ergebnissen geführt hat, weil die Annahmen über die Eintrittswahrscheinlichkeit von Schadensereignissen von subjektiven Einschätzungen bestimmt waren, die weniger von Sicherheitsaspekten als von finanziellen Erwägungen geprägt waren. Die Risikoanalyse lief damit Gefahr, weniger zur Erarbeitung eines guten IT-Sicherheitskonzeptes zu dienen als als Argumentationshilfe für ein billiges und entsprechend schwaches Konzept.

Wir hätten es begrüßt, wenn der Hauptuntersuchungsbericht ein vollständiges technisches und organisatorisches Datenschutzkonzept enthalten hätte, das die Umsetzung der Anforderungen der §§ 9 und 18 BDSG zusammenfassend beschreibt.

In der Zwischenbilanz des extern gewonnenen Managements im Hauptuntersuchungsbericht erfolgt die Aussage, daß es nicht angehen könne, „daß im BASIS-Projekt ein detailliertes Datenschutzkonzept für die Bezirke erarbeitet wird, das dann möglicherweise mit den konzeptionellen Vorstellungen anderer Großverfahren kollidiert". Diese Aussage interpretieren wir so, daß auf ein detailliertes Datenschutzkonzept für BASIS verzichtet werden soll, bis „ein gemeinsames Dach für die Berliner Großverfahren" entstanden ist. Die vermutete Kollision ist jedoch nicht erkennbar. Ein detailliertes Datenschutzkonzept für den Einsatz von BASIS muß mit Beginn des Echteinsatzes im Modellbezirksamt Weißensee in die Praxis umgesetzt worden sein, wenn den gesetzlichen Vorgaben der §§ 9 und 18 BDSG Genüge getan werden soll. Ein solches Datenschutzkonzept für BASIS steht vergleichbaren Konzepten für andere Großverfahren nicht entgegen. Jedes Datenschutzkonzept baut auf den spezifischen Rahmenbedingungen eines Projektes auf, die sich aus der Art und der Schutzbedürftigkeit der dabei zu verarbeitenden personenbezogenen Daten, der Ausprägung der vorgesehenen Phasen der Datenverarbeitung gem. § 3 Abs. 5 BDSG und der eingesetzten Technik ergeben. Diesem verfahrenbezogenen Datenschutzkonzept steht die Entwicklung eines „Dachkonzeptes" für den Datenschutz in einem Bezirksamt im Rahmen eines „gemeinsamen Daches" der bezirklichen Großverfahren nicht entgegen. Hierbei handelt es sich im wesentlichen um organisatorische Regelungen, um das Setzen von Standards aber auch um Bewußtseinsbildung, daß Datenschutz und IT-Sicherheit und die daraus resultierenden Maßnahmen notwendige Bestandteile einer jeden ADV-Anwendung sind, deren Resultate in rechtmäßige und verbindliche Verwaltungsentscheidungen für oder über den Bürger umgesetzt werden sollen und deren Daten vor Mißbrauch für gesetzlich nicht gebilligte Ziele oder vor dem Zugriff Unbefugter geschützt werden müssen.

4.10 Stadtentwicklung und Umweltschutz

Gesetzgebung

Bereits im Jahresbericht 1992 wurde geschildert, daß der Bundesgesetzgeber in der Pflicht stand, bis zum 31. Dezember 1992 die EG-Richtlinie über den freien Zugang zu Informationen über die Umwelt in deutsches Recht umzusetzen. Erst im November 1993 hat die Bundesregierung einen Gesetzentwurf beschlossen. In diesem Gesetzentwurf sind Regelungen sowohl hinsichtlich des freien Zugangs zu Informationen über die Umwelt als auch zum Schutz privater Belange vorgesehen[102]. Zuvor war von der Gruppe Bündnis 90/Die Grünen ein Gesetzentwurf im Bundestag eingebracht worden, der - im Unterschied zum Entwurf der Bundesregierung - sowohl den Schutz von personenbezogenen Daten sowie von Geschäfts- und Betriebsgeheimnissen als auch Ausschluß- und Beschränkungsgründe dieses Anspruches präziser regelt[103]. Dies trifft auch auf die Regelungen hinsichtlich der Antragstellung und der Form der Einsicht in Unterlagen zu.

Der Gesetzentwurf der Bundesregierung weist erhebliche Defizite auf:

Fraglich ist, in welchem Verfahren über die Ablehnung von Informationsbegehren zu entscheiden ist. Der Entwurf der Gruppe Bündnis 90/Die Grünen sieht hierfür die Funktion eines Bundesbeauftragten für Informationsfreiheit vor. Auch werden nach diesem Entwurf die Länder ermächtigt, gesetzliche Vorschriften für die Einrichtung und Aufgaben eines Landesbeauftragten für Informationsfreiheit zu regeln. Der in der letzten Legislaturperiode in Berlin beratene Entwurf eines Informationsfreiheitsgesetzes sah ebenso wie das nunmehr in Vorbereitung befindliche Hessische Gesetz über den freien Zugang zu Informationen über die Umwelt vor, dem Landesdatenschutzbeauftragten diese Aufgabe zu übertragen. Das Bundesgesetz will dies offenbar den Verwaltungsgerichten überlassen.

Zum Abschluß gebracht wurden die Arbeiten an einem Entwurf für ein *Gesetz über die Datenverarbeitung für Zwecke der räumlichen Stadtentwicklung, Stadt- und Regionalplanung, bodenwirtschaftliche Aufgaben (Stadtplanungsdatenverarbeitungsgesetz).* Der dem Abgeordnetenhaus vorliegende Gesetzentwurf berücksichtigt unsere Hinweise. Ein umfangreicher und detaillierter Datenkatalog ist Bestandteil des Gesetzes. Klar geregelt werden soll, welche Senatsverwaltung für welchen Teil der Daten zuständig ist und wo die Verantwortung der Bezirke liegt. Daten, die einen unmittelbaren Personenbezug erlauben - wie beispielsweise Name und Anschrift von Eigentümern - sind in besonders geschützten Teilen der Stadtplanungsdateien zu halten. Auch läßt der Gesetzentwurf die Einrichtung eines automatisierten Abrufverfahrens, das im Detail durch Rechtsverordnung zu regeln ist, zu.

Der Entwurf eines *Bodenschutzgesetzes* ist dagegen bisher nicht in das Abgeordnetenhaus eingebracht worden. Bis zur Verabschiedung dürfen Datenerhebungen nur auf die Einwilligung der Betroffenen gestützt werden, soweit nicht anderweitige Regelungen - wie im Berliner Wassergesetz - greifen. Auch zur Durchführung der *Wassergesetze* sowie für *Maßnahmen der Gewässeraufsicht und -überwachung* ist die Erhebung personenbezogener Daten erforderlich. Mit der 8. Änderung des Berliner Wassergesetzes ist vorgesehen, die Wasserbehörde zu ermächtigen, für diese Zwecke personenbezogene Daten zu erheben und zu verarbeiten. Der vorliegende Entwurf berücksichtigt unsere Hinweise.

Kleingärtner im Datenschleppnetz?

Im Frühjahr 1993 wurde den Kleingärtnern eines Bezirksverbandes ein Erhebungsbogen des zuständigen Bezirksamtes übergeben. Mit diesem Formular sollen jährlich Meldungen an die Senatsverwaltung für Stadtentwicklung und Umweltschutz nach einer Allgemeinen Anweisung aus dem Jahr 1987 erfolgen. Ferner

102 BR-Drs. 797/93
103 BT-Drs. 12/5696

sollten die Unterlagen bei Pächterwechsel oder Bauanträgen fortgeschrieben werden. Offensichtlich handelte es sich zum einen um eine Statistik, zum anderen um eine parzellenbezogene Fortschreibung. Gefragt wurde u.a. nach Laubengröße, Nebengebäuden, Terrassen, Wegen, Spielflächen und Abwasserentsorgung.

Eine statistische Erhebung unterliegt - wenn sie nicht durch Bundesgesetz geregelt ist - den Anforderungen des Landesstatistikgesetzes. Danach sind Landesstatistiken grundsätzlich durch Gesetz anzuordnen. Die Einzelangaben aus Landesstatistiken unterliegen einem Reidentifizierungsverbot. Die Befragten sind schriftlich über die Modalitäten der Landesstatistik zu informieren.

Soll hingegen eine Statistik aus Daten des Verwaltungsvollzuges erstellt werden, müssen die Daten zuvor auf Grundlage einer besonderen Rechtsvorschrift oder der Einwilligung der Betroffenen erhoben werden. Das Bundeskleingartengesetz beinhaltet keine Befugnis zu einer derartigen Datenerhebung. Der Hinweis darauf, daß das Bundeskleingartengesetz bestimmte Grenzwerte der Bebauung, Bepflanzung und Nutzung angibt, genügt nicht für die Legitimation einer Datenerhebung.

Das zuständige Bezirksamt brach nach unserem Hinweis auf die Rechtslage die Erhebung ab und vernichtete die bisher eingegangenen Unterlagen. Die Senatsverwaltung für Stadtentwicklung und Umweltschutz teilte uns mit, daß die Berliner Kleingartenstatistik wie bisher nur auf Grundlage von flächenbezogenen Mitteilungen der Kleingartenverbände, nicht aber durch Einzelbefragungen der Pächter erhoben werden soll. Dieses Verfahren dient als Beleg dafür, daß nicht in jedem Fall zur Erstellung von Statistiken auf personenbezogene Einzelangaben zurückgegriffen werden muß.

Der gläserne Landwirt

Die im Mai 1992 vom EG-Ministerrat beschlossene Reform der Gemeinsamen Agrarpolitik sieht zur Entscheidung über direkte flächen- bzw. tierbezogene Ausgleichszahlungen den Aufbau eines Integrierten Verwaltungs- und Kontrollsystems (InVeKoS) zur Landwirtschaftsförderung vor. Kern dieses Systems ist ein automatisierter Abgleich der Angaben der Landwirte mit *Satelliten- und Luftbildaufnahmen,* die über die aktuelle Größe und Nutzung landwirtschaftlicher Parzellen Auskunft geben. Die Datenschutzbeauftragten des Bundes und der Länder haben sich dafür ausgesprochen, die Fernerkundung nicht für flächendeckende Totalüberwachungen einzusetzen und keine zentrale Erfassung von Daten aller Landwirte zuzulassen[104]. Nach Auffassung der Datenschutzbeauftragten hat die EG mit dem InVeKoS den Landwirtschaftsverwaltungen der Länder ein Überwachungssystem verordnet, das dem Grundsatz der Verhältnismäßigkeit - insbesondere dem Übermaßverbot - widersprechen kann. Die Fernerkundung mittels Satellit oder Flugzeug kann zu einem mindestens ebenso gravierenden Einschnitt in die Persönlichkeitsrechte führen, wie dies mit der vor Jahren beabsichtigten Schaffung eines einheitlichen Personenkennzeichens geplant war. Es besteht die Gefahr, daß technische Entwicklungen in Gang gesetzt werden, deren Spätfolgen nicht abschätzbar sind[105].

4.11 Verkehr und Betriebe

Bewegungsprofile im Straßenverkehr

Aufgrund der angespannten Haushaltslage des Bundes wird öffentlich zunehmend über eine Abwälzung der Unterhaltungskosten für die Autobahnen auf die Benutzer durch Erhebung von *Straßenbenutzungsgebühren* diskutiert. Während Anfang 1994 die Erhebung solcher Gebühren bei LKWs durch eine jährliche Einmal-Zahlung im Voraus eingeführt worden ist, hat der Bundesverkehrsminister die Einführung der *elektronischen Autobahnmaut („road pricing")* auch für PKW-Fahrer in den nächsten Jahren angekündigt. Zwei entsprechende Modellversuche sollen ab 1994 in Baden-Württemberg und Nordrhein-Westfalen durchgeführt werden.

Die konkrete technische Ausgestaltung der Systeme ist zwar gegenwärtig noch nicht bekannt, allen Verfahren ist jedoch gemeinsam, daß sie im Gegensatz zu der pauschal vorab bezahlten Gebühr (Vignettenlösung) die Gebührenberechnung nur für tatsächlich gefahrene Autobahnstrecken vorsehen. Damit wird einerseits eine gerechtere Verteilung der Gebühr erreicht, andererseits sollte schon in diesem frühen Stadium berücksichtigt werden, daß einige der vorgeschlagenen Verfahren das informationelle Selbstbestimmungsrecht der Kraftfahrer beeinträchtigen würden.

So muß von vornherein verhindert werden, daß zur Erhebung von Straßenbenutzungsgebühren eine Infrastruktur geschaffen wird, die es ermöglicht, umfassende *Bewegungsbilder aller Kraftfahrer* zu erstellen. Auch hier[106] ist die Benutzung von Guthabenkarten („prepaid"), von denen beim Passieren einer elektronischen Bake (Mautstelle) am Straßenrand eine bestimmte Gebühr automatisch abgebucht wird, einer Kreditkartenlösung („postpaid") vorzuziehen, weil nur so die Entstehung von Bewegungsprofilen ausgeschlossen ist und eine *„datenfreie Fahrt"* für den Bürger möglich bleibt.

Auch in Berlin hat die Senatsverwaltung für Verkehr und Betriebe im Rahmen des Europäischen Forschungsprogramms DRIVE eine Studie zur „Gezielten Nutzung des Straßenraumes als Teil eines Gesamtverkehrsmanagements" *(LIAISON)* erstellen lassen.

Ziel des Projekts LIAISON ist es, einzelne Fahrspuren im Innenstadtbereich zu bestimmten Zeiten Wirtschaftsfahrzeugen, öffentlichem Nahverkehr und gewerblichem Güterverkehr vorzubehalten. Die Zugangsberechtigung für derartige Sonderfahrspuren soll elektronisch überwacht werden. Die beschrifteten Fahrzeuge sollen mit elektronisch lesbaren Ausweisen oder mit einer Bordeinrichtung, die mit Baken am Straßenrand über Funk kommuniziert, ausgestattet werden.

Es wird zwar angestrebt, ausschließlich Daten solcher Fahrzeuge festzuhalten, die ohne Zugangsberechtigung die Sonderfahrspuren nutzen. Wie die Identifizierung der nicht-berechtigten Fahrzeuge erfolgen soll (mit Hilfe von Kameras wie bei der Rotlicht-Überwachung oder durch den Einsatz von Videokameras), ist noch nicht entschieden.

Datenschutzgerecht sind allenfalls solche Lösungen, bei denen gewährleistet ist, daß die Überwachungssysteme ausschließlich solche Fahrzeuge erfassen und registrieren können, die ohne entsprechende Zugangsberechtigung die Vorzugsspur benutzen. Die Verkehrsteilnehmer müssen schon in einer möglichen Versuchsphase in geeigneter Weise und *vor* Nutzung der Vorzugsspur darüber aufgeklärt werden, welche Daten zu welchem Zweck über sie erhoben und gespeichert werden.

Neues zum Führerschein

Am 1. Juli 1996 tritt die zweite EG-Richtlinie über den Führerschein[107] vom 29. Juli 1991 in Kraft. Diese Richtlinie dient der Vereinheitlichung der Klasseneinteilung und der Voraussetzungen für die Fahrerlaubniserteilung und regelt die Einführung eines einzelstaatlichen Führerscheins nach EU-Muster unter gegenseitiger Anerkennung durch die Mitgliedstaaten.

Das Bundesministerium für Verkehr hat in einem Referentenentwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze die Einrichtung eines *bundesweiten Fahrerlaubnisregisters* vorgesehen, um den Informationsaustausch zwischen den Mitgliedstaaten der EU effizienter zu gestalten. Aus datenschutzrechtlicher Sicht ist gegenüber diesem Projekt Skepsis angebracht: Damit würde eine zentrale Datei geschaffen, in der beinahe alle erwachsenen Bürger erfaßt sind, ohne daß die Notwendigkeit bisher überzeugend dargelegt wurde. Mit den heutigen Instrumentarien - z. B. über das Verkehrszentralregister oder einer Anfrage bei der örtlichen Führerscheinstelle - sind Verstöße feststellbar und ist auch ein gegenseitiger Informationsaustausch möglich.

104 siehe Anlage 2.8
105 vgl. auch Jahresbericht 1992, 5.3, Anlage 3

106 vgl. auch oben 2.3
107 91/439 EWG

Schon seit Jahren laufen Planungen, anstelle der bisherig manuell geführten Führerscheinkartei eine *automatisierte Führerscheindatei* einzurichten[108]. Das bereits geklärte Verfahren zur Ersterfassung der Daten, nämlich die unmittelbare Erfassung aus der manuellen Führerscheinkartei, wurde vom Landeseinwohneramt wegen des damit verbundenen zeitlichen und personellen Aufwandes erneut in Frage gestellt. Es wurde vorgeschlagen, die Grunddaten aller Berliner Einwohner ab 16 Jahren aus dem Melderegister zu übermitteln. Nach Abgleich mit den ca. 2,2 Mio. Karteikarten aus dem Führerscheinregister sollte bei Übereinstimmungen der Datensatz aus dem Melderegister übernommen werden. Gegen dieses Verfahren bestanden Bedenken, da das Meldegesetz eine Übermittlung und einen Abgleich dieser - nicht nur Führerscheininhaber betreffenden Daten - nicht zuläßt. Zudem ist zweifelhaft, ob dieser einmalige Datenabgleich für das erstrebte Ziel geeignet ist[109].

Das Landeseinwohneramt hat von diesen Planungen wieder Abstand genommen und beabsichtigt nun, die Datenerfassung wieder unmittelbar aus den Karteikarten vorzunehmen. Dies soll durch ein privates Unternehmen erfolgen. Nach der Automatisierung wird das Landeseinwohneramt ein neues Konzept für einen Datenabgleich mit dem Datenbestand des Melderegisters zur Berichtigung falsch eingegebener Personalien vorlegen.

Im Jahresbericht 1992[110] hatten wir über die Praxis des Landeseinwohneramtes berichtet, *medizinisch-psychologische Gutachten* unverschlossen zu den Akten zu nehmen.

Die Senatsverwaltung für Inneres ist unserer Empfehlung gefolgt und hat im Juni 1993 das Landeseinwohneramt angewiesen, diese erheblich in das Persönlichkeitsrecht eingreifenden Unterlagen in den Fahrerlaubnisakten künftig in verschlossenen Umschlägen aufzubewahren[111].

Das Landeseinwohneramt hat uns hierzu nach sieben Monaten mitgeteilt, daß hier noch „Einzelheiten und Verfahrensregelungen zu gestalten" seien. Wir gehen davon aus, daß dies nunmehr erfolgt ist und die Anweisung der Senatsverwaltung für Inneres umgesetzt wurde.

Neue Rechtsgrundlagen für die Datenverarbeitung der bisherigen Eigenbetriebe

Mit dem Artikelgesetz vom Januar 1993 war auch die Verarbeitung personenbezogener Daten bei den damaligen Eigenbetrieben erstmals auf eine eigene Rechtsgrundlage gestellt worden. Diese ist in das am 1. Januar 1994 in Kraft getretene *Berliner Betriebe-Gesetz (BerlBG)*[112] übernommen worden. Sie bedarf allerdings noch der Ergänzung durch eine entsprechende Rechtsverordnung, die gegenwärtig erarbeitet wird.

Weitere datenschutzrechtliche Fragen, die insbesondere bei der BVG auftraten, sind an anderer Stelle bereits erörtert worden[113].

4.12 Wissenschaft und Forschung

Gesetzgebung

Durch den Erlaß der Verordnung zur Erhebung und Verarbeitung personenbezogener Daten der Studienbewerber, Studenten und Prüfungskandidaten für Verwaltungszwecke der Hochschulen *(Studentendatenverordnung - StudDatVO -)*[114] aufgrund des geänderten Hochschulgesetzes ist mit Wirkung vom 1. Januar 1994 für den betroffenen Personenkreis erstmals größere Transparenz und Klarheit darüber hergestellt worden, welche Daten die Hochschulen verarbeiten dürfen. Die für bestimmte Zwecke (z. B. Zulassung, Immatrikulation, Rückmeldung, Beurlaubung) erforderlichen Daten der Studienbewerber, Studenten und Prüfungskandidaten werden in der Rechtsverordnung im Einzelnen benannt. Die Senatsverwaltung für Wissenschaft und Forschung hat bei der Erarbeitung der Verordnung unsere Empfehlungen berücksichtigt.

Dagegen bleibt die Verarbeitung der Personaldaten an allen Berliner Hochschulen weiterhin ungeregelt. Die Wissenschaftsverwaltung hat insofern auf die noch ausstehende Änderung des Landesbeamtenrechts[115] verwiesen, die allerdings nicht die speziellen Probleme des Personaldatenschutzes an den Hochschulen mit ihren zahlreichen Gremien (Kuratorien, Personalkommissionen, Fachbereiche usw.) lösen wird. Eine entsprechende Ergänzung des Hochschulgesetzes wird also spätestens nach der Änderung des Landesbeamtengesetzes unausweichlich sein.

Ungeregelt ist auch nach dem Inkrafttreten der Studentendatenverordnung die Verarbeitung von Studentendaten im Zusammenhang mit Leistungsbewertungen und Prüfungen. Dies durch Rechtsvorschriften klar zu regeln (soweit noch nicht geschehen), ist in erster Linie Sache der Hochschulen, die die Prüfungsordnungen erlassen.

An den drei größten Berliner Hochschulen sind *behördliche Datenschutzbeauftragte* bestellt worden, mit denen wir - wie auch mit allen anderen behördlichen Datenschutzbeauftragten - eng zusammenarbeiten. Gerade an den Berliner Hochschulen werden in besonders großem Umfang personenbezogene Daten sensibelster Art (z. B. Patientendaten in den Universitätsklinika, Personaldaten, personenbezogene Daten aus Forschungsprojekten) verarbeitet, deren Kontrolle eine vordringliche Aufgabe ist. Sie kann nur erfüllt werden, wenn in erster Linie die Leitung der jeweiligen Hochschule ihrer Verantwortung für den Datenschutz im eigenen Zuständigkeitsbereich gerecht wird.

Suche nach arbeitslosen Doktoranden

Mitarbeitern eines Berliner Arbeitsamtes war zu Ohren gekommen, daß ausgeschiedene wissenschaftliche Mitarbeiter die Zeit ihrer Arbeitslosigkeit nutzen, um an der Universität ihre Promotion weiterzubetreiben. Sie verlangten daher von der Universität Einsicht in die Personalliste ausgeschiedener wissenschaftlicher Mitarbeiter. Das Arbeitsamt war der Auffassung, daß Promovenden nicht gleichzeitig dem Arbeitsmarkt zur Verfügung stehen könnten.

Weder das Arbeitsförderungsgesetz noch das Berliner Hochschulgesetz enthalten Befugnisse zu einer derartigen Datenerhebung und -übermittlung. Die Listen von ehemaligen Mitarbeitern der Universität sind als gesperrt zu betrachten. Sie dürfen ohne Einwilligung der Betroffenen nicht genutzt werden. Soweit möglicherweise Straf- oder Bußgeldverfahren gegen ehemalige Mitarbeiter eingeleitet worden sind, kann allerdings eine Auskunft gegenüber der Verwaltungsbehörde bzw. dem Gericht *im Einzelfall* zulässig sein. Die Einsichtnahme in Listen von Personen, die ganz überwiegend keine Leistungen vom Arbeitsamt erhalten haben, ist dagegen rechtswidrig. Die Universität hat deshalb die Herausgabe der Liste zu Recht abgelehnt.

Zwang zur wiederholten Begründung der Namensänderung?

Ein Bürger hatte aus schwerwiegenden familiären Gründen beantragt, seinen Familiennamen ändern zu dürfen. Diesem Antrag wurde durch die zuständige Senatsinnenverwaltung stattgegeben. Diese Namensänderung hat zur Folge, daß der Bürger verpflichtet wird, einer Reihe von Behörden die Änderung mitzuteilen und entsprechende Änderungen in seinen Dokumenten vornehmen zu lassen. Bewirbt sich nun dieser Bürger beispielsweise bei einem neuen Arbeitgeber, so tut er dies unter seinem neuen Namen. Sein Diplomzeugnis weist aber noch seinen alten Namen

108 Jahresbericht 1988, 4.9
109 siehe Jahresbericht 1988, 4.9
110 4.2.4
111 Stellungnahme des Senats zu unserem Jahresbericht 1992, Drs. 12/3081 (neu), S. 55
112 GVBl. 1993, S. 319
113 3.2
114 GVBl. 1993, S. 628 f.
115 vgl. oben 4.5.5

aus. Also wird sein künftiger Arbeitgeber ihn fragen, ob dieses überhaupt sein Diplomzeugnis sei und warum er die Namensänderung habe vornehmen lassen. Um sich solchen Fragen nicht auszusetzen, beantragte nun der Bürger bei der Hochschule die Neuausstellung seines Zeugnisses. Dies wurde ihm verweigert, wenn er nicht auch dort die besonderen Gründe nachreicht, die eine Neuausstellung rechtfertigen würden.

Eine Änderung von Familien- oder Vornamen darf nur auf Grundlage des Namensänderungsgesetzes vorgenommen werden, wenn ein wichtiger Grund eine Änderung rechtfertigt. Das Bundesverwaltunsgericht hat in mehreren Entscheidungen dargelegt, wann diese Voraussetzungen gegeben sind. Der Name eines Menschen wird vom allgemeinen Persönlichkeitsrecht umfaßt. Er dient nicht nur als Unterscheidungs- und Zuordnungsmerkmal, sondern ist darüber hinaus Ausdruck der Identität und Individualität.

Nach der Änderung kann der Bürger verlangen, daß die Rechtsordnung seinen neuen Namen respektiert und schützt. Neben den Mitteilungen und Behördengängen nach der Namensänderung, zu denen der einzelne verpflichtet ist, kann - wie im hier geschilderten Fall - jedoch auch nachträglich die Neuausstellung von anderen Dokumenten erforderlich sein. Die Initiative in diesen Fällen geht vom Betroffenen aus. Der Grund der Namensänderung ist anerkannt, sonst wäre dem Antrag auf Namensänderung nicht stattgegeben worden. Damit ist aber auch eine nochmalige Begründung der Namensänderung nicht erforderlich. Hinreichend ist, daß der Betroffene ein besonderes Interesse glaubhaft macht. Die Hochschule folgte schließlich unserer Argumentation.

Datenschutz bei Forschungsvorhaben und Befragungen

Auch im vergangenen Jahr wandten sich wiederum eine Reihe von Forschern an den Berliner Datenschutzbeauftragten und baten um datenschutzrechtliche Beratung und Begleitung ihrer *Forschungsvorhaben.*

So war es für einige Forschungsvorhaben erforderlich, Daten aus sensibelsten Bereichen der Bürger zu erheben. Dies kann generell nur mit Einwilligung der Betroffenen geschehen. Wir haben die Wissenschaftler beraten und insbesondere verlangt, daß Hilfsmerkmale wie Namen und Adressen frühzeitig von den Erhebungsmerkmalen getrennt und die Daten schrittweise anonymisiert werden. So wurden für die Forschungsvorhaben im Rahmen des *Berliner Forschungsverbundes „Public Health"* zwölf Projekte unmittelbar durch uns datenschutzrechtlich begleitet.

Besonders problematisch sind Forschungsvorhaben, die sich nicht auf die Einwilligung der Betroffenen stützen können. Auch wenn die Voraussetzungen für eine Anwendung der Wissenschaftsklausel nach § 30 BlnDSG vorliegen, ist zu prüfen, ob der dann erfolgende Eingriff in das informationelle Selbstbestimmungsrecht ohne Kenntnis des Betroffenen das mildeste Mittel darstellt. Es zeigte sich auch hier, daß es häufig möglich ist, die Datenerhebungen bereits beim Erfassen der Primärdaten einer weitgehenden Anonymisierung zu unterziehen. Derartige Forschungsprojekte unterlagen unserer verstärkten Kontrolle vor Ort.

Inhaltliche Schwerpunkte der Forschungsvorhaben, zu denen wir Empfehlungen gegeben haben, waren der Gesundheits- und der Schulbereich. Aber auch in anderen Bereichen werden personenbezogene Daten für Forschungszwecke erhoben, wie die folgende Übersicht von Forschungsprojekten und Befragungen verdeutlicht, bei denen datenschutzrechtliche Fragen auftraten:

- Wirkungsweise sozialpsychiatrischer Dienste in Ost- und West-Berlin;
- Schwangerenbefragungen hinsichtlich der psychosozialen Gefahren sowie der Wirksamkeit von gesundheitsfördernden und medizinischen Maßnahmen in der Schwangerschaft;
- Entwicklung von Frühgeborenen im Vorschulalter;
- Wirkung von ärztlich initiierten Schulungsprogrammen und von Selbsthilfegruppen bei der Bewältigung chronischer Krankheit im Kindesalter sowie zum Leben mit Krankheit und Behinderung im Kindesalter;
- Befragung zur Folge von Zeckenstichen bei Kindern;
- Infektionskrankheiten bei Drogenabhängigen;
- Zum Lebensalltag psychisch Kranker im Ost-West-Vergleich;
- Bürgerbeteiligung in der gesundheitsorientierten Stadtentwicklung,
- Befragung von Behinderten zu ihrer Integration;
- Arbeitsplatzuntersuchungen in Krankenhäusern;
- Vergleichende Analyse von onkologischen Schwerpunktpraxen und Geschwulstberatungsstellen;
- Schätzung des Umfangs der Berliner Opiatszene;
- Berliner Schülerstudie und Schuljugend im vereinten Berlin;
- Schülerbefragung zum Sexualverhalten;
- Schülerbefragung zum Leistungsverhalten im Sportunterricht;
- Befragung von Osteoporose-Patienten;
- Befragung von hörbehinderten Kindern und ihrer Eltern;
- Gymnasiastenbefragung im Ost-West-Vergleich;
- Schülerbefragung im Umfeld von Jugendeinrichtungen und zur Wirksamkeit der mobilen Suchtprophylaxe;
- Schülerbefragung zu Kindheit und Jugend in Deutschland vor und nach der Vereinigung,
- Befragung zu aggressionsrelevanten Situationen in Kindertagesstätten;
- Vergleichende Befragung von behinderten Frauen im Ost- und Westteil der Stadt;
- Modellversuch zur Förderung verhaltensgestörter Kinder in Kooperation von Schule- und Jugendhilfe;
- Befragung von Studienanfängern aus den neuen Bundesländern;
- Befragung von Realschülern an Ostberliner Schulen zur Entscheidungsgrundlage für die Kurswahl;
- Absolventenbefragungen an Fachbereichen;
- Befragung zum interkulturellen Vergleich jugendlicher Sportkultur;
- Interviews von Hauptschülern zur Gewaltbereitschaft;
- Schülerbefragung zu Bewältigungsstrategien bei Streß und Ärger;
- Evaluationsstudie - 10 Jahre „Hilfe zur Arbeit" in Berlin (West);
- Telefonische Ausländerumfrage;
- Befragung zur Lebenssituation von Vorruheständlern und Beziehern von Altersübergangsgeld;
- Untersuchung zur Wirksamkeit der Frauenförderung;
- Haushaltsbefragung zum Verkehrsverhalten und zur Nutzung des Individual- bzw. öffentlichen Personennahverkehrs;

Positiv zu bewerten ist die Tatsache, daß immer mehr Wissenschaftler sich bereits sehr frühzeitig an uns wenden, denn bei datenschutzgerechter Anlage eines Forschungsprojektes können Probleme häufig von vornherein vermieden werden.

5. Telekommunikation und Medien

Bei der Behandlung von Datenschutzfragen bei Telekommunikation und Medien, die auch im vergangenen Jahr wieder einen Schwerpunkt unserer Tätigkeit bildeten, erweist sich, daß datenschutzgerechte Lösungen heute nicht mehr regional oder national, sondern nur auf europäischer und internationaler Ebene erreicht werden können. Umgekehrt werden europäische Initiativen zur Liberalisierung und Harmonisierung der bestehenden Netze in naher Zukunft starke Auswirkungen im nationalen Bereich haben. Im Auftrag der entsprechenden Koordinierungsgremien haben wir uns deshalb auch im Berichtszeitraum inten-

siv um eine Abstimmung zwischen den Datenschutzbeauftragten auf der Ebene der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und auf europäischer und internationaler Ebene bemüht. Nur durch eine solche Abstimmung besteht eine gewisse Gewähr dafür, daß Gefahren für die Persönlichkeitssphäre frühzeitig erkannt und Konzepte entwickelt werden, um ihnen zu begegnen.

5.1 Berlin

Telekommunikation in öffentlichen Krankenhäusern

In einer Rehabilitationswohngemeinschaft für Jugendliche, die unter einer psychischen Erkrankung leiden, riefen Betreuer nach Telefonaten ihrer Schützlinge deren Gesprächspartner erneut an, um sich nach deren Identität und den Gesprächsinhalten zu erkundigen.

Was den Mißbrauch der Zielnummernspeicherung aus der Telefondatenerfassung einer digitalen Nebenstellenanlage vermuten ließ, war in Wirklichkeit ein Beispiel für die datenschutzrechtliche Relevanz der *Wahlwiederholfunktion* bei noch analogen Nebenstellenanlagen. Dabei wird die zuletzt gewählte Telefonnummer gespeichert. Nach dem Drücken der Wahlwiederholtaste wird diese automatisch angewählt. Genau diese Funktion wurde im beschriebenen Fall zu Kontrollanrufen genutzt.

Eine Umfrage bei den öffentlichen Krankenhäusern zur Technik der Telefonnebenstellenanlagen und dabei insbesondere zur Praxis der *Gebührenabrechnung für Patiententelefone* hat ergeben, daß auch in den Krankenhäusern eine schnelle Ablösung der alten analogen Nebenstellen durch moderne ISDN-fähige digitale Nebenstellenanlagen erfolgt. Mit dieser Umstellung wird die Chance genutzt, die beim Einsatz solcher Anlagen anfallenden Gesprächsdaten für eine detaillierte Abrechnung mit den Patienten zu verwenden.

Während bei den alten Anlagen meist Gesprächseinheitenzähler verwendet werden, die zwar die Gebühreneinheiten patientenbezogen zählen, aber Rückschlüsse auf die Gesprächspartner nicht ermöglichen, wird mit der Umstellung auf digitale Nebenstellenanlagen einer Reihe von Krankenhäusern - aber keineswegs allen - angestrebt, die Zielnummer der Patientengespräche zu erfassen, um einen detaillierten und von den Patienten besser überprüfbaren Einzelgebührennachweis liefern zu können.

In rechtlicher Hinsicht stellt die Situation im Vergleich zur Problematik des Einzelgebührennachweises der TELEKOM an ihre Kunden und zur Gesprächsdatenerfassung zur Abrechnung privater Gespräche von Dienstanschlüssen aus einen Sonderfall dar, denn die dafür geltenden Vorschriften[116] sind nicht unmittelbar auf die von Krankenhäusern an Patienten vermieteten Anschlüsse anwendbar. Krankenhäuser erbringen mit ihren Nebenstellenanlagen keine „Telekommunikationsdienstleistungen für andere" im Sinne des Fernmeldeanlagengesetzes. Anwendbar ist zunächst nur das Landeskrankenhausgesetz in Verbindung mit dem Krankenhausaufnahmevertrag sowie (subsidiär) § 28 BDSG.

Allerdings sind die öffentlichen Krankenhäuser nach § 5 Abs. 4 der Rahmendienstvereinbarung zu digitalen Nebenstellenanlagen[117] daran gehindert, für die Gespräche ihres *Personals* Gebührendaten mit vollständiger Zielnummer in der Nebenstellenanlage zu speichern, da dafür eine gesonderte gesetzliche Regelung fehlt. Da nicht anzunehmen ist, daß in den Krankenhäusern verschiedene Nebenstellenanlagen für Patienten und Personal betrieben werden, muß dies indirekt auch den Patienten zugutekommen.

Abgesehen davon sollte zumindest der Rechtsgedanke der §§ 6 TDSV/UDSV auch im Verhältnis Krankenhaus-Patient entsprechend herangezogen werden, da die Patienten dem Krankenhaus gegenüber nicht schlechter gestellt werden sollten als die TELEKOM-Kunden gegenüber dem öffentlichen Netzbetreiber (ebenso die Kunden im privaten D 2-Netz). Das würde bedeuten, daß den Patienten zumindest ein Wahlrecht eingeräumt werden muß, ob sie eine verkürzte oder gar keine Speicherung der Zielrufnummer wünschen. Dieses Wahlrecht sollte sich aber nicht - wie in öffentlichen Fernsprechnetzen - auf den Einzelentgeltnachweis mit vollständiger Zielnummer erstrecken.

Allerdings erklärten verschiedene Krankenhäuser, daß bei ihrer digitalen Nebenstellenanlage die Verkürzung der Zielnummer technisch nicht möglich und aus Gründen der Abrechnungstransparenz auch nicht gewünscht sei.

Trotz aller Hinweise auf die leichte Abhörbarkeit analoger *schnurloser Telefone* besteht ein Trend, solche Telefone für die Sprachkommunikation des ärztlichen und pflegerischen Personals in Krankenhäusern einzusetzen, um die schnelle Erreichbarkeit dieser Mitarbeiter auch am Krankenbett sicherzustellen und gegebenenfalls auch Gespräche über den Zustand von Patienten unabhängig von der Verfügbarkeit stationärer Telefone führen zu können.

Wir haben in mehreren Fällen zu entsprechenden Anfragen klargestellt, daß der Nutzung solcher Telefongeräte für Gespräche mit patientenbezogenem Inhalt die ärztliche Schweigepflicht entgegensteht und empfohlen, dafür - allerdings teurere - digitale Geräte zu beschaffen, die nicht so leicht abhörbar sind.

Abhörsicherheit des Funksprechverkehrs der Behörden und Organisationen mit Sicherheitsaufgaben

Der Sprechfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) war bekanntlich seit jeher abhörbar, wenn an Empfangsgeräten geringe technische Veränderungen vorgenommen wurden. Dies war strafbar, das Entdeckungsrisiko war jedoch gering. Wirksame Maßnahmen gegen das Mithören des Sprechfunkverkehrs durch Unbefugte, insbesondere durch Straftäter, sind aus Kostengründen unterblieben. Nach der Freigabe der Frequenzbereichsgrenzen Mitte 1992 ist der Funkverkehr inzwischen mit handelsüblichen Radioempfängern mithörbar.

Aus diesem Grund wurden Überlegungen angestellt, wie in Zukunft dieser Funkverkehr vor dem Abhören durch Unbefugte geschützt werden sollte. Die Technische Kommission der Konferenz der Innenminister des Bundes und der Länder wollte die Empfehlung beschließen, nach einem in Niedersachsen erprobten Modell die vorhandenen Analogfunkgeräte mit einer Inverterschaltung (Sprachverschleierungstechnik) nachzurüsten. Diese Maßnahme ist jedoch nicht geeignet, die gewünschte Vertraulichkeit des Sprechfunkverkehrs zu erreichen, da jedermann sich legal und für einen geringen Preis geeignete Funkempfänger mit Inverter beschaffen könnte, mit denen auch das Mithören invertierter Funkgespräche möglich ist.

Es war daher zu befürchten, daß mit der unzureichenden Entscheidung der Weg verbaut wird, wirksame Methoden einzuführen. Der Innenministerkonferenz wurde daher empfohlen, die Entscheidung zu überdenken und stattdessen den Anstoß zu geben, sukzessiv den digitalen und damit leicht verschlüsselbaren Sprechfunk einzuführen, der ohnehin auf Sicht Stand der Technik und damit jedenfalls in einem Teil der Länder datenschutzrechtlich verpflichtend (vgl. z. B. § 5 Abs. 1 S. 2 BlnDSG) sein wird.

Auch aufgrund der Bedenken der Konferenz der Datenschutzbeauftragten[118] hat die Technische Kommission der Innenministerkonferenz letztlich von der Einführung der Invertertechnik Abstand genommen: Vielmehr sollen weitere technologisch und wirtschaftlich in Frage kommende Sprachverschleierungssysteme auf ihre Einsatztauglichkeit als Übergangslösungen bis zur Einführung des digitalen Funksprechverkehrs geprüft werden.

116 Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (Telediensternehmen - Datenschutzverordnung - UDSV) vom 18. Dezember 1991, BGBl. I, S. 2337;
Verordnung über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM (TELEKOM - Datenschutzverordnung - TDSV) vom 24. Juni 1991, BGBl. I S. 1390

117 Rundschreiben über Rahmendienstvereinbarung zu digitalen Telefonnebenstellenanlagen vom 15. August 1991 (Dienstblatt I S. 305)

118 vgl. Anlage 2.6

Es ist zu hoffen, daß die im Rahmen des Schengener Abkommens gefaßte Entscheidung, im BOS-Bereich eine europäische Normierung zu erarbeiten, die die Digitalisierung und damit die Verschlüsselung des Funkverkehrs vorsieht, zur Beschleunigung der Einführung solcher Systeme beiträgt.

5.2 Deutschland und Europa

Zunehmende Konflikte zwischen dem Persönlichkeitsrecht des Einzelnen und der Medienfreiheit

Im Berichtszeitraum ist in der Öffentlichkeit verstärkt darüber diskutiert worden, ob die Persönlichkeitsrechte einzelner Bürger gegenüber der Berichterstattung durch die Medien ausreichend geschützt sind. Anlaß dafür waren beispielsweise

- Berichte vor allem privater Fernsehveranstalter über Unfallopfer oder Rettungseinsätze der Feuerwehr, an denen sich auch Feuerwehrbeamte oder Mitarbeiter von Rettungsdiensten beteiligten (sogenannte „Reality-TV"),
- der Fernsehbericht einer öffentlich-rechtlichen Rundfunkanstalt über Mißstände in einer Einrichtung für psychisch Kranke, bei denen die Berichterstattung keinerlei Rücksicht auf die Intimsphäre der Kranken nahm,
- die „öffentlichkeitswirksame" Durchführung von Razzien und Maßnahmen gegen mutmaßliche Schwarzarbeiter unter Hinzuziehung von Pressevertretern, wobei die kontrollierten Personen teilweise frontal fotografiert und in den Zeitungen abgebildet wurden,
- die Weitergabe personenbezogener Daten durch öffentliche Stellen, z. B. durch Polizei und Staatsanwaltschaft, aus Ermittlungsverfahren an die Medien.

Das Grundrecht auf freie Berichterstattung durch Presse und Rundfunk hat nach unserer Verfassungsordnung einen hohen Stellenwert. Dennoch genießt dieses Grundrecht keinen generellen Vorrang vor der Menschenwürde und dem Persönlichkeitsrecht des Einzelnen, über den berichtet wird.

So unterschiedlich die genannten Fälle im Einzelnen zu beurteilen sein mögen, verdeutlichen sie dennoch eine Reihe von gemeinsamen Problemen, deren Lösung gegenwärtig der Arbeitskreis Telekommunikation und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter Vorsitz des Berliner Datenschutzbeauftragten erörtert.

Das sogenannte „Medienprivileg" der Datenschutzgesetze, das Rundfunk und Presse bei ihrer journalistisch-redaktionellen Tätigkeit von den materiell-rechtlichen Vorschriften des Datenschutzrechts und von der Kontrolle unabhängiger Datenschutzbeauftragter freistellt, ist kein Freibrief für unbeschränkte Eingriffe in die Privatsphäre des Bürgers. Die Mißachtung der Menschenwürde durch die Zurschaustellung von Unfallopfern oder Menschen in Not kann nicht unter Berufung auf die Medienfreiheit gerechtfertigt werden. Dies widerspricht auch den im Rundfunkstaatsvertrag und in den Landesmediengesetzen niedergelegten Programmgrundsätzen. Vielmehr müssen die Grundrechte der Medienfreiheit und des Persönlichkeitsrechts - zu dem letztgenannten gehört auch das Recht am eigenen Bild - miteinander zum Ausgleich gebracht werden.

Daher ist der Appell der Innenministerkonferenz vom Mai 1993 an die Medien, „sich ihrer mit der Presse- und Rundfunkfreiheit verbundenen Verantwortung bewußt zu sein und von einer die Menschenwürde verletzenden Berichterstattung Abstand zu nehmen", uneingeschränkt zu begrüßen. Zwar würde der Gesetzgeber bei inhaltlichen Beschränkungen der Berichterstattungsfreiheit schnell in Konflikt mit der grundgesetzlich geschützten Medienfreiheit kommen. Andererseits muß weiter kritisch beobachtet werden, ob die bestehenden Verfahren zum Schutz des Persönlichkeitsrechts des einzelnen Bürgers (z. B. Anrufung des Deutschen Presserats und Klage vor den Zivilgerichten auf Schmerzensgeld) das Problem angemessen lösen. Zweifel bleiben angebracht.

In jedem Fall sind die Dienstbehörden in Bund und Länder verpflichtet sicherzustellen, daß sich öffentliche Bedienstete an Fernsehsendungen des sogenannten „Reality-TV" nicht beteiligen. Darauf haben wir den Polizeipräsidenten und die Feuerwehr hingewiesen.

Bei schweren Straftaten hat die Öffentlichkeit zwar in der Regel ein berechtigtes Informationsinteresse hinsichtlich des mutmaßlichen Täters; andererseits muß nicht jeder einer geringfügigen Straftat Verdächtigte es hinnehmen, in Presse oder Fernsehen abgebildet zu werden. Dies gilt beispielsweise bei der „öffentlichkeitswirksamen" Durchführung von Razzien und anderen polizeilichen Maßnahmen, bei denen zwar häufig die Gesichter der am Einsatz beteiligten Beamten, nicht aber die der kontrollierten Personen (z. B. mutmaßliche Schwarzarbeiter oder Hütchenspieler) auf den Pressefotos unkenntlich gemacht werden.

Erst recht ist es nicht hinnehmbar, wenn die Opfer von Straftaten, die sich dagegen nicht wehren können, zum Gegenstand einer Bildberichterstattung gemacht werden, die ausschließlich der Befriedigung von Sensationslust und der Steigerung der Zeitungsauflage dient. Die Veröffentlichung eines Fotos des abgetrennten Kopfes eines Mordopfers oder eines aus dem Fenster geworfenen Säuglings in der Boulevardpresse verletzt massiv das über den Tod hinaus zu achtende Persönlichkeitsrecht der Opfer und beeinträchtigt zudem die schutzwürdigen Belange der Angehörigen.

Auch die gezielte Weitergabe personenbezogener Daten durch öffentliche Stellen - z. B. Polizei und Staatsanwaltschaft - aus laufenden Ermittlungsverfahren, an denen die Öffentlichkeit ein legitimes Informationsinteresse hat, ist bisher nicht hinreichend normenklar geregelt. Weder der allgemeine Informationsanspruch der Presse nach dem Landespressegesetz noch die bundeseinheitlichen Richtlinien für das Straf- und Bußgeldverfahren enthalten verfassungskonforme Regelungen, die die Weitergabe personenbezogener Daten an die Medien rechtfertigen. Bisher müssen Polizei und Staatsanwaltschaft selbst bei einem berechtigten Informationsinteresse der Öffentlichkeit bei einer Abwägung im Einzelfall auf die Verfassung zurückgreifen, was nicht immer hinreichend geschieht und in der Praxis Probleme bereitet.

Es ist deshalb notwendig, daß der Bundesgesetzgeber durch entsprechende Festlegungen im Rahmen der ohnehin längst überfälligen Novellierung der Strafprozeßordnung und der Landesgesetzgeber durch Präzisierungen des Landespressegesetzes für einen sachgerechten Ausgleich zwischen den schutzwürdigen Belangen der betroffenen Bürger und dem Informationsinteresse der Allgemeinheit sorgen.

Die Länder haben durch den Abschluß des *Staatsvertrages über die Körperschaft des öffentlichen Rechts „Deutschlandradio"* und eines entsprechenden Hörfunk-Überleitungsstaatsvertrages mit der Bundesrepublik Deutschland[119] eine neue Rundfunkanstalt gegründet, die zwei Hörfunkprogramme veranstaltet. In ihnen sind die Programme von RIAS 1 und DS-Kultur aufgegangen. Das Deutschlandradio hat seinen Sitz in Berlin und Köln. Der „Deutschlandradio"-Staatsvertrag enthält auch Datenschutzvorschriften, die allerdings erheblich hinter dem Standard zurückbleiben, den das Berliner Datenschutzgesetz für den Sender Freies Berlin vorsieht. Während beim Sender Freies Berlin die Verarbeitung personenbezogener Daten im Verwaltungsbereich, also insbesondere der Daten von Gebührenzahlern und Mitarbeitern, durch den Berliner Datenschutzbeauftragten kontrolliert werden, gibt es beim Deutschlandradio keine vergleichbare unabhängige Datenschutzkontrolle. Vielmehr werden die Datenschutzvorschriften des „Deutschlandradio"-Staatsvertrages ausschließlich durch den internen Rundfunkdatenschutzbeauftragten überwacht. Bei den Verhandlungen über diesen Staatsvertrag sind wir nicht beteiligt worden, so daß es uns nicht möglich war, auf eine Verbesserung des Datenschutzes bei der neuen Rundfunkanstalt hinzuwirken.

GEZ: schneller als der Möbelwagen?

Der Sender Freies Berlin (SFB) betreibt gemeinsam mit den übrigen öffentlich-rechtlichen Rundfunkanstalten die Gebühreneinzugszentrale (GEZ) in Köln. Diese Einrichtung verarbeitet aufgrund des Rundfunkstaatsvertrages zentral die Daten der Rundfunkteilnehmer im Auftrag der jeweiligen Landesrundfunk-

119 vgl. das Berliner Zustimmungsgesetz vom 25. Oktober 1993, GVBl. 1993, S. 473 ff.

anstalt, also auch des Sender Freies Berlin. Können Mitteilungen oder Zahlungsaufforderungen der GEZ von der Post nicht zugestellt werden, so holt der SFB gegenwärtig eine Melderegisterauskunft beim Landeseinwohneramt über den betroffenen Bürger ein, um ihm das Schreiben zustellen zu können. Dies geschieht in der Praxis mittels Magnetbändern, mit denen die Daten postalisch nicht erreichbarer Bürger aus dem Bestand der Rundfunkanstalt mit dem Adressenbestand der Meldebehörde verglichen werden. Dabei handelt es sich um gebündelte Einzelauskünfte aus dem Melderegister, die nach § 25 Meldegesetz zulässig sind. Dieses Verfahren ist nicht zu beanstanden und hat sich auch nach Auffassung der Senatsverwaltung für Inneres bewährt.

Demgegenüber fordert der SFB gemeinsam mit den anderen Rundfunkanstalten, in Zukunft sollten die Meldebehörden verpflichtet werden, von sich aus regelmäßig bei einer Reihe von Änderungen des Meldedatenbestandes - bei jedem Umzug und jedem Sterbefall - die GEZ hierüber unaufgefordert zu informieren. In Hessen und Nordrhein-Westfalen ist dies bereits geltendes Recht. Hintergrund für diese Forderung der Rundfunkanstalten ist der härter werdende Konkurrenzkampf mit den privaten, nicht gebührenfinanzierten Rundfunkveranstaltern, der die öffentlich-rechtlichen Rundfunkanstalten neben Einsparungen im eigenen Bereich dazu zwingt, den Gebühreneinzug effektiver zu gestalten. Nach Angaben der Rundfunkanstalten ist der Adressenbestand der GEZ deshalb vielfach veraltet, weil die Rundfunkteilnehmer der GEZ Anschriftenänderungen entweder überhaupt nicht oder verspätet mitteilen. Durch die regelmäßige Übermittlung von Meldedatenänderungen hoffen die Rundfunkanstalten, ihr Gebührenaufkommen entscheidend zu erhöhen, indem der von ihnen vermutete erhebliche Anteil der „Schwarzseher" ermittelt werden könnte.

Die Konferenz der Ministerpräsidenten der Länder hat die Forderung der Rundfunkanstalten aufgegriffen und die Innenministerkonferenz um einen Vorschlag zur bundeseinheitlichen Änderung des Melderechts gebeten. Der Entwurf der Innenministerkonferenz, der bei Stimmenthaltung Berlins beschlossen wurde, sieht eine Änderung des Melderechtsrahmengesetzes vor, wonach künftig alle Meldebehörden im Fall der Anmeldung, der Abmeldung oder des Todes eines volljährigen Einwohners dessen Namen, Geburtstag, gegenwärtige und frühere Anschriften, Tag des Ein- bzw. des Auszuges, Familienstand und im Todesfall den Sterbetag den Rundfunkanstalten übermitteln sollen.

Bei einer Verwirklichung dieses Vorschlags würde ein entscheidender Schritt in Richtung auf ein Bundesmelderegister aller volljährigen Einwohner der Bundesrepublik getan, das bei den Beratungen des Melderechtsrahmengesetzes im Bundestag ausdrücklich aus Gründen des Datenschutzes abgelehnt worden ist. Zwar sieht der Rundfunkstaatsvertrag vor, daß die Rundfunkanstalten jeweils nur auf die Daten der zu ihrem Sendebereich gehörenden Hörer und Zuschauer zugreifen dürfen, im Fall des Umzugs in die Bereiche anderer Sender darf aber auch auf deren Datenbestände zugegriffen werden. Außerdem ist abzusehen, daß schon die Existenz des dann entstehenden bundesweiten Meldedatenbestandes bei der GEZ zu großen Begehrlichkeiten bei einer Vielzahl von öffentlichen und privaten Stellen führen würde.

Entscheidend ist aber, daß bei dem vorgeschlagenen Verfahren in großem Umfang Meldedaten an die Rundfunkanstalten übermittelt würden, die diese zum Einzug von Rundfunkgebühren nicht benötigen. Viele Bürger teilen von sich aus der GEZ mit, daß sie ein Rundfunkgerät zum Empfang bereithalten oder daß sie umgezogen sind. Durch die vorgeschlagene regelmäßige Meldedatenübermittlung an die Rundfunkanstalten würde in unverhältnismäßiger Weise in das informationelle Selbstbestimmungsrecht dieser Bürger eingegriffen. Ein solcher Eingriff läßt sich weder mit den finanziellen Problemen der öffentlich-rechtlichen Rundfunkanstalten noch mit deren verfassungsrechtlicher Bestandsgarantie rechtfertigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deshalb die vorgeschlagene regelmäßige Übermittlung von Meldedaten an die öffentlich-rechtlichen Rundfunkanstalten abgelehnt[120]. Selbst wenn der Entwurf der Innenministerkonferenz Eingang in das Melderechtsrahmengesetz finden sollte, sind wir mit der Senatsverwaltung für Inneres[121] der Auffassung, daß eine entsprechende Änderung des Berliner Meldegesetzes nicht in Betracht kommt, solange datenschutzrechtliche Alternativen nicht einmal geprüft worden sind.

Dringend erforderlich ist dagegen die bereits Anfang 1992 von uns angemahnte Ergänzung der *Verordnung über die Feststellung der Befreiung von der Rundfunkgebührenpflicht*[122] um die erforderlichen Befugnisse zur Datenverarbeitung. Insbesondere die Übermittlung der Daten von Personen, die von der Rundfunkgebührenpflicht durch die Sozialämter befreit worden sind, an den SFB erfolgt gegenwärtig immer noch ohne die erforderliche Rechtsgrundlage.

Die zweite Stufe der Postreform - Privatisierung der TELEKOM zu Lasten der Kunden?

Die vollständige Privatisierung der Deutschen Bundespost TELEKOM, die in eine AG umgewandelt werden soll, ist politisch beschlossene Sache. Die Beratungen über die dazu erforderliche Grundgesetzänderung und ergänzende gesetzliche Regelungen haben Anfang 1994 begonnen.

Schon im Juni 1993 hat die TELEKOM allerdings ein Tochterunternehmen, die DeTeMobil-GmbH, gegründet und ihr den Betrieb sämtlicher Mobilfunkeinrichtungen (C- und D 1-Netze, Eurosignal, CITY-Ruf, Bündelfunk) übertragen.

Die mit jeder Privatisierung öffentlicher Aufgabenerfüllung verbundenen datenschutzrechtliche Probleme sind bereits an anderer Stelle[123] behandelt worden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat gerade im Zusammenhang mit der zweiten Stufe der Postreform betont, daß die Privatisierung der TELEKOM nicht zu einer Schlechterstellung der Bürger duch eine Absenkung des materiell-rechtlichen Datenschutzstandards führen darf. Dies gilt insbesondere bei dem wichtigsten von der TELEKOM angebotenen Dienst, dem Sprachtelefondienst. Außerdem muß der Gesetzgeber sicherstellen, daß für eine zukünftige TELEKOM-AG und ihre Tochterunternehmen eine einheitliche Datenschutzkontrolle gewährleistet wird, bei der auch eine Kontrolle von Amts wegen möglich ist. Die Aufsichtsbehörden für den privaten Bereich können dagegen nach dem geltenden Bundesdatenschutzgesetz nur einschreiten, wenn ihnen hinreichende Anhaltspunkte für eine Verletzung datenschutzrechtlicher Bestimmungen vorliegen. Die meisten Aufsichtsbehörden werden deshalb erst auf Beschwerden von Bürgern hin tätig. Dies ist jedoch gerade im Bereich der Telekommunikation nicht ausreichend, zumal der Bürger die Datenverarbeitung in digitalen Telekommunikationsnetzen kaum durchschauen kann und deshalb nur selten Anlaß für eine Beschwerde sehen wird[124].

Die durch den *Fangschaltungsbeschluß* des Bundesverfassungsgerichts[125] notwendig gewordene Neuregelung des Telekommunikationsrechts steht noch immer aus und soll jetzt im Zusammenhang mit der zweiten Stufe der Postreform erfolgen. Dabei wird es darauf ankommen, eine verfassungskonforme Rechtsgrundlage für die Verarbeitung der zwangsläufig anfallenden Verbindungsdaten in öffentlichen und privaten Telekommunikationsnetzen zu schaffen. Zugleich muß der verfassungsrechtlich bedenkliche Zustand beendet werden, daß gegenwärtig Auskünfte über Verbindungsdaten an die Strafverfolgungsbehörden auch bei Bagatelldelikten zulässig sind.

Zum 1. Januar 1994 ist eine Vorschrift der TELEKOM-Datenschutzverordnung (TDSV) in Kraft getreten, die dem Telefonkunden das Recht gibt, fallweise - also bei jedem Telefongespräch - darüber zu entscheiden, ob er die bei ISDN-fähigen Telefonapparaten mögliche *Anzeige seiner Rufnummer* beim Angerufenen unterdrücken will oder nicht. Dies könnte technisch durch Knopfdruck oder durch Wahl einer bestimmten Nummer vor der eigentlichen Rufnummer geschehen. Bisher ist jedoch nicht

120 Anlage 2.3

121 vgl. die Antwort des Senats auf die Kleine Anfrage Nr. 4619, LPD vom 15. Dezember 1993
122 vgl. Jahresbericht 1991, 2.3
123 vgl. 3.2
124 vgl. Anlage 2.4
125 dazu vgl. Jahresbericht 1992, 5.2

erkennbar, daß die TELEKOM oder andere Hersteller von Telefonapparaten entsprechende Geräte anbieten. Damit droht ein wichtiges Wahlrecht der TDSV leerzulaufen, weil der Telefonkunde, der einen ISDN-Hauptanschluß hat, bisher darauf verwiesen wird, sich ein für alle Mal für oder gegen die Rufnummernanzeige zu entscheiden. Die Anzeige der Rufnummern von analogen Anschlüssen, von denen aus beim Inhaber eines ISDN-fähigen Telefons angerufen wird, ist zwar technisch möglich, wird aber nach Angaben der TELEKOM bisher nicht durchgeführt. Nach dem Wortlaut der TDSV müßte auch in diesem Fall eine individuelle Unterdrückungsmöglichkeit (z. B. durch Wahl einer bestimmten Ziffer) geschaffen werden, bevor Rufnummern von analogen Anschlüssen angezeigt werden dürfen.

Auf der Ebene der *Europäischen Union* tritt die Entwicklung des Telekommunikationsdatenschutzrechts noch immer auf der Stelle. Die Europäische Kommission hat im Berichtszeitraum keine geänderte Fassung ihres Vorschlags für eine *ISDN-Richtlinie* beschlossen, so daß der Abstand zwischen diesem für den europäischen Telekommunikationsmarkt so wichtigen Vorhaben und der *allgemeinen Datenschutzrichtlinie*, mit der er ursprünglich gemeinsam in Kraft gesetzt werden sollte, immer größer wird. Gleichzeitig sind andere Initiativen der Europäischen Kommission im Telekommunikationssektor schon sehr viel weiter gediehen, etwa der Entwurf für eine Richtlinie über den *offenen Netzzugang* im Sprachtelefondienst[126], die zum Teil Regelungen enthält, die erheblich hinter dem Vorschlag für eine ISDN-Datenschutzrichtlinie zurückbleiben. Die endgültige Beschlußfassung im Rat bleibt allerdings abzuwarten.

Besonderes Gewicht mißt die Kommission auch dem Aufbau der im Europäischen Unionsvertrag von Maastricht genannten *transeuropäischen Netze* bei. Insbesondere das ISDN wird zu einem der ersten transeuropäischen Netze ausgebaut werden[127]. Auch der grenzüberschreitende Datenaustausch zwischen Verwaltungen wird von der Kommission gefördert[128].

Der Ministerrat der Europäischen Gemeinschaften (Europäische Rat) hat am 22. Juli 1993[129] beschlossen, daß die Monopole im öffentlichen Sprachtelefondienst europaweit bis zum 1. Januar 1998 beseitigt werden müssen. Dies soll im Zuge der zweiten Stufe der Postreform auch in der Bundesrepublik umgesetzt werden. Damit wird es in naher Zukunft in der Europäischen Union zu einem Wettbewerb zwischen zahlreichen Diensteanbietern kommen, so daß sich das oben beschriebene Problem der Gewährleistung eines einheitlichen hohen Datenschutzstandards auch auf europäischer Ebene stellen wird. Schon deshalb ist es dringend erforderlich, daß die von der Kommission vorgeschlagene *Datenschutzrichtlinie für das ISDN* zügig verabschiedet wird. Darauf hat auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hingewiesen[130].

Einer Lösung auf europäischer Ebene bedürfen auch die Datenschutzprobleme im Zusammenhang mit der Mobilkommunikation. So müssen die Daten der Mobilfunkteilnehmer auf der Funkstrecke wirksam verschlüsselt werden. Eine bloße Digitalisierung der Signale reicht nicht aus, denn durch sie wird das Abhören nur erschwert, nicht aber zuverlässig ausgeschlossen. Den Benutzern sollte eine kostenlose Ende-Zu-Ende-Verschlüsselung angeboten werden. Vor allem aber müssen gerade bei der Mobilkommunikation, wo Informationen über den jeweiligen Standort des Teilnehmers auch dann verarbeitet werden, wenn sein Gerät nur empfangsbereit ist, wirksame Vorkehrungen gegen die Entstehung von Bewegungsbildern getroffen werden. Dazu müssen laufende und künftige Normierungsprozesse entsprechend beeinflußt werden. Wenn schon der Anfall solcher Standortdaten nicht von vornherein technisch ausgeschlossen werden kann, muß durch die Gesetzgebung der Union oder der Mitgliedstaaten eine strenge Zweckbindung dieser Daten an die technische Vermittlung der Telekommunikationsverbindung gewährleistet werden. Jede darüber hinausgehende Nutzung sollte ausdrücklich untersagt werden.

Gerade im Bereich der Telekommunikation ist es entscheidend, daß die Europäische Union nicht unter Hinweis auf den Grundsatz der Subsidarität davon absieht, die angesprochenen Fragen möglichst einheitlich zu regeln. Die Mobilkommunikation wird gerade im grenzüberschreitenden Verkehr große Bedeutung erlangen, wie das Beispiel der Erhebung von Straßenbenutzungsgebühren zeigt[131]. Einheitliche hohe Datenschutzanforderungen sind deshalb eine Grundvoraussetzung für die Akzeptanz dieser Technik, der die Europäische Kommission mit Recht so große Bedeutung beimißt.

6. Durchsetzung des Datenschutzes

6.1 Datenschutz im Verwaltungsverfahren

Offener Versand von Schriftstücken

Der offene Versand von Schriftstücken und die Verwendung offener Postkarten mit personenenbezogenem Inhalt sind unzulässig, weil dadurch unbefugte Dritte Rückschlüsse auf die Beziehungen eines Bürgers zur Verwaltung ziehen können[132].

Die Senatsverwaltung für Inneres hat dies in zwei Rundschreiben[133] allgemein bekanntgegeben. Nun sollte man meinen, daß dies in der Berliner Verwaltung auch so gehandhabt wird. Dem ist leider - wie mehrere Beschwerden belegen - nicht immer so.

Ein Wohnungsamt kündigte auf offenen Postkarten die Besichtigung von Wohnungen zum Zweck der Bau- bzw. Wohnungsaufsicht an.

Das Bau- und Wohnungsaufsichtsamt vertrat die Auffassung, daß es sich bei den Ankündigungen eines Termins für die Besichtigung der Wohnung nicht um ein zum persönlichen Lebensbereich gehörendes Geheimnis handele und kündigte an, die offenen Postkarten weiterzuverwenden. Das Bezirksamt selbst, an das die Beanstandung zu richten war (§ 26 BlnDSG), hatte sich gar nicht geäußert. Erst die Ankündigung, die Bezirksaufsicht einzuschalten, brachte den gewünschten Erfolg.

Das Landeseinwohneramt legte uns eine Mitteilung in Strafsachen mit der Abschrift der Anklageschrift, die einen dort beschäftigten Mitarbeiter betraf, vor. Der Vorgang ist im Landeseinwohneramt offen eingegangen, nachdem ihn zuvor 17 Stellen (!) bei der Senatsverwaltung für Inneres, dem Landesamt für Verfassungsschutz und dem Landesverwaltungsamt zur Kenntnis erhalten haben.

Das Landeseinwohneramt teilte mit, daß es schon mehrfach die Amtsanwaltschaft gebeten hatte, vergleichbare Vorgänge direkt und verschlossen zuzuleiten. Schriftstücke mit personenbezogenem Inhalt sind dann, wenn sich herausstellt, daß es sich um einen Irrläufer handelt, wieder zu verschließen und an die richtigen Empfänger weiterzuleiten. Die Leiterin der Amtsanwaltschaft hat den Vorgang zum Anlaß genommen, in ihrem Geschäftsbereich nochmals auf die Verpflichtung hinzuweisen, diese sogenannten „Mistra"-Mitteilungen verschlossen zu versenden.

Geburtsdaten im Adreßfeld

Bei den Anhörungsbögen und Bußgeldbescheiden zu Verkehrsordnungswidrigkeiten werden das Geburtsdatum und -ort so ausgedruckt, daß diese im Sichtfenster der Briefumschläge erscheinen können. In den Anhörungsbögen sind die Geburtsdaten knapp unter dem Sichtfensterteil ausgedruckt. Das kann bei einer unsachgemäßen Kuvertierung dazu führen, daß diese Daten - auch für unbefugte Dritte - sichtbar werden, obwohl sie für

126 KOM (92) 247 endg.-SYN 437; geänderter Vorschlag KOM (93) 182 endg.-SYN 437
127 KOM (93) 347 endg.
128 KOM (93) 69 endg.
129 Amtsblatt der EG Nr. C 213 vom 6. August 1993
130 Anlage 2.5
131 vgl. oben 4.11
132 vgl. zuletzt Jahresbericht 1986, 4.5, 1987, 5.7 1989, 4.10 und 1990, 3.11
133 DBl I v. 18. Dezember 1985, DBl I v. 11. September 1987

einen ordnungsgemäßen Postversand nicht erforderlich sind[134]. Unabhängig davon werden die Geburtsdaten auch bei einer ordnungsgemäßen Kuvertierung bei leichtem Druck auf den Umschlag sichtbar.

Die Geburtsdaten sind nach § 66 Ordnungswidrigkeitengesetz (OWiG) erforderlich, weil die Personalien des Betroffenen in den Bescheiden möglichst genau angegeben werden müssen, damit keine Zweifel über die Identität entstehen können. Diese Vorschrift regelt aber nicht, *wo* die Zusatzdaten ausgedruckt werden.

Der Polizeipräsident hatte bisher immer erklärt, daß Programmänderungen außerordentlich schwierig seien. Im übrigen sind die Vordrucke in Verkehrsordnungswidrigkeitenverfahren auf Bund-Länder-Ebene abgestimmt und bundeseinheitlich empfohlen worden.

Wir haben bereits vor Jahren darauf hingewiesen, daß an der technischen Realisierbarkeit rechtliche Vorgaben nicht scheitern dürfen. Der Polizeipräsident wird um einen von uns vorgeschlagenen und einfach zu realisierenden Vorschlag aufzugreifen alle Geburtsdaten um eine Zeile nach unten zu verschieben.

Zahle bei der Zulassungsstelle nie mit großen Scheinen ...

Die Zahlstellen der Zulassungsstelle waren dazu übergegangen, Personen, die Verwaltungsgebühren oder andere Einzahlungen mit 500-DM- oder 1000-DM-Scheinen begleichen wollen, namentlich auf gesonderten Listen zu erfassen.

Diese Praxis wurde wegen der Vorlage eines gefälschten Geldscheines eingeführt. Die Senatsverwaltung für Finanzen war mit uns einig, daß eine derartige Erhebung personenbezogener Daten ohne Rechtsgrundlage erfolgte. Sie hat das Landeseinwohneramt darauf hingewiesen, daß die namentliche Aufzeichnung unterbleiben muß und stattdessen die Scheine besonders zu prüfen sind. Bei größeren Umsätzen wird die Anschaffung eines Banknotenprüfgerätes empfohlen. Bei der Berliner Zulassungsstelle wird seither entsprechend verfahren.

Vorlage des Scheidungsurteils

Eine alleinerziehende Mutter wandte sich an uns, weil sie bei der Landesbank Berlin zur Eröffnung eines Jugend-Giro-Kontos für ihren minderjährigen Sohn das Scheidungsurteil vorlegen sollte.

Zur Eröffnung eines Giro-Kontos für einen Minderjährigen ist die Zustimmung der gesetzlichen Vertreter erforderlich. Da bei der Scheidung das Sorgerecht geregelt wird, muß nachgewiesen werden, wem die elterliche Sorge übertragen wurde. Hierfür reicht allerdings die Vorlage des Urteilstenors aus, soweit es die Entscheidung des Gerichtes über die Vermögenssorgeberechtigung betrifft. Weitergehende Scheidungsaussprüche - insbesondere Scheidungsfolgesachen - müssen geschwärzt werden können.

Wir haben der Landesbank Berlin empfohlen, Kunden bei der Eröffnung eines Jugend-Giro-Kontos künftig darauf hinzuweisen, daß nur der Scheidungsspruch, der das Sorgerecht betrifft, vorgelegt werden muß. Die Landesbank ist unserer Empfehlung gefolgt und wird eine entsprechende Arbeitsanweisung für alle Mitarbeiterinnen und Mitarbeiter der Landesbank veröffentlichen.

6.2 Falschverstandener Datenschutz

Mitunter muß der Datenschutz dafür herhalten, ganz andere Zwecke zu verdecken:

Ein arbeitsloser Berliner und seine lettische Frau sind mehreren Kindern unterhaltsverpflichtet. Bei der Amtsvormundschaft eines Bezirksamtes versuchte der Ehemann, seine Zahlungsbeträge zu verringern, indem er auf die auch noch zu leistende Unterstützung der in Rußland lebenden Familienangehörigen der Ehefrau verwies. Als er dieses Ziel nicht erreichen konnte, hat er Durchschriften seiner Schreiben an das Bezirksamt den in Rußland lebenden Familienangehörigen und dortigen öffentlichen Stellen zur Verfügung gestellt, um Verständnis für die Verringerung der Unterstützung zu werben. Dieses Vorgehen erschien dem Bezirksamt datenschutzrechtlich bedenklich.

Diese Bedenken sind natürlich unbegründet. Selbstverständlich kann der Betroffene selbst Durchschriften seiner privaten Schreiben jedermann im In- und Ausland zur Verfügung stellen. Anders sähe es nur für das Bezirksamt selbst aus: Die Amtsvormundschaft arbeitet im Anwendungsbereich des Sozialgesetzbuches und darf Angaben über die persönlichen und sachlichen Verhältnisse eines Betroffenen nur dann offenbaren, wenn entweder eine der Voraussetzungen der §§ 67 bis 78 SGB X erfüllt ist oder der Betroffene eingewilligt hat.

Das SGB bindet den Betroffenen selbst nicht. Zu beachten ist allerdings, daß - sofern die Briefe z. B. unwahre Tatsachenbehauptungen oder Beleidigungen enthalten - möglicherweise Straftatbestände erfüllt sein können. Das ist dann allerdings nicht mehr unter den Aspekten des Datenschutzrechtes zu untersuchen.

Eine Tageszeitung glossierte folgenden Vorgang:

Jemand fand seine Notizen über die dienstliche Telefonnummer eines Behördenangestellten in der Finanzverwaltung nicht mehr und versuchte, über die Telefonzentrale Kontakt mit ihm aufzunehmen. Nach mehreren Versuchen gab er dieses Unterfangen entnervt auf. Zunächst teilte ihm die Telefonzentrale mit, daß der Mitarbeiter nicht in der Telefonliste enthalten sei. Die Personalabteilung, mit der er dann verbunden wurde, habe ihm erklärt, daß sie aus datenschutzrechtlichen Gründen keine Auskunft erteilen dürfe.

Das Datenschutzrecht verbietet zwar die Offenbarung von Personaldaten durch die Personalabteilung, dies gilt selbstverständlich nicht für Angaben, die erforderlich sind, um den Verwaltungsablauf einerseits, den Kontakt zwischen Verwaltung und Bürger andererseits zu ermöglichen. Die amtliche Telefonnummer gehört dazu - bei bestimmten Berufsgruppen, deren Arbeitsplatz zu Hause ist, im übrigen auch die private!

Eine Soziologiestudentin möchte ihr soziologisches Studium mit einer Dissertation über die Rolle der Berliner Kioske abschließen. Sie wandte sich hierzu an die BVG mit der Bitte, ihr die Standorte der von der BVG verpachteten Kioske mitzuteilen. Obwohl sie nach keinen personenbezogenen Daten gefragte hatte, wurde ihr Ansinnen mit einem kargen Hinweis auf den Datenschutz abgelehnt.

Wie sich bei Nachforschungen herausstellte, lag das Problem nicht darin, daß die BVG die Herausgabe personenbezogener Daten gefürchtet hätte. Vielmehr sind die von der Studentin erwünschten Daten nur auf Karteikarten notiert; eine Einsichtnahme in die Karteikarten hätte zur Offenbarung aller personenbezogenen Daten im Zusammenhang mit den jeweiligen Kiosken geführt. Die von der Studentin erwünschte Auflistung der Standorte der Kioske wurde wegen des damit verbundenen Arbeitsaufwandes abgelehnt.

Ganz offenkundig wurde hier der Datenschutz vorgeschoben, um den eigentlichen Grund, nämlich die Scheu vor den mit dem Auskunftsersuchen verbundenen Arbeiten, zu verschleiern. Wir haben uns bemüht, die BVG dazu zu bewegen, die Studentin gleichwohl in ihrem Projekt zu unterstützen.

Ein Strafgefangener berichtete uns, die Anstaltsleitung habe seinen Wunsch, eine Speicherschreibmaschine in der Haft benutzen zu dürfen, ebenfalls unter Hinweis auf den Datenschutz abgelehnt.

Auch hier kann schließlich der Datenschutz kein Grund für die Ablehnung des Gesuchs des Strafgefangenen sein: Abgesehen davon, daß eine Speicherschreibmaschine in der Regel über keine Funktionen verfügt, mit denen Daten im strengen Sinne verarbeitet werden können, ist kein datenschutzrechtlicher Grund für die Ablehnung des Wunsches ersichtlich. Sollte es aus irgendeinem Grund für den Strafvollzug für untunlich gehalten werden, Strafgefangenen eine Speicherschreibmaschine zu überlassen, sollte dies auch so begründet werden.

134 vgl. Jahresbericht 1986, 4.5

6.3 Dateienregister

Im Berichtszeitraum gingen zum Dateienverzeichnis ca. 1000 und zum Geräteverzeichnis ca. 950 Meldungen bei uns ein. Trotz der relativ hohen Zahlen sind bei weitem nicht alle Stellen ihrer Meldepflicht nachgekommen. Um die säumigen Stellen erneut auf ihre Meldepflicht aufmerksam zu machen, werden wir im laufenden Jahr die ausstehenden Meldungen anmahnen, da die in der Dateienregisterverordnung angegebenen Fristen längst verstrichen sind.

Auch Behörden haben Schwierigkeiten mit Formularen ...

Trotz der ausführlichen Ausfüllanleitung in der von uns herausgegebenen Broschüre „Informationen zum Berliner Dateienregister" gab es doch viele Mängel, die bei Beachtung der Hinweise hätten vermieden werden können. Nicht nur uns, sondern auch den Stellen selbst bringt eine fehlerhafte Meldung erhebliche Mehrarbeit ein, da in den meisten Fällen die Meldungen zurückgeschickt, geändert und neu ausgefüllt werden müssen.

Unter den fehlerhaften Meldungen befanden sich viele, die mit der Hand und nicht wie in der Dateienregisterordnung vorgeschrieben auf Schreibmaschine oder Drucker ausgefüllt wurden. Dies machte die Weiterverarbeitung mit einem Scanner unmöglich.

Auf zahlreichen Meldungen wurden - überwiegend handschriftlich - sachfremde Angaben, z. B. interne Vermerke, Notizen, Abzeichnungshinweise gemacht, so daß bei der Erfassung unsinnige Zeichenfolgen abgebildet werden, die nachträglich manuell gelöscht werden müssen.

Das Nebeneinander von Dateien- und Geräteregister macht nur dann Sinn, wenn eine Verknüpfung möglich ist: Erst dann kann ermittelt werden, welche Dateien auf welchen Geräten verarbeitet werden. Hierzu dient eine Ordnungsnummer, die in jeder Meldung anzugeben ist. Bei sehr vielen Meldungen fehlte die Angabe dieses Ordnungsmerkmals.

Zur Angabe der „Art der Daten" werden immer wieder die programmtechnischen Feldbezeichnungen verwendet. Mit diesen wenig aussagekräftigen Angaben kann ein Bürger ohne intensive Beratung durch uns kaum etwas anfangen.

Automatisierte Meldungen

Im vergangenen Jahr sind immer mehr Stellen dazu übergegangen, ihre Meldungen auf Disketten abzugeben. Um die Verarbeitung dieser Angaben zu ermöglichen, haben wir ein Merkblatt herausgegeben, auf dem die softwaremäßigen Voraussetzungen für unser Rechnersystem festgehalten sind.

Auch für die Stellen selbst ist diese Form der Meldung vorteilhaft. Da nach § 19 Abs. 2 und 4 BlnDSG auch interne Dateien- und Geräteübersichten zu führen sind, lassen sich mit der Automation dieser internen Übersichten beim behördlichen Datenschutzbeauftragten auch die Meldungen an uns automationsgestützt abwickeln.

Gelegentlich erhalten wir Anfragen, ob im Zusammenhang mit automatisierten Meldungen auch Abweichungen von Form und Inhalt der Meldeformulare akzeptiert werden können. Wir müssen hier auch im Hinblick auf die Dateiregisterverordnung darauf Wert legen, daß

- die Meldungen zum Dateien- und Geräteregister § 19 Abs. 2 und 4 BlnDSG vollständig umsetzen;
- die Meldungen so gestaltet sind, daß dem Bürger die nach § 25 Abs. 1 Satz 2 BlnDSG zu gewährenden Einsichtsrechte in zumutbarer, das heißt verständlicher Form ermöglicht werden können, ohne daß eine fachliche Beratung durch unser Haus dabei erforderlich ist;
- die Meldungen dazu geeignet sind, uns die Kontrolle nach § 24 Abs. 1 BlnDSG in der jeweils angemessenen Form zu ermöglichen, das heißt z. B. bei dezentralen Systemen wie PCs oder LANs, daß auch unangekündigte Kontrollbesuche an den Standorten möglich sind;
- die Meldungen ohne manuelle Erfassung automatisiert weiter verarbeitbar sind (Scanner, Umsetzung in Textdateien).

ADV-Verfahren INVENT

Eine weitere Möglichkeit, der Meldepflicht zum Geräteregister nachzukommen, wird derzeit vom LIT realisiert. Im Zusammenhang mit dem Verfahren INVENT (Inventarisierung des IT-Gerätebestandes), das für die Bedürfnisse der Haushaltsplanung entwickelt wird, wird ein Report-Programm erstellt, das den datenverarbeitenden Stellen ausgehändigt werden soll. Mit Hilfe dieses Programms können von den Stellen, die bereits Daten für ihre IT-Geräte eingegeben haben, die erforderlichen Daten für das Geräteregister aus dem Datenbestand des INVENT herausgezogen und entsprechend dem Formular des Geräteverzeichnisses dargestellt werden. Informationen, die für das Geräteverzeichnis verlangt werden, aber in INVENT nicht enthalten sind, müssen von der meldenden Stelle nachgetragen werden. Die derart aufbereitete Meldedatei kann dann auf eine Diskette gespeichert und uns zugesandt werden. Später ist daran gedacht, ein ähnliches Programm auch für die Dateimeldungen zu entwickeln.

6.4 Der Berliner Datenschutzbeauftragte

Die Dienststelle

Das Gesetz über den Landesbeauftragten zur Aufarbeitung der Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik im Land Berlin vom 20. November 1992[135] bestimmt, daß der Landesbeauftragte dem Geschäftsbereich des Berliner Datenschutzbeauftragten zugeordnet ist. Diese nicht ganz unproblematische Zuordnung führte zu einer intensiven Zusammenarbeit: Der vom Abgeordnetenhaus gewählte Landesbeauftragte Martin Gutzeit leistete am 6. Januar vor der Präsidentin des Abgeordnetenhauses seinen Amtseid und unterzeichnete mit dem Datenschutzbeauftragten seinen Vertrag. In der Folgezeit unterstützten wir ihn beim Aufbau der Dienststelle. Da ihm allerdings das ganze Jahr über keine angemessenen Diensträume zur Verfügung standen, war seine Dienststelle nur begrenzt arbeitsfähig. Es ist zu hoffen, daß mit dem Umzug in die endgültige Dienststelle (Krausenstraße 8, 10117 Berlin) die Aufgaben in vollem Umfang wahrgenommen werden können. Inhaltlich kam es zu keinen Differenzen.

Auch unsere eigene Dienststelle hat neue Räume bezogen. Wegen des Ablaufs der Mietfrist bei der Bauberufsgenossenschaft wurden zusammen mit zwei Prüfgebieten des Rechnungshofes Diensträume in einem Verwaltungsgebäude der AOK (Pallasstraße 25, 10781 Berlin) angemietet. Hier stehen nun angemessene Räume insbesondere auch für die Bürgerberatung zur Verfügung.

Personell blieb es beim Vorjahresstand; um wenigstens eine Verminderung der Mitarbeiterzahl zu verhindern, stimmte das Abgeordnetenhaus dem Wegfall eines bis dahin an einer Juristenstelle angebrachten kw-Vermerks („kann wegfallen") zu. Für den kommenden Doppelhaushalt haben wir trotz der Haushaltssituation eine gewisse Stellenmehrung beantragt: Die erheblichen Stelleneinsparungen, die wegen der knappen Mittel in der Verwaltung vorgenommen werden sollen, sollen durch intensiven Einsatz von IuK-Technik kompensiert werden. Die oben beschriebenen neuen ADV-Verfahren belegen dies. Diese Entwicklung macht es aber auch erforderlich, die Kontrollkapazitäten zu erhöhen; mit dem derzeitigen Mitarbeiterstab ist die Sicherstellung des Datenschutzes unter den künftigen Bedingungen nicht mehr zu gewährleisten.

Aufgabenentwicklung

Die Zahl der Beschwerden und Beratungswünsche von Bürgern ist für den Berichtszeitraum gegenüber dem Vorjahr nochmals leicht angestiegen. Die meisten Beschwerden richteten sich gegen Behörden aus dem Sicherheitsbereich (Justiz, Polizei und Landesamt für Verfassungsschutz), gefolgt von den Gesundheits- und Sozialbehörden (einschließlich Jugendbereich) sowie die Ordnungsbehörden - hier insbesondere der Bereich Meldewesen. Eine beachtliche Anzahl von Beschwerden richtete sich gegen die Verarbeitung von Personaldaten und in steigendem Maße auch gegen Geschäftsordnungsangelegenheiten (Zusatzdaten im Adreßfeld, Formulare).

135 GVBl S. 335

Die Beratungsersuchen der Verwaltung sind im Berichtsjahr auf dem hohen Niveau des Vorjahres geblieben, im Zusammenhang mit der Einführung neuer IuK-Techniken erheblich gestiegen. Bei den Rechtsfragen stehen hier die Bereiche Bildung und Forschung sowie Gesundheit und Soziales vorn, aber auch die Ordnungsverwaltung macht von dieser Möglichkeit verstärkt Gebrauch.

Abgeordnetenhaus

Auch im Berichtsjahr hat der Berliner Datenschutzbeauftragte anläßlich der parlamentarischen Beratung des Jahresberichts 1992 von seinem Rederecht vor dem Abgeordnetenhaus Gebrauch gemacht.[136] Der Unterausschuß „Datenschutz" des Innenausschusses hat die anstehenden Probleme intensiv beraten. Insbesondere hat der Ausschuß großen Wert auf die Benennung behördlicher Datenschutzbeauftragter gelegt, deren Aufgabe die Umsetzung des Datenschutzes vor Ort ist.

Auch in anderen Ausschüsse des Hauses wurden datenschutzrechtliche Fragen beraten; hervorzuheben sind hier die Beratungen des Archivgesetzes im Ausschuß für kulturelle Angelegenheiten sowie im Rechtsausschuß. Der Petitionsausschuß hat uns mehrere Fragen zur Begutachtung vorgelegt.

Kooperation

Das Datenschutzgesetz verpflichtet den Datenschutzbeauftragten, mit allen Stellen zusammenzuarbeiten, die wie er die Aufgabe haben, die Einhaltung der Vorschriften über den Datenschutz zu kontrollieren (§ 24 Abs. 4 BlnDSG). Besondere Bedeutung kommt dabei der Zusammenarbeit im Rahmen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu. Im Berichtsjahr hatte der Berliner Datenschutzbeauftragte den Vorsitz übernommen. In zwei Sitzungen wurden Beschlüsse zu grundlegenden Fragen gefaßt[137].

Besondere Bedeutung kommt nach wie vor dem Datenschutz beim Aufbau der Verwaltung in den neuen Bundesländern zu. Berlin hat sich hier von Anfang an an einer Arbeitsgruppe der Datenschutzbeauftragten der neuen Länder beteiligt, die sich im Laufe des Jahres mehrfach traf und manche Entwicklung wie etwa das Schicksal der weiteren Verwertung der PKZ kritisch verfolgte.

Besonders intensiv ist naturgemäß die Zusammenarbeit mit dem brandenburgischen Datenschutzbeauftragten. Neben der Abstimmung zu den allgemein interessierenden Fragen zwingen mehr und mehr gemeinsame Stellen oder zumindest gemeinsam betriebene Informationssysteme auch zu einer ganz spezifischen Zusammenarbeit. Hier wurde in jedem Fall ein sehr gutes Einvernehmen erzielt.

Von Beginn an hat der Berliner Datenschutzbeauftragte den Vorsitz im Arbeitskreis Medien der Konferenz inne. Auch die Internationale Konferenz der Datenschutzbeauftragten hat uns mit dem Vorsitz des Arbeitskreises Telekommunikation und Medien betraut. Traditionsgemäß wurde die Internationale Funkausstellung als Gelegenheit für die Durchführung einer Arbeitssitzung genutzt. Über die Ergebnisse wurde auf der diesjährigen Sitzung in Manchester berichtet[138]. Auch auf der Ebene der Europäischen Union wurde eine Arbeitsgruppe geschaffen, deren Aufgabe die Erarbeitung von Stellungnahmen zu den verschiedenen, den Datenschutz berührenden Themen der Telekommunikation ist.

Auch die Zusammenarbeit mit den anderen Kontrollinstanzen, insbesondere mit der Aufsichtsbehörde für den Datenschutz bei der Senatsverwaltung für Inneres sowie den behördlichen Datenschutzbeauftragten wurde in der bewährten Weise fortgeführt.

Aus- und Fortbildung

Im Berichtsjahr wurde erneut eine Vielzahl von Aus- und Fortbildungswünschen an uns herangetragen. Lehraufträge an den Berliner Universitäten, Veranstaltungen bei den Fortbildungseinrichtungen des Landes oder Unterrichtsbesuche an Schulen stellen nur einen kleinen Ausschnitt der übernommenen Verpflichtungen dar.

Hervorzuheben ist, daß die hierfür erforderlichen Nebentätigkeiten von den Mitarbeiterinnen und Mitarbeitern in der Freizeit durchgeführt werden. Im Gegensatz zu anderen Verwaltungen sehen wir uns z. B. nicht in der Lage, die Durchführung von Lehraufträgen an der Fachhochschule für Verwaltung und Rechtspflege als Arbeitszeit anzuerkennen.

6.5 Öffentlichkeitsarbeit

Wie in den vergangenen Jahren, haben wir der Öffentlichkeitsarbeit auch in diesem Berichtszeitraum eine besondere Bedeutung beigemessen. Neben Stellungnahmen unserer Dienststelle zu aktuell diskutierten Fragen des Datenschutzes lag der Schwerpunkt in diesem Bereich in der Erstellung und Herausgabe von Informationsmaterialien.

„Berliner Informationsgesetzbuch"

Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil gefordert, die Verarbeitung personenbezogener Daten in der öffentlichen Verwaltung normenklar zu regeln. Der Berliner Gesetzgeber hat diese Forderung im Berliner Datenschutzgesetz konsequent umgesetzt und die Datenerhebung, aber auch andere Formen der Datenverarbeitung durch Behörden und sonstige öffentliche Stellen des Landes Berlin unter den Vorbehalt einer Erlaubnis durch eine spezialgesetzliche Rechtsgrundlage gestellt.

Aufgrund von vielen Nachfragen haben wir uns entschlossen, nacheinander die wichtigsten Regelungen in einer praktikablen, aber nicht zuletzt im Hinblick auf die Haushaltslage einfachen Form allen Interessenten zugänglich zu machen. Die dadurch entstehende Sammlung von Einzelheften trägt die Bezeichnung „Berliner Informationsgesetzbuch".

Das erste Heft dieser Reihe enthält den Text des Berliner Datenschutzgesetzes in der neuesten Fassung und ist in unserer Dienststelle erhältlich. Die Texte des Bundesdatenschutzgesetzes sowie der wesentlichen Gesetze im Bereich der Sicherheit und Ordnung, des Sozialwesens, des Bildungswesens und anderer Verwaltungsbereiche werden in unregelmäßigen Abständen folgen.

Datenschutz bei Telekommunikation und Medien

Die Datenschutzbeauftragten haben sich bereits sehr frühzeitig auf nationaler und internationaler Ebene mit den Datenschutzproblemen bei Telekommunikation und Medien befaßt und in ihren Konferenzbeschlüssen Forderungen zur datenschutzgerechten Gestaltung von Telekommunikationsnetzen und -diensten erhoben. Dem Berliner Datenschutzbeauftragten wurde der Vorsitz zu den zuständigen Arbeitskreisen übertragen.

Eine Sammlung der Beschlüsse dieser Arbeitskreise haben wir in unserer Schriftenreihe „Materialien zum Datenschutz" im Heft „Datenschutz bei Telekommunikation und Medien", das im Berichtszeitraum in seiner dritten Auflage erschienen ist, veröffentlicht.

Datenschutz in der Schule

Das Heft „Datenschutz in der Schule - Ein Leitfaden für Schuldatenschutzbeauftragte" wurde in die Reihe „Materialien zum Datenschutz" aufgenommen.

Im Bewußtsein des Spannungsfeldes zwischen Datenschutz und Schule fand sich unter dem Dach der DGB-Technologieberatung e. V. Berlin ein Kreis von Lehrern, Personalräten und Mitarbeitern von Schulämtern unter Beteiligung des Berliner Datenschutzbeauftragten zusammen, um über diese Problemstellung zu diskutieren.

Die Anregungen dieses „Runden Tischs zum Datenschutz an Schulen" sowie das vielfach an uns herangetragene Informationsbedürfnis zu diesem Thema haben uns veranlaßt, den Leitfaden zu erstellen.

136 vgl. Anlage 1
137 vgl. Anlagen zu 2
138 vgl. Anlage 3

Datenscheckheft

„Wie kann ich Auskunft über meine gespeicherten Daten erhalten? Bei welchen Stellen kann ich dies beantragen? Wie kann ich Akteneinsicht in über mich vorhandene Unterlagen bekommen? Wie die Berichtigung und Löschung meiner Daten erreichen?" - Dies sind einige der immer wiederkehrenden Fragen, mit denen sich betroffene Bürger an uns wenden.

Als ein wirkungsvolles Instrument zur praktischen Selbsthilfe hat sich in den vergangenen Jahren das von uns bereits im Jahr 1981 in seiner ersten Auflage herausgegebene sogenannte „Datenscheckheft" bewährt. In ihm sind Musterbriefe enthalten, mit denen die Bürger an Behörden und andere Stellen schreiben können, um ihre Datenschutzrechte auf diese Weise wahrzunehmen.

Aufgrund der anhaltenden Nachfrage sowie der Änderungen der relevanten Gesetze haben wir im vergangenen Berichtszeitraum ein gänzlich überarbeitetes und neu gestaltetes Datenscheckheft herausgegeben. In ihm sind z. B. Schreiben enthalten, mit denen die Zusendung von Werbematerial eingeschränkt werden kann, Schreiben, mit denen Auskunft und Akteneinsicht bei der Polizei, beim Verfassungsschutz und beim Landeseinwohneramt beantragt werden können, Schreiben, mit denen die Eintragungen im Telefonbuch oder die Speicherung von Telefonverbindungsdaten untersagt werden können. Angeregt durch Anfragen von betroffenen Bürgern haben wir zusätzlich Musterschreiben für Auskünfte über Daten, die von Stellen der ehemaligen DDR gespeichert wurden, in das Datenscheckheft aufgenommen.

Aufkleber zum Datenschutz 1993 - Ausschreibung eines Wettbewerbs zur Motivsuche unter Studenten der Hochschule der Künste Berlin

Im Rahmen unserer Öffentlichkeitsarbeit haben wir im vergangenen Jahr wiederum einen Aufkleber mit einem Motiv zum Themenbereich: „Datenschutz - Grundrecht auf informationelle Selbstbestimmung - Schutz der Privatsphäre" herausgegeben. Zur Motivsuche haben wir diesmal einen geschlossenen Wettbewerb unter Studenten der Berliner Hochschule der Künste ausgeschrieben. Unter den eingereichten Wettbewerbsarbeiten, die von Juni bis Oktober 1993 in einer Ausstellung im Foyer des Rathauses Schöneberg zu besichtigen waren, hat die Fachjury die Arbeit eines chinesischen Studenten mit dem 1. Preis prämiert. Sein Entwurf versinnbildlicht in einfachen Formen das Verhältnis von Daten und Datenschutz: Das Buch als klassischer Informationsträger und der Schriftzug „Daten" in leuchtender Computerschrift werden von einem „Schutzumschlag" umhüllt.

Mit dem pinkfarbenen Aufkleber kann alles gekennzeichnet werden, was dem persönlichen Datenschutz unterliegen soll. Eine Besonderheit beim diesjährigen Aufkleber ist, daß dieser beschrieben werden kann.

Auf einer Freifläche in der Mitte des Aufklebers ist Raum für individuelle Bemerkungen oder Notizen. Dadurch kann der Aufkleber z. B. zur Beschriftung von Aktenrücken, Heftern und Tagebüchern verwendet werden oder als Briefkastenaufkleber, Kofferanhänger usw. dienen.

Berlin, 16. März 1994

Dr. Hansjürgen Garstka

Berliner Datenschutzbeauftragter

Anlage 1

1. Rede des Berliner Datenschutzbeauftragten vor dem Abgeordnetenhaus am 16. September 1993

Das Berliner Datenschutzgesetz verpflichtet den Berliner Datenschutzbeauftragten, dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen.

Der Senat hat in Frage gestellt, ob diese Berichtspflicht auch die aktuelle Entwicklung des Bundesrechts und der Rechtsprechung umfaßt.

Dieser Bericht soll diesem Hause, den öffentlichen Stellen des Landes Berlin, aber auch dem Bürger einen Überblick darüber verschaffen, welche aktuellen Probleme es bei der Umsetzung des Datenschutzes im jeweiligen Berichtsjahr gegeben hat. Dieser Überblick wäre unvollständig, würde er nicht entsprechende Hinweise enthalten, da sie ja in entscheidendem Maße die Verwaltungsabläufe prägen. Ich denke im übrigen auch, daß gerade Berlin als Bundeshauptstadt - auch was das Bundesrecht angeht - eine herausgehobene Stellung hat. Das bedeutet, daß Berlin Bundesrecht durchaus beeinflussen sollte - und zwar positiv im Sinne der informationellen Selbstbestimmung und nicht nur zum Abbau datenschutzrechtlicher Barrieren wie jüngst auf dem Gebiet der Sozialhilfe.

Der Datenschutz im Land selbst stand 1992 im Zeichen spezialrechtlicher Gesetzgebung: Ein Auftrag, den dieses Haus selbst mit dem Berliner Datenschutzgesetz im Jahre 1990 schuf, war einzulösen. In einer gewaltigen Kraftanstrengung wurden Gesetze zur Regelung der Datenverarbeitung geschaffen: Neben der seit langem überfälligen Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetz (ASOG) sowie des Verfassungsschutzgesetzes, der Verabschiedung von Rechtsgrundlagen für die Datenverarbeitung in Justiz und Statistik wurden in einem Artikelgesetz über 25 Einzelgesetze geändert. Als letztes großes Projekt steht lediglich die Archivgesetzgebung aus, deren Verabschiedung aber ebenfalls bevorsteht. Erst danach kann endgültig über das Schicksal so brisanter Datensammlungen wie Akten aus der Aufarbeitung der nationalsozialistischen Vergangenheit, mancherlei Hinterlassenschaft der DDR, aber auch tausender ausgesonderter Unterlagen des Landesamtes für Verfassungsschutz entschieden werden.

Bei einer Reihe von Bestimmungen im ASOG, im Verfassungsschutzgesetz und im Ausführungsgesetz zum Gerichtsverfassungsgesetz ist dieses Haus nicht den Empfehlungen des Berliner Datenschutzbeauftragten gefolgt, sondern hat anderen Belangen höheres Gewicht beigemessen. Dies ist das zu akzeptierende Ergebnis einer Güterabwägung des Gesetzgebers.

Allerdings hätte ich erwartet, daß gerade bei besonders umstrittenen Bestimmungen von der Verwaltung Vorgehensweisen gewählt werden, die der informationellen Selbstbestimmung möglichst großzügig Rechnung tragen. Die Erfahrungen in den ersten Monaten nach Inkrafttreten der Gesetze haben diese Hoffnung leider nicht überall bestätigt. Wenn bei der Polizei nach Inkrafttreten des ASOG nach anfänglichen formalen Bereinigungen die Anzahl der unverdächtigen Personen, über die Daten gespeichert werden, etwa im Bereich der Prostitution, nicht absank, sondern erheblich anstieg, wenn das Landesamt für Verfassungsschutz die Voraussetzung des besonderen Interesses für die Geltendmachung des Auskunftsanspruchs dahingehend interpretierte, daß die Betroffenen aufgefordert wurden, sich selbst zu extremistischen Betätigungen zu bekennen, oder wenn sich die Justizverwaltung weigerte, bei der Mitteilung von Räumungsklagen an die Sozialämter im Einzelfall die Erforderlichkeit zu prüfen und damit auch Daten über Bürger übermittelte, die gar nicht bedürftig sind, ist dies nicht das bürgerorientierte Verständnis, das ich erwartet hätte.

Zum Umgang mit Daten aus der DDR zwei Anmerkungen: Für die Verwaltung und Sicherung der Unterlagen, die in Millionenhöhe in den staatlichen medizinischen Einrichtungen angefallen waren, sind Regelungen gefunden worden. Über die Verwendung eines nur auf die ehemalige PKZ und die notwendigsten Personendaten beschränkten Abzugs des ehemaligen Zentralen Einwohnerregisters (im übrigen werden die Daten vernichtet) müssen die Gesetzgeber befinden: Diese von den Datenschutzbeauftragten der neuen Länder und Berlins schon immer vertretene Position mußte allerdings erst vor Gericht durch einen Vergleich erzwungen werden. Der übrige Bestand wird vernichtet.

Die Details unseres Berichts werden in dem zuständigen Unterausschuß Datenschutz des Ausschusses für Innere Sicherheit und Ordnung dieses Hauses zu erörtern sein. Ich möchte mich an dieser Stelle für den Ernst und das Engagement bedanken, mit dem dort Fragen der informationellen Selbstbestimmung erörtert werden.

Die heutige Gelegenheit möchte ich für einen Ausblick nutzen:

Informationstechnisch befindet sich das Land Berlin in einer Phase, in der die Informationstechnik nicht nur durch landesweite Großprojekte etwa in den Bereichen der Sozialhilfe, des Personalwesens oder des Haushaltswesens, sondern auch durch eine Neuorientierung der Datenverarbeitung in den Bezirksämtern im Rahmen des Modellbezirksamtes sowie hunderte kleinere abgegrenzte Automationsprojekte geradezu sprunghaft von der Landesverwaltung Besitz nimmt. Diese Entwicklung wird auch für unsere Arbeit Konsequenzen haben müssen.

Erhebliche Folgen für den Datenschutz wird der zunehmende Trend zur Privatisierung oder zumindest zur Entkameralisierung mit sich bringen: Es zeichnet sich ab, daß unter dem Stichwort „Outsourcing" auch auf dem Gebiet der Datenverarbeitung bedeutende und teilweise auch sensible Datenbestände privaten Auftragnehmern überantwortet werden. Diese Entwicklung muß erneut die Frage aufwerfen, ob die bestehende und dem Bürger ohnehin nicht verständlich zu machende Zersplitterung der Datenschutzkontrolle in den Datenschutzbeauftragten für öffentliche Stellen einerseits und die Aufsichtsbehörde für den Datenschutz bei der Innenverwaltung andererseits noch angemessen ist. Dies ist umso fraglicher, als die möglicherweise noch Ende diesen Jahres in Kraft tretende EG-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr eine einheitliche unabhängige Kontrollinstanz vorsieht.

Das Artikelgesetz sieht vor, daß in Rechtsverordnungen klar geregelt wird, welche Daten über den Bürger im einzelnen verarbeitet werden dürfen. Nach deren Erlaß bis Ende des Jahres wird Berlin dasjenige Land sein, in dem der Bürger auf vorbildliche Weise bereits durch Lektüre von Gesetz und Verordnungen erfahren kann, welche Daten öffentliche Stellen des Landes erheben, verarbeiten oder weitergeben. Der Forderung des Bundesverfassungsgerichtes nach Normenklarheit wird dadurch in außerordentlicher Weise Rechnung getragen.

Vor diesem Hintergrund erscheint mir die Position des Senats wenig verständlich, daß § 6 des Datenschutzgesetzes, der derartige klare Regelungen vorschreibt, wieder aufgeweicht werden sollte. Damit würden diejenigen Verwaltungen bestraft, die bereits jetzt die erwünschte Transparenz hergestellt haben - und dies ist ein Großteil der Ressorts. Dies schließt selbstverständlich nicht aus, daß es Sachverhalte gibt, bei denen die Umsetzung Schwierigkeiten macht. Für den Bereich des Bundesrechts, der bisher umstritten geblieben ist, haben wir einen Vorschlag gemacht, der unter Aufrechterhaltung des § 6 einen bundeskonformen Vollzug ermöglicht; für Querschnittsbereiche, die in jeder Verwaltung gleichermaßen auftreten, kann durch eine Anreicherung des in diesem Jahr ebenfalls in Kraft getretenen Informationsverarbeitungsgesetzes Abhilfe geschaffen werden.

Ich kann nicht schließen, ohne eine Bemerkung zum Atmosphärischen zu machen: Berichtet wird eingangs der Stellungnahme des Senats darüber, daß ich bei der Übergabe meines Berichtes dem Regierenden Bürgermeister bestätigen konnte, daß in der Grundtendenz das Verhältnis von Kooperation geprägt ist; dies wurde in den vergangenen Jahren auch in der Art und Weise deutlich, wie der Datenschutzbeauftragte berichtet und der Senat Stellung genommen hat. Dies wurde in anderen Ländern stets positiv zur Kenntnis genommen. In diesem Jahr bekam ich verwunderte Anrufe von Kollegen, die nach Lektüre der Stellung-

nahme des Senats nicht ohne Häme darauf hinwiesen, daß der Ton in Berlin wohl auch nicht mehr der alte sei. In der Tat beherrscht die diesjährige Stellungnahme des Senats ein Unterton, der dahin mißverstanden werden könnte, die informationelle Selbstbestimmung genieße nicht mehr den Stellenwert, den sie in den vergangenen Jahren in der Berliner Verwaltung hatte.

Ich hoffe, dies ist in der Tat ein Mißverständnis: Berlin hat in Sachen Datenschutz einen guten Ruf zu verlieren.

Anlage 2

2. Stellungnahmen und Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

2.1 Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 15. April 1993 zum Entwurf eines Gesetzes zur Umsetzung des Föderalen Konsolidierungsprogramms - FKPG - (Bundesrats-Drucksache 121/93 vom 5. März 1993)

Der Gesetzentwurf sieht Regelungen vor, die eine mißbräuchliche Inanspruchnahme von Sozialleistungen verhindern sollen und von erheblicher datenschutzrechtlicher Bedeutung sind.

Über die bisher gesetzlich vorgesehene Einzelfallprüfung hinaus würde durch den Gesetzentwurf ermöglicht, daß insbesondere die Daten aller Sozialhilfeempfänger, also auch derjenigen, bei denen kein Anhaltspunkt für falsche Angaben oder Verletzungen von Mitteilungspflichten besteht, ohne weiteres pauschal mit den Datenbeständen der Renten- und der Arbeitslosenversicherung abgeglichen werden. Darüber hinaus soll nach dem Regierungsentwurf der Online-Abruf von Daten aus einer unbegrenzten Vielzahl von Dateien anderer Verwaltungsbereiche ohne Rücksicht auf die jeweilige Sensibilität dieser Daten möglich sein.

Im Bereich der Arbeitslosenversicherung soll die erst zum 1. Januar 1993 in Kraft getretene, datenschutzgerechte Vorschrift über die Erhebung von Daten bei Außenprüfungen ohne erkennbaren sachlichen Grund durch eine Vorschrift ersetzt werden, die wichtige Grundsätze des Persönlichkeitsschutzes nicht berücksichtigt.

Im einzelnen weisen die Datenschutzbeauftragten - unter Einbeziehung der Empfehlungen der Ausschüsse des Bundesrats vom 8. April 1993, Drs. 121/2/93 - auf folgendes hin:

Artikel 9 Nr. 29 (§ 117 Bundessozialhilfegesetz - BSHG -)

1. **§ 117 Abs. 1 BSHG**

   Nach der Begründung zu § 117 Abs. 1 BSHG (Regierungsentwurf) - allerdings nicht nach dem Wortlaut der Vorschrift - soll der Leistungsmißbrauch über einen *Datenabgleich* mit der Bundesanstalt für Arbeit (BA) und der gesetzlichen Rentenversicherung aufgedeckt werden. Irgendein Anlaß für diesen Datenabgleich muß nicht gegeben sein. Ein solches, die Glaubwürdigkeit aller Sozialhilfeempfänger in Zweifel ziehendes Vorgehen ist allenfalls dann verhältnismäßig und damit vertretbar, wenn *verifizierbare Erkenntnisse* darüber vorliegen, daß ein erheblicher Anteil der Sozialhilfeempfänger der schon jetzt bestehenden Verpflichtung, den Sozialhilfeträgern Leistungen der BA und das Eingehen von Beschäftigungsverhältnissen mitzuteilen, nicht nachkommt. Der Gesetzesbegründung lassen sich solche Feststellungen nicht entnehmen.

   Die Zwecktauglichkeit dieses Abgleichs erscheint zudem zweifelhaft, da etwa Nebeneinkünfte von Sozialhilfeempfängern, für die keine Sozialabgaben entrichtet wurden, auch der Sozialversicherung nicht bekannt sind.

   Die Ausschüsse des Bundesrates haben nunmehr empfohlen, von dem pauschalen Datenabgleich abzusehen, sowie eine Zweckbindungs- und eine Löschungsregelung einzuführen. Die Datenschutzbeauftragten begrüßen diese Empfehlung.

2. **§ 117 Abs. 2 BSHG**

   Die Bundesratsausschüsse haben empfohlen, § 117 Abs. 2 BSHG des Regierungsentwurfs, insbesondere wegen der Unklarheiten des Gesetzestextes, zu streichen. In der Begründung verweisen sie auf die Regelungen von Datenübermittlungen aus anderen Verwaltungsbereichen in den jeweiligen bereichsspezifischen Vorschriften.

   Die Datenschutzbeauftragten begrüßen die Empfehlungen der Bundesratsausschüsse schon wegen der fehlenden Normenklarheit des Regierungsentwurfs.

Artikel 13 Nr. 20 (§§ 150 a und 150 b Arbeitsförderungsgesetz - AFG -)

a) Es ist unverständlich, daß die Neuregelung der §§ 19 a und 132 a Abs. 1 a AFG, die erst am 1. Januar 1993 in Kraft getreten sind, schon wenige Monate danach wieder aufgehoben und durch neue Regelungen ersetzt werden sollen. Gegen eine solche Notwendigkeit spricht auch die einschlägige Presseinformation der BA vom 18. März 1993, in der betont wird,

   „. . . die von Jahr zu Jahr zunehmende Zahl der aufgedeckten Verstöße zeige, daß das rechtliche und administrative Instrumentarium immer besser greife."

b) Entgegen der in den §§ 132 a Abs. 1 a und 19 a AFG enthaltenen Regelung sieht § 150 a AFG keinen Datenkatalog dahingehend mehr vor, welche Daten im Rahmen der Prüfungen zulässigerweise erhoben werden können. Weil in den in § 150 a AFG zu regelnden Fällen Unverdächtige in den Datenabgleich einbezogen werden, ist es erforderlich, den Eingriff auf das unbedingt notwendige Maß zu beschränken. Dazu ist weiterhin erforderlich, daß im ersten Schritt nur die hierfür unbedingt notwendigen Daten abgeglichen werden. Der Datenkatalog ist umso dringender, als die neue Vorschrift über Außenprüfungen nach § 150 a AFG eine Erweiterung gegenüber den bisherigen Vorschriften bringt.

c) Es ist ferner unerläßlich, daß die erhobenen Daten auch weiterhin der derzeit in § 132 a Abs. 1 a Satz 3 AFG nomierten - Zweckbindung unterliegen.

d) § 150 a Abs. 5 AFG erweitert die nach dem geltenden Recht bestehende Auskunftspflicht von Arbeitgeber und Arbeitnehmer auf *jedermann*. Dies erscheint überzogen, nachdem im Bereich der Datenerhebung für Steuerzwecke eine Auskunftspflicht Dritter nur besteht, „wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziel führt oder keinen Erfolg verspricht" (§ 93 Abs. 1 AO).

2.2 Entschließung der 45. Konferenz am 16./17. Februar 1993 zur Richtlinie des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt (30/313/EWG)

Im Interesse eines wirksamen Umweltschutzes hat der Ministerrat der Europäischen Gemeinschaft die Umweltinformationsrichtlinie erlassen, die jedem Bürger ein Recht auf Zugang zu den bei Behörden vorhandenen Informationen über die Umwelt gewährt. Da es nicht gelungen ist, die Richtlinie innerhalb der vorgegebenen Frist bis Ende 1992 in deutsches Recht umzusetzen, herrscht gegenwärtig Rechtsunsicherheit bei Bürgern und Behörden über den Zugang zu Umweltinformationen.

Die Konferenz der Datenschutzbeauftragten sieht in der Gewährleistung eines freien Zugangs zu Umweltinformationen einen wesentlichen Beitrag zu größerer Transparenz des Verwaltungshandelns. Informationsfreiheit und Datenschutz bilden dabei keinen unlösbaren Gegensatz. Die Konferenz hält es für geboten, die Arbeit am Entwurf des Umweltinformationsgesetzes (UIG) zügig zum Abschluß zu bringen. Sie begrüßt entsprechende Initiativen auf Landesebene.

In den Gesetzen sind folgende datenschutzrechtliche Grundsätze zu berücksichtigen:

Soweit Umweltinformationen auf Personen beziehbar sind, ist das Grundrecht auf informationelle Selbstbestimmung zu beachten. Deshalb sind Informationen grundsätzlich in anonymisierter oder aggregierter Form zu geben. Wenn damit das Informationsinteresse nicht erfüllt werden kann, sind Eingriffe in das Persönlichkeitsrecht nur unter klaren gesetzlichen Voraussetzungen zulässig, welche die Rechte, insbesondere die Verfahrensrechte, der Betroffenen wahren.

2.3 Entschließung der 46. Konferenz am 26./27. Oktober 1993 gegen die Stimme Bayerns und bei Stimmenthaltung Sachsens zu regelmäßigen Datenübermittlungen an die öffentlich-rechtlichen Rundfunkanstalten und die Gebühreneinzugszentrale (GEZ)

Die öffentlich-rechtlichen Rundfunkanstalten drängen seit langem auf die Schaffung einer Rechtsgrundlage für die regelmäßige Übermittlung von Meldedaten aller Einwohner an die gemeinsame Gebühreneinzugszentrale (GEZ). Sie verweisen dazu auf bereits bestehende Regelungen in den Ländern Hessen und Nordrhein-Westfalen. Auf Bitten der Konferenz der Regierungschefs der Länder hat deshalb nunmehr der zuständige Arbeitskreis der Innenministerkonferenz einen Musterentwurf für eine bundesweite Lösung im Melderecht erarbeitet. Der Entwurf sieht vor, daß künftig alle Meldebehörden in der Bundesrepublik im Fall der Anmeldung, Abmeldung oder des Todes eines volljährigen Einwohners bis zu acht Kerndaten an die GEZ übermitteln dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen eine derartige Regelung insbesondere aus folgenden Gründen ab:

Die Regelung könnte im Ergebnis zu einem bundesweiten Melderegister bei Volljährigen führen. Sie könnte außerdem gegen das verfassungsrechtlich garantierte Verhältnismäßigkeitsprinzip verstoßen. Den Rundfunkanstalten stünde möglicherweise der unkontrollierte Zugriff auf Millionen personenbezogener Daten volljähriger Einwohner der Bundesrepublik zu, obwohl es für die Rundfunkanstalten nur von Interesse ist, welcher Einwohner bei ihnen gebührenpflichtig ist und bislang seine Gebührenpflicht nicht angemeldet hat. Das vorgesehene generelle Übermittlungsverfahren kennt keine Unterscheidung zwischen erforderlichen und nicht erforderlichen Daten, sondern überläßt diese Unterscheidung der GEZ. Über die Frage, ob ein Volljähriger überhaupt gebührenpflichtig ist, geben die Meldedaten keine Auskunft. Das muß nach wie vor im herkömmlichen Verfahren durch Befragung ermittelt werden.

Die Datenschutzbeauftragten des Bundes und der Länder sind bereit, an geeigneten und verfassungskonformen Lösungen der Landesregierungen zur Sicherung des Gebührenaufkommens der Rundfunkanstalten mitzuwirken.

2.4 Entschließung der 46. Konferenz am 26./27. Oktober 1993 zum Datenschutz bei der Privatisierung der Deutschen Bundespost Telekom und bei der europaweiten Liberalisierung des Telefonnetzes und anderer Telekommunikationsdienste

Im Zuge der sogenannten Postreform II soll die Deutsche Bundespost Telekom - nach der dafür notwendigen Änderung des Grundgesetzes - in Form einer Aktiengesellschaft privatisiert werden. Zugleich hat der Ministerrat der Europäischen Gemeinschaften in seiner Entschließung vom 22. Juli 1993 (Amtsblatt der EG Nr. C 213 vom 6. August 1993) seine Entschlossenheit bekräftigt, die Monopole im öffentlichen Sprachtelefondienst (Festnetz) der Mitgliedstaaten bis zum 1. Januar 1998 zu beseitigen.

In absehbarer Zeit werden daher in Deutschland neben der „Telekom AG" auch im Telefondienst andere private Unternehmen Telekommunikationsdienstleistungen anbieten. Diese Privatisierung hat Konsequenzen für den Datenschutz, der bisher für die Deutsche Bundespost Telekom auf einem vergleichsweise hohen Niveau geregelt ist. Insbesondere das grundgesetzlich garantierte Fernmeldegeheimnis würde für private Netzbetreiber und Diensteanbieter jedenfalls nicht mehr unmittelbar gelten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für unabdingbar, daß durch die Privatisierung und Liberalisierung der Schutz der Bürger insbesondere in solchen Bereichen nicht verringert wird, die - wie der Telefondienst - der Daseinsvorsorge zuzurechnen sind. So wie bisher die konkurrierenden privaten Betreiber der Mobilfunknetze einen gleichmäßig hohen Datenschutzstandard gewährleisten müssen, hat dies auch zu gelten, wenn in Zukunft private Unternehmen im Wettbewerb miteinander stationäre Telefonnetze betreiben und entsprechende Dienste anbieten. Die Einhaltung von datenschutzrechtlichen Bestimmungen bei Telekommunikationsnetzen und -diensten muß zukünftig von einer unabhängigen Stelle nach bundesweit einheitlichen Kriterien und von Amts wegen kontrolliert werden können.

Da der Wettbewerb zwischen privaten Netzbetreibern und Diensteanbietern nicht nur national begrenzt, sondern im europäischen Binnenmarkt stattfinden wird, sind auch Rechtsvorschriften der Europäischen Gemeinschaften erforderlich, die einen möglichst hohen, einheitlichen Datenschutzstandard in der Telekommunikation gewährleisten.

2.5 Entschließung der 46. Konferenz am 26./27. Oktober 1993 zur Gewährleistung des Datenschutzes bei der Mobilkommunikation

Die Verbreitung mobiler Sprach- und Datenübertragungsdienste hat in jüngster Vergangenheit stark zugenommen. So gibt es bereits jetzt in Deutschland mehr als eine Million Teilnehmer der Funktelefonnetze C und D; mit der Aufnahme des Regelbetriebs von MODACOM ist seit Juni dieses Jahres auch ein öffentlicher mobiler Datenübertragungsdienst in Deutschland verfügbar. Es ist zu erwarten, daß sich die Teilnehmerzahl mobiler Kommunikationsdienste in Zukunft weiter vergrößern wird.

Die mit der Nutzung von Mobilfunkdiensten verbundenen Vorteile gehen mit Gefährdungen für den Datenschutz einher. Neben den auch bei anderen Telekommunikationsdiensten gespeicherten Angaben, wer wann mit wem in Verbindung war, wird bei der Mobilkommunikation auch erhoben, wo sich der mobile Teilnehmer jeweils aufhält. Die Speicherung dieser Daten ermöglicht die Bildung von problematischen Bewegungsprofilen.

Darüber hinaus ist vielfach auch die Vertraulichkeit der Kommunikationsinhalte gefährdet, insbesondere dann, wenn Daten unverschlüsselt per Funk übertragen werden. Dies gilt sowohl für die analogen Funktelefon-Netze B und C als auch für den von der Deutschen Bundespost Telekom betriebenen mobilen Datenübertragungsdienst MODACOM. Bei satellitengestützten Diensten ist es sogar möglich, die übertragenen Daten im gesamten, teilweise viele tausend Quadratkilometer umfassenden Abstrahlbereich des Satelliten unbemerkt abzuhören und aufzuzeichnen.

Von den Herstellern und Betreibern mobiler Kommunikationsdienste ist zu fordern, daß sie diesen Gefahren für das Fernmeldegeheimnis und für den Datenschutz durch eine entsprechende Gestaltung entgegenwirken und technische Vorkehrungen für eine sichere Kommunikation treffen.

Die Teilnehmer mobiler Kommunikationsdienste müssen von den Anbietern, Herstellern und Betreibern über die mit der Nutzung verbundenen Risiken und das erreichte Sicherheitsniveau aufgeklärt werden. Sofern bei bestimmten Diensten Sicherheitsmerkmale realisiert sind - wie z. B. in den digitalen D-Netzen -, muß die Sicherheit für die Aufsichts- und Kontrollorgane auch nachprüfbar sein. Falls durch den Dienstbetreiber nicht die erforderliche Sicherheit gewährleistet werden kann, ist eine Übertragung personenbezogener oder sonstiger sensibler Daten mit dem jeweiligen Dienst nur dann vertretbar, wenn der Benutzer zusätzliche Sicherheitsvorkehrungen trifft, also z. B. die übertragenen Daten anwendungsseitig verschlüsselt.

Zusätzlich kompliziert wird die Datenschutzproblematik bei der Mobilkommunikation dadurch, daß unter Umständen bei verschiedenen Dienst- und Netzbetreibern, aber auch bei anderen Unternehmen - den sogenannten Service-Providern, die lediglich Dienste vermarkten -, personenbezogene Daten gespeichert werden.

Hier muß im Zuge der anstehenden Überarbeitung des Telekommunikationsrechts dafür Sorge getragen werden, daß sich die Verarbeitung der Kommunikationsdaten auf das wirklich erforderliche Maß beschränkt und daß die Nutzer darüber aufgeklärt werden, bei welcher Stelle welche personenbezogenen Daten gespeichert oder sonst verarbeitet werden.

Besonders problematisch ist es, wenn bei der internationalen Mobilkommunikation auch in solchen Staaten personenbezogene Daten gespeichert werden, in denen kein ausreichendes Datenschutzniveau gewährleistet ist oder in denen das Fernmeldegeheimnis nicht sichergestellt wird. Deshalb ist es erforder-

lich, auf internationaler Ebene Regelungen zu treffen, die den Datenschutz bei mobilen Kommunikationsdiensten gewährleisten.

Die Konferenz unterstreicht aus diesem Grunde ihre Forderung, die Arbeiten an der EG-Richtlinie über Datenschutz im ISDN und in öffentlichen digitalen Mobilfunknetzen zu einem datenschutzrechtlich befriedigenden Abschluß zu bringen. Auch für den noch gänzlich datenschutzrechtlich ungeregelten Bereich der Satellitenkommunikation müssen endlich völkerrechtlich verbindliche Regelungen getroffen werden.

2.6 Entschließung der 46. Konferenz am 26./27. Oktober 1993 zur Gefährdung der Vertraulichkeit der Funkkommunikation von Sicherheitsbehörden und Rettungsdiensten

Durch die Aufhebung der bisher gültigen Beschränkungen der zulässigen Empfangsbereiche für Rundfunkempfänger zum 30. Juni 1992 werden zunehmend Empfangsgeräte betrieben, die das Abhören des Funkverkehrs ermöglichen. Dies stellt eine erhebliche Bedrohung des Fernmeldegeheimnisses dar.

Die Datenschutzbeauftragten des Bundes und der Länder beobachten die damit verbundene Gefährdung der Vertraulichkeit der Funkkommunikation von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) mit Sorge. Sie erkennen die Bemühungen der Polizeiverwaltungen der Länder an, durch zusätzliche technische Maßnahmen die Sicherheit des Sprechfunkverkehrs zu erhöhen. Sie stellen jedoch fest, daß die erforderliche Vertraulichkeit bisher nicht gewährleistet werden konnte. Auch Sprachverschleierungssysteme erreichen diese nicht hinreichend.

Daher begrüßt die Konferenz die im Rahmen des Schengener Abkommens getroffene grundsätzliche Entscheidung, im BOS-Bereich eine europäische Normierung zu erarbeiten, die die Digitalisierung und eine Verschlüsselung des BOS-Funkverkehrs vorsieht.

Die Konferenz hält es für erforderlich, daß das Normierungsverfahren so zügig wie möglich durchgeführt wird und auch schon vor der Umsetzung dieser Norm alle Möglichkeiten für einen effektiven Schutz der Vertraulichkeit des BOS-Funkverkehrs entsprechend dem jeweiligen Stand der Technik genutzt werden.

Die Konferenz weist weiter darauf hin, daß nicht nur bei den Behörden der Polizei, sondern auch in anderen BOS-Bereichen, wie z. B. dem Rettungswesen, eine Vertraulichkeit des Funkverkehrs zu gewährleisten ist. Daher sind auch in den übrigen BOS-Bereichen frühestmöglich entsprechende Absicherungen zur Vertraulichkeit des Funkverkehrs gefordert.

2.7 Entschließung der 46. Konferenz am 26./27. Oktober 1993 zum Integrierten Verwaltungs- und Kontrollsystem (InVeKoS) (Verordnungen der EWG Nrn. 3508/92 und 3887/92)

Die vom Ministerrat der EG 1992 beschlossene Reform der gemeinsamen Agrarpolitik sieht die Angleichung der gemeinschaftlichen Preise für bestimmte Kulturpflanzen an den Weltmarkt vor und gewährt auf Antrag als Ausgleich für die dadurch bedingten Einkommenseinbußen flächen- und tierbezogene Zuwendungen an die Erzeuger. Zur Verhinderung einer mißbräuchlichen Verwendung von Fördermitteln hat die EG die Mitgliedsstaaten dabei zur Einführung eines „Integrierten Verwaltungs- und Kontrollsystem (InVeKoS)" verpflichtet. Diese haben danach integrierte Datenbanken mit Angaben über Flurstücke, deren kulturartige Nutzung sowie den Tierbestand einzurichten und in einem Mindestumfang entsprechende Kontrollen durchzuführen.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder hat die EG mit dem „Integrierten Verwaltungs- und Kontrollsystem" den Landwirtschaftsverwaltungen der Länder ein Überwachungssystem verordnet, das dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot, widersprechen kann. Insbesondere legt das EG-Recht für die Kontrolldichte nur ein Mindestmaß an Kontrollen, jedoch keine Obergrenze fest.

Zur Vermeidung unverhältnismäßiger Einschränkungen des informationellen Selbstbestimmungsrechts der betroffenen Landwirte fordern daher die Datenschutzbeauftragten des Bundes und der Länder,

- ortsunabhängige Überwachungsmöglichkeiten (Fernerkundung mittels Satellit oder Flugzeug) nicht für eine flächendeckende Totalüberwachung einzusetzen, sondern auf den von der EG geforderten Stichprobenumfang zu beschränken;
- bei der Nutzung des Kontrollsystems InVeKoS und der darin gespeicherten personenbezogenen Daten den Grundsatz der Verhältnismäßigkeit und insbesondere der Zweckbindung zu beachten;
- nur dezentrale Datenbanken in den einzelnen Bundesländern einzurichten (keine Euro- oder Zentraldatenbank über Landwirte!), und an zentrale Datenbanken keine personenbezogenen Daten zu übermitteln;
- zu beachten, daß die EG-Verordnungen zu InVeKoS keine Rechtsgrundlage für eine Erweiterung der Nutzungen enthalten (z. B. zu Kontrollzwecken bei anderen landwirtschaftlichen Förderungsmaßnahmen oder außerhalb des landwirtschaftlichen Bereichs, z. B. zur Besteuerung).

2.8 Entschließung der 46. Konferenz am 26./27. Oktober 1993 zu kartengestützten Zahlungssystemen im öffentlichen Nahverkehr

Mit der Weiterentwicklung von Chipkarten werden kartengestützte Zahlungssysteme zunehmend auch im Verkehrsbereich eingesetzt. Damit besteht die Gefahr, daß sehr detaillierte Bewegungsprofile entstehen, die den persönlichen Bereich jedes Einzelnen einschränken und z. B. auch für Strafverfolgungsbehörden, Finanzämter und für die Werbewirtschaft von Interesse sein könnten. Da sämtliche Fahrten für einen gewissen Zeitraum aufgelistet werden können, hat jeder Kontoinhaber die Möglichkeit, Fahrten sämtlicher Familienmitglieder jederzeit nachzuvollziehen.

So sind im öffentlichen Nahverkehr zahlreiche sogenannte Postpaid-Verfahren in Erprobung, bei denen dem Fahrgast am Monatsende die aufsummierten Fahrpreise vom Konto abgebucht werden. Diese Zahlungsweise erfordert die Speicherung umfangreicher personenbezogener Daten: Neben der Konto-Nr. und Bankleitzahl des Fahrgastes werden sowohl Datum und Uhrzeit des Fahrscheinkaufs bzw. des Fahrantritts als auch Automatennummer und Preisstufe der jeweiligen Fahrt erhoben.

Eine solche Vorgehensweise ist umso problematischer, als technische Alternativen existieren, die weitaus datenschutzfreundlicher sind. Im öffentlichen Nahverkehr können - wie skandinavische und auch deutsche Projekte aufzeigen - Wertkartensysteme eingesetzt werden, bei denen im voraus bezahlt wird und die daher gänzlich ohne personenbezogene Daten auskommen.

Die Datenschutzbeauftragten halten es daher für dringend erforderlich, daß mehr als bisher bei der Einführung kartengestützter Zahlungssysteme darauf geachtet wird, die „datenfreie Fahrt" zu ermöglichen. Im öffentlichen Nahverkehr sollte weiterhin auch die datenschutzfreundlichste Lösung angeboten werden: Der Kauf einer Fahrkarte am Automaten mit Bargeld.

Die Konferenz fordert weiter, daß noch vor der Pilotierung der dargestellten Technikvorhaben im Verkehrsbereich eine Untersuchung möglicher Alternativen, eine Analyse der von ihnen ausgehenden Gefahren für das informationelle Selbstbestimmungsrecht und eine Darstellung der technischen und organisatorischen Möglichkeiten zur Gewährleistung des Persönlichkeitsschutzes zu erstellen ist (Technikfolgen-Abschätzung). Nur Verfahren mit dem geringsten Eingriff in das allgemeine Persönlichkeitsrecht sollten eine Chance zur Erprobung erhalten.

Anlage 3

3. Bericht der Arbeitsgruppe Telekommunikation und Medien an die 15. Internationale Konferenz der Datenschutzbeauftragten in Manchester (27. bis 30. September 1993)

Die Arbeitsgruppe hat im laufenden Jahr zwei Treffen abgehalten.

1.

Seit 1991 nimmt der Direktor des Instituts für Systemanalyse der Russischen Akademie der Wissenschaften, der für die Automatisierung der russischen Verwaltung zuständig ist, als Gast an den Treffen der Arbeitsgruppe teil. Während dieser Treffen hat er immer wieder auf die Wichtigkeit der Schaffung von Datenschutzregelungen insbesondere bei der Einführung neuer Telekommunikationsstrukturen hingewiesen.

Auf seine Initiative hin hat das Regierungskomitee für Informatisierung der Russischen Föderation die Arbeitsgruppe eingeladen, ihr Frühjahrstreffen vom 17. bis 19. Mai 1993 in Moskau abzuhalten.

Um die Arbeitsgruppe über die gegenwärtige Situation im Bereich der Automatisierung und Telekommunikation zu informieren, haben dort Experten von verschiedenen russischen Regierungsstellen und akademischen Institutionen Vorträge über die gegenwärtige Situation in ihren jeweiligen Bereichen gehalten. Die Berichte umfaßten

- den Fortschritt in der Russischen Föderation bei der Entwicklung von gesetzlichen Grundlagen für die Benutzung von Informationstechnologien;
- den Gesetzentwurf der Russischen Föderation über Information, Automatisierung und Informationssicherheit;
- die Entwicklung von Satellitenkommunikations- und Mobilkommunikationssystemen. (Diese Systeme spielen in Rußland eine besondere Rolle, da die existierenden Festnetze in sehr schlechtem Zustand sind).

Mitglieder der Arbeitsgruppe berichteten über

- Maßnahmen zur Datensicherheit in der Telekommunikation;
- Regelungen zur Datensicherheit in Westeuropa;
- Nachrichtenstandards, Sicherheit und rechtliche Aspekte des elektronischen Datenaustausches (Electronic Data Interchange - EDI);
- neuere Entwicklungen bei der Anwendung von Prinzipien der Datensicherheit auf Mobilkommunikationssysteme.

Die Diskussion mit den russischen Experten zeigte, daß das Bewußtsein für Datenschutzprobleme im Zusammenhang mit der schnellen Ausbreitung von Telekommunikationsnetzen und -diensten, die gegenwärtig in Rußland stattfindet, bisher wenig entwickelt ist.

Es ist daher dringend notwendig, die existierenden Initiativen im Bereich der Datenschutzgesetzgebung und die Anwendung von Datensicherungsmaßnahmen bei den sich ausbreitenden Telekommunikationsnetzen zu unterstützen. Vor diesem Hintergrund erklärte sich die Arbeitsgruppe bereit, Möglichkeiten zu prüfen, wie der Informationsaustausch über Datenschutzregelungen im Bereich der Telekommunikation mit dem Russischen Komitee für Informatisierung verbessert werden könnte.

Auf Wunsch der Vertreter des Russischen Komitees für Informatisierung und des Instituts für Systemanalyse der Russischen Akademie der Wissenschaften bot die Arbeitsgruppe fachliche Unterstützung bei aufkommenden Problemen in diesem Bereich an.

2.

Traditionsgemäß wurde die zweite Sitzung der Arbeitsgruppe in Berlin während der Internationalen Funkausstellung 1993 abgehalten (30. August 1993).

2.1

Die Privatisierung, Liberalisierung und Deregulierung von Telekommunikationsnetzen und -diensten findet in den meisten in der Arbeitsgruppe repräsentierten Ländern statt, wobei Geschwindigkeit und Ausmaß dieser Bemühungen differieren.

Aufgrund eines von uns erarbeiteten Fragebogens erhielten wir schriftliche Länderberichte aus Österreich, Belgien, Finnland, Frankreich, den Niederlanden, Norwegen, Portugal und Großbritannien. Die Vertreter Ungarns, Luxemburgs, Rußlands und Schwedens berichteten mündlich während des Treffens über die Situation in ihren Ländern. In den meisten westlichen Ländern, über die berichtet wurde, ist das allgemeine Datenschutzrecht sowohl auf den öffentlichen als auch auf den privaten Sektor anwendbar. Trotzdem haben bisher nur wenige Länder bereichsspezifische Regelungen erlassen, die die Speicherung und den Schutz von Verkehrsdaten, die in modernen Kommunikationsnetzen erzeugt werden, regeln.

Die Mitglieder der Arbeitsgruppe waren sich einig, daß Bürger, die Telekommunikationsnetze oder -dienste benutzen, unabhängig davon, ob die Netze oder Dienste von einer öffentlichen oder einer privaten Telekommunikationsorganisation betrieben werden, dasselbe Datenschutzniveau genießen sollen. Die Arbeitsgruppe sieht jedoch die Gefahr, daß die Privatisierung, Liberalisierung und Deregulierung dieser Märkte tatsächlich zu einer Absenkung des Datenschutzstandards führen könnte.

Es ist daher dringend notwendig, auf den Erlaß spezifischer gesetzlicher Regelungen zu dringen, die im Zusammenhang mit dem Wettbewerb zwischen Netzbetreibern und Dienstanbietern einen gleichmäßig hohen Standard des Datenschutzes für die Benutzer regeln. Darüber hinaus sollten für private und öffentliche Netzbetreiber und Diensteanbieter die gleichen Regelungen gelten.

2.2

Die Anwendung moderner Telekommunikationseinrichtungen zur Überwachung des Straßenverkehrs wird gegenwärtig in verschiedenen Ländern diskutiert. Die Überwachung des Verkehrs dient so unterschiedlichen Zwecken wie dem Flottenmanagement, der Wiederauffindung gestohlener Fahrzeuge sowie der Erhebung von Straßenbenutzungsgebühren. Diese Pläne lassen ernsthafte Bedenken bezüglich der damit verbundenen Datenschutzrisiken aufkommen.

Die Mitglieder der Arbeitsgruppe für Telekommunikation und Medien waren sich darüber einig, daß solche Pläne nur dann umgesetzt werden sollten, wenn gleichzeitig wirksame Maßnahmen gegen diese Risiken getroffen werden. Insbesondere sollte die Erstellung von Bewegungsbildern einzelner Verkehrsteilnehmer ausdrücklich verboten werden.

Die Arbeitsgruppe wird die weitere Entwicklung auf diesem Gebiet gründlich untersuchen und sich dabei insbesondere um die Findung alternativer Technologien kümmern, die besser im Einklang mit den Prinzipien des Datenschutzes stehen.

2.3

Darüber hinaus wurden erörtert

- Datenschutz im Bezug auf grenzüberschreitende Telekommunikation mit Mobiltelefonen („International Roaming");
- die Ausbreitung nationaler und internationaler Teilnehmerverzeichnisse in Forschungs- und sonstigen Telekommunikationsnetzen („X.500 directories");
- Mobilkommunikation in Luftfahrt und Verkehr.

Die Arbeitsgruppe wird diese Probleme auf ihren nächsten Sitzungen näher untersuchen.

Anlage 4

Abkürzungsverzeichnis

ABIDA	–	Automation der Ausbildungsstellen
ABM	–	Arbeitsplatzbeschaffungsmaßnahmen
ADIS	–	Abgeordnetenhaus-Dokumentations- und Informationssystem
ADV	–	Automatisierte Datenverarbeitung
AGGVG	–	Gesetz zur Ausführung des Gerichtsverfassungsgesetzes
AHW	–	Automatisiertes Haushaltswesen (Projekt)
ALB	–	Automatisiertes Liegenschaftsbuch
ALK	–	Automatisierte Liegenschaftskarte
AO	–	Abgabenordnung
APC	–	Arbeitsplatzcomputer
APW	–	Automatisierte Personalwirtschaft
ASOG	–	Allgemeines Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin (Allgemeines Sicherheits- und Ordnungsgesetz)
ASRG	–	Arbeitsschutzrahmengesetz
ASTA	–	ADV-Verfahren Amts- und Staatsanwaltschaften
AusReg	–	Ausländerregister
AUTISTA	–	Automation im Standesamt
AV-Schüler-unterlagen	–	Ausführungsvorschriften über die Führung schriftlicher Unterlagen über Schüler
BASIS	–	Berliner Automatisiertes Sozialhilfe Interaktions-System (Projekt)
BBG	–	Bundesbeamtengesetz
BBesG	–	Bundesbesoldungsgesetz
BDSG	–	Bundesdatenschutzgesetz
BGB	–	Bürgerliches Gesetzbuch
BGBl.	–	Bundesgesetzblatt
BImschG	–	Bundesimmissionsschutzgesetz
BlnDSG	–	Berliner Datenschutzgesetz
BOS	–	Behörden und Organisationen mit Sicherheitsaufgaben
BOWI	–	Bußgeld und Verkehrsordnungswidrigkeiten
BOWIDA	–	Bodenwirtschaftliche Datei
BR-Drs.	–	Bundesrats-Drucksache
BRRG	–	Beamtenrechtsrahmengesetz
BT-Drs.	–	Bundestags-Drucksache
BVG	–	Berliner Verkehrsbetriebe
COISTRA	–	Computer-Integriertes Strafverfahren
DateiRegVO	–	Dateienregisterverordnung Berlin
DCL	–	Dezentrale Computer-Leistung (Besteuerungsverfahren)
DV	–	Datenverarbeitung
DVO-MeldeG	–	Durchführungsverordnung zum Meldegesetz
EU	–	Europäische Union
EWW	–	ADV-Verfahren Einwohnerwesen
f.	–	folgende Seite
ff.	–	folgende Seiten
FIS	–	Fachübergreifendes Informationssystem (Projekt)
FISCUS	–	Föderales Integriertes Standardisiertes Computer-Unterstütztes Steuersystem
FÜDA	–	Führerscheindatei (Projekt)
GEWDAT	–	Gewerbedatenbank
GEZ	–	Gebühreneinzugszentrale
GIBES	–	Grundlagen der Ausstattung mit IT-Infrastruktur für die Bezirks- und Senatsverwaltungen (Infrastruktur-Projekt)
GSD	–	Gesellschaft für Systemforschung und Dienstleistungen im Gesundheitswesen
GMBl.	–	Gemeinsames Ministerialblatt
GVBl.	–	Gesetz- und Verordnungsblatt
HdK	–	Hochschule der Künste
IMPFBÜ	–	ADV im Impfbüro (Projekt)
INPOL	–	Informationssystem der Polizei
INVENT	–	Inventarisierung des IT-Gerätebestandes
IPV	–	Integrierte Personalverwaltung (Projekt)
ISVB	–	Informationssystem Verbrechensbekämpfung
IT	–	Informationstechnik
IuK-...	–	Informations- und Kommunikations-...
IVG	–	Informationsverarbeitungsgesetz Berlin
I. v. m.	–	In Verbindung mit
JUKOS	–	ADV-Verfahren Justizkosten
KpS-Richtlinien	–	Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen
KVA	–	ADV-Verfahren Kraftverkehrsamt
LADG	–	Landesantidiskriminierungsgesetz
LAN	–	Local Area Network - lokales Netz
LBG	–	Landesbeamtengesetz
LEA	–	Landeseinwohneramt
LfVG	–	Gesetz über das Landesamt für Verfassungsschutz
LGG	–	Landesgleichstellungsgesetz
LID	–	Lehrerindividualdatei
LIT	–	Landesamt für Informationstechnik
LIV	–	Lehrer-Informations- und Verwaltungssystem (Projekt)
LVwA	–	Landesverwaltungsamt
MAN	–	Metropolitan Area Network - stadtweites Netz
MBA	–	Modellbezirksamt (Infrastrukturprojekt)
MfS	–	Ministerium für Staatssicherheit der ehemaligen DDR
OWA	–	Ordnungswidrigkeitenverfahren Autowrackbeseitigung
PC	–	Personalcomputer
SAZ	–	Service- und Administrationszentrum (Infrastruktur-Projekt)
SFB	–	Sender Freies Berlin
SGB	–	Sozialgesetzbuch
SIS	–	Senatsinformationssystem
SMD	–	Sozialmedizinischer Dienst
StaLa	–	Statistisches Landesamt
StPo	–	Strafprozeßordnung
StudDatVO	–	Studentendatenverordnung
StUG	–	Stasi-Unterlagen-Gesetz
WAN	–	Wide Area Network - Weitbereichsnetz
ZIS	–	Zollinformationssystem

Anlage 5

Auszug aus dem Geschäftsverteilungsplan des Berliner Datenschutzbeauftragten

Stand: 1. Januar 1994

Berliner Datenschutzbeauftragter

Dr. Hansjürgen Garstka

Sekretariat

Birgit Münch

Bereich Recht und Verwaltung

Bereichsleiter, Vertreter des DSB für den Bereich und für AV; Datenschutzrecht; nationale und internationale Kooperation;

GB: Abgeordnetenhaus, Senatskanzlei, Bundes- und Europaangelegenheiten, Rechnungshof

Dr. Alexander Dix

GB: Gesundheit; Jugend und Familie; Kulturelle Angelegenheiten; Soziales

QB: Schutz von Gesundheits- und Sozialdaten

Dr. Ulrich von Petersdorff

GB: Schule, Berufsbildung und Sport; Wissenschaft und Forschung; Umweltschutz

QB: Forschung und Statistik

Dr. Rainer Metschke

GB: Arbeit und Frauen; Eigenbetriebe

QB: Personaldaten; Beratung von Personalräten

Birgit Saager

GB: Medien und Telekommunikation

Diplom-Informatiker Sven Mörs

Allgemeine Verwaltung, Büroorganisation, Haushaltsplanung und -bewirtschaftung

Diplom-Verwaltungswirtin Doris Werth

Allgemeine Verwaltung, Personalsachbearbeitung

Dagmar Klossek

Rechnungsstelle, Sekretariat

Monika Klössing

Sekretariat

Marion Werth

Bereich Bürger und Öffentlichkeit

Bereichsleiterin; Vertreterin des DSB für den Bereich; Konzeption und Durchführung der Öffentlichkeitsarbeit

GB: Landesamt für Verfassungsschutz

Claudia Schmid

GB: Finanzen; Justiz; Wirtschaft und Technologie; Verkehr

QB: Rechtspflege

N. N.

Redaktion von Veröffentlichungen

GB: Bau- und Wohnungswesen; Inneres; Stadtentwicklung

Volker Brozio

Bürgerberatung und -betreuung

GB: Landeseinwohneramt, Bezirksämter

QB: Geschäftsordnung

Detlef Schmidt

Sekretariat

Sabine Krissel

Bereich Technik und Organisation

Bereichsleiter; Vertreter des DSB als Dienststellenleiter und für den Bereich;

QB: Grundsatzfragen der ADV-Organisation und -technik und ihrer Entwicklung

Diplom-Informatiker Hanns-Wilhelm Heibey

SG: Großrechner mit proprietären Betriebssystemen

Diplom-Physiker Achim Laß

Koordination der technisch-organisatorischen Beratung; Beratung der behördlichen Datenschutzbeauftragten; Dateien- und Geräteregister

Jürgen Horn

SG: Systeme unter UNIX und seinen Derivaten; Rechner- und Kommunikationsnetze

Diplom-Informatikerin Ursula Meyer zu Natrup

SG: PCs, lokale Netze, nicht automatisierte Datenverarbeitung

Diplom-Verwaltungswirt Arne Kubla

Systemverwaltung

Andre Drescher

Sekretariat

Nicole Müller

GB: Geschäftsbereiche
QB: Querschnittsbereiche
SG: Sachgebiete
DSB: Datenschutzbeauftragter

Stichwortverzeichnis

Angegeben sind die Fundstellen aller Jahresberichte seit 1979. Die Ziffern ohne Jahreszahl beziehen sich auf den Zusammendruck der Jahresberichte in den von mir herausgegebenen Materialien zum Datenschutz, Band 2, Datenschutz in Berlin 1979 bis 1983. Die Ziffern mit den Jahreszahlen von 1983 bis 1989 beziehen sich auf die jeweiligen Drucksachen des Abgeordnetenhauses, ab 1990 auf die von mir herausgegebene Broschüre des jeweiligen Jahresberichts.

Abfall 1986/26; 1992/121; 1993/19
Abgabenordnung 1988/9; 1993/60
Abgangskontrolle 104
Abgeschlossenheitsbescheinigung 1993/58
Abgeordnetenhaus 14, 121; 1984/28; 1985/17; 1986/28; 1987/30; 1988/34; 1989/40; 1990/96; 1992/145
Abgeordnetenhaus-Informationssystem (ADIS) 1988/14; 1991/23; 1992/135, 138; 1993/31
ABIDA s. Ausbildungsstellen
Abiturienten 118
Ablichtung 42, 55, 87, 113
Abonnentenverwaltung 106
Abruf, unbefugter 76, 107; 1986/16
Abwasser 1990/83
Adoption 108, 109; 1985/4; 1986/6; 1987/27
Adrema-Platten 115
Adressenhandel 1991/9
Adressenmittlung 26; 1991/96; 1992/125
Adreßbuch 1985/6; 1989/26
Adreßlisten 58, 115
AdSoDi s. Soziale Dienste
ADV-Gesetz 1985/3, 26
ADV-Grundsätze 1984/18; 1993/26
ADV-Verfahren Einwohnerwesen (EWW) 1992/73
AdW s. Akademie der Wissenschaften
AHW s. Automatisiertes Haushaltswesen
AIDS 1987/3, 4, 19, 23; 1988/18; 1989/22; 1990/51; 1991/93; 1992/56
Akademie der Künste 1992/18; 1993/21
Akademie der Wissenschaften (KAI/AdW) 1991/86; 1992/18
Akademisches Auslandsamt 1990/28
Akten 25, 49, 58; 1990/93
Akten, Aufbewahrung 1986/16; 1987/28; 1988/21, 33; 1991/60
Akten, Vollständigkeitsprinzip 56
Akteneinsicht 25, 28, 50, 59; 1990/62, 78; 1991/5, 101, 102; 1992/69, 92, 96, 97; 1993/40, 80, 98
s. a. Einsichtsrecht
Akteneinsicht, Sozialgesetzbuch 59
Aktenführung 110; 1986/25; 1987/30; 1988/21; 1993/97
Aktenvernichter 1990/94
Aktenvernichtung 63; 1987/29; 1988/33, 41; 1990/52, 93; 1993/108
Altdaten der ehem. DDR 1993/17
Altersstudie 1990/88
Allgemeine Geschäftsbedingungen 1984/6
Allgemeine Ortskrankenkasse 1984/16
Allgemeines Sicherheits- und Ordnungsgesetz 107; 1984/3, 10; 1985/3, 7, 26, 27; 1986/16; 1987/22; 1988/4; 1990/59; 1991/19, 74; 1992/13, 59; 1993/67, 77, 78
allgemeine Verwaltungstätigkeit 1992/136
Alliierte 1987/5
Alternative Liste (AL) 1989/8
Altlasten 1986/26; 1987/30; 1990/82; 1991/115; 1993/54
Amerika-Gedenkbibliothek 85; 1984/28; 1986/16; 1991/107
Amtsanwaltschaft, s. Staatsanwaltschaft
Amtsarzt 1984/9; 1985/23; 1987/21; 1992/115
Amtsblatt, Dateiveröffentlichung 57
Amtsgeheimnis 55
Amtsgericht 54
Amtshilfe 25
Amt zur Regelung offener Vermögensfragen (AROV) 1991/105
Anonymisierung 34, 40, 51, 104; 1987/8
Anonymität der telefonischen Beratung 1991/43
Anordnung über Mitteilung in Strafsachen 40, 41, 44, 108; 1984/12, 24; 1985/3, 23; 1986/5, 1988/5; 1990/74; 1991/88; 1992/100; 1993/97
Anordnung über Mitteilungen in Zivilsachen 54; 1984/25; 1991/98; 1992/100; 1993/97
Anrufungen 9, 25, 32, 50, 89, 121; 1984/29; 1986/29; 1991/121
Anschriften 115
Anstaltszählung 1987/10
Antidiskriminierungsgesetz 1990/49, 86
s. jetzt Landesgleichstellungsgesetz
Anzapfen 77
APIS 1987/23; 1988/25
Arbeitsförderungsgesetz 1993/9, 125, 156
Arbeitgeber 1992/85
Arbeitskreis Europäische Gemeinschaft 1990/106
Arbeitsplatzcomputer 1986/3
Arbeitsrecht 1988/5
Arbeitsschutzrahmengesetz 1993/55
Arbeitssicherheitsgesetz 1990/84
Archive 46, 88, 106; 1984/3; 1985/11, 26; 1991/108; 1992/42, 124
Archivgesetz 1985/3; 1986/3, 4; 1987/4; 1988/5, 29; 1989/32; 1990/12; 1991/108; 1992/17; 1993/16, 84
Artikelgesetz 1992/14; 1993/16, 18
Asbest 1988/22
ASOG, s. Allgemeines Sicherheits- und Ordnungsgesetz
ASTA, s. Staatsanwaltschaft
Asylbewerber 1991/89; 1992/83; 1993/111
Asylverfahren 1986/7
Asylverfahrensgesetz 1992/5, 84
Aufenthaltserlaubnis 1991/86
Aufklärung bei der Erhebung 42
Aufsichtsbehörde für den Datenschutz 27, 45, 61, 64, 88, 120; 1984/29; 1985/24; 1986/29; 1987/30; 1989/40; 1993/23, 148
Autowrackbeseitigung 1993/33
Auftragsdatenverarbeitung 112; 1984/17; 1991/84; 1993/50, 51, 108
Ausbildungsförderung, s. Bundesausbildungsförderungsgesetz
Ausbildungsstellen 1993/32
Ausführungsgesetz zum Gerichtsverfassungsgesetz 1991/19; 1992/13, 96; 1993/67, 97, 106
Auskunft 25, 35, 52, 116; 1985/23; 1986/6; 1991/102; 1992/70; 1993/40
Auskunft, Gebührenpflicht 28; 1993/65
Auskunft, Sicherheitsbehörden 35; 1990/62
Auskunftssperre 108, 109; 1989/27
Auskunftsverweigerung 35
Ausländer 33, 53, 82, 117; 1991/86; 1993/106
Ausländerbeauftragte 1990/28
Ausländerbehörde 58, 111, 119; 1986/7; 1987/29; 1990/26; 1993/48
Ausländergesetz 1990/5, 26; 1991/87; 1992/83
Ausländerzentralregister 1987/36; 1989/28; 1991/89
Ausweisdaten 1992/64
Artikelgesetz 1991/20, 110, 117
AUTISTA s. Standesamt
Autobahnmaut, elektronische 1993/121, 139
Automatisiertes Fingerabdruckverfahren (AFIS) 1992/83
Automatisiertes Haushaltswesen (AHW) 1993/27
Automatisiertes Liegenschaftsbuch und -karte (ALB/ALK) 1993/31
Automatisiertes Sozial- und Jugendhilfe Interaktions-System (BASIS) 1991/111; 1992/116; 1993/27, 33, 34, 115
ärztliche Schweigepflicht, s. medizinische Daten

BABSY s. Beihilfe
BAföG, s. Bundesausbildungsförderungsgesetz
Bankauskünfte 1984/6
Bankdienste 1987/12
Banken, Bildschirmtext 60
BASIS s. Automatisiertes Sozial- und Jugendhilfe Interaktions-System
Basisdokumentation Psychiatrie 1984/9
Bau- und Planungsakten 73
Bau- und Wohnungswesen 116; 1988/16; 1990/40; 1991/65
Beamtenrecht 56; 1984/3, 9, 18; 1985/3, 26; 1986/3; 1992/5, 92
Beamtenversorgungsgesetz 72
Bebauungsplan 74
BEHALA 105
behördlicher Datenschutzbeauftragter 1991/140; 1993/50, 125

Beihilfe 1984/20; 1987/5; 1993/32
Beihilfeheft 1991/53
Belegfluß 54
Beliehene Unternehmen 1993/49
Benutzerdialog 1992/75
Benutzerkontrolle 86
Benutzerprofil 1990/91
Beratung 13, 26, 32, 43, 50, 64, 89, 121; 1984/29; 1986/29; 1991/121
Beratungsgeheimnis 1990/80
Beratungsstelle für Geschlechtskrankheiten 1992/55
bereichsspezifischer Datenschutz 28, 31, 45; 1984/3, 12; 1985/3, 26; 1991/20; 1992/14; 1993/18
Berichtigungsanspruch 35
BERKOM 1988/14; 1989/19
Berlin 2000 Marketing GmbH 1992/112
Berlin 2000 Olympia GmbH 1992/112
Berliner Altersstudie 1990/88
Berliner Datenschutzgesetz 24, 121; 1985/26; 1988/5, 1990/8; 1991/5, 18; 1992/134
Berliner Entwässerungswerke 105
Berliner Kammergesetz 1991/72
Berliner Pfandbriefbank 1985/16
Berliner Philharmonisches Orchester 106
Berliner Stadtreinigungsbetriebe 57; 1985/16; 1990/94; 1992/121
Berliner Wassergesetz 1992/120
Berliner Wasserwerke 105
Berufs- und besondere Amtsgeheimnisse 1993/53
Beschwerden s. Anrufung
Besonderes Dateienregister 1992/139
Besucherüberwachung 1991/100
Betriebsärzte 1990/84
Betriebsdatenbank 85; 1985/24
Betriebskrankenkasse des Landes und der Stadt Berlin 1984/17
Bewährungshilfe 1992/15; 1993/19
Bevölkerungsstatistikgesetz 1993/87
BEWAG 36
Bewegungsprofil 1992/133; 1993/36, 121, 139, 163
Beweisverwertungsverbot 1992/8
Bewerberverfahren 1991/34
Bewerbungsunterlagen 1990/80; 1991/52, 62
bezirkliche Personalverwaltung 1990/90
Bezirksämter 109, 116; 1984/16; 1985/16; 1986/23, 38; 1989/35; 1992/142
Bezirkseinwohneramt 54
Bezirksverordnetenversammlungen 15, 73; 1991/37
Bibliotheken 85, 105; 1985/11, 26; 1986/16, 24; 1990/86
Bibliotheksgesetz 1985/3; 1988/29; 1989/32
Bildberichterstattung 1993/133
Bildschirmtext 33, 37, 45, 59, 67, 75, 87, 101; 1984/12, 28; 1985/12; 1986/12; 1987/15; 1989/17
Bildschirmtext, Anbieter 1984/14; 1985/17; 1990/35
Bildschirmtext, Betreiber 1984/14
Bildschirmtext, externe Rechner 101
Bildschirmtext, Staatsvertrag 75, 88, 123; 1991/39
Bildschirmtext, Zustimmungsgesetz 101, 120
Blutspendedienst 1984/8
Bodenbelastungskataster 1991/115; 1992/120
s. auch Altlasten
Bodenschutzgesetz 1992/119; 1993/119
BOWIDA 1990/41; 1993/31
Brandenburg 1991/24; 1992/126, 146; 1993/22
Brandenburgischer Datenschutzbeauftragter 1992/18; 1993/22, 147
Breitbandkommunikation 59, 101; 1987/16; 1988/14
Briefumschläge, verschlossen 1992/107
Broschüren 27
BSI-Errichtungsgesetz 1990/19
Bundesamt für die Sicherheit der Informationstechnik 1990/19; 1991/14; 1992/22, 24
Bundesarchiv
s. Archive
Bundesausbildungsförderungsgesetz 63
Bundesbaugesetz 119
Bundesbeauftragter für die Unterlagen des Ministeriums für Staatssicherheit 1991/7; 1992/35; 1993/85, 91
Bundesdatenschutzgesetz, Novellierung 65, 88, 89, 120, 121; 1986/4; 1988/5, 12, 36; 1990/12, 105; 1991/5
Bundesgerichtshof 1992/8
Bundeshauptstadt Berlin 1991/4
Bundeskindergeldgesetz s. Kindergeld
Bundeskriminalamt 44
Bundessozialhilfegesetz 72; 1993/9, 155
Bundesstatistikgesetz 31; 1986/8; 1987/4; 1990/67
Bundesverfassungsgericht 1984/3; 1986/5; 1987/4; 1991/10; 1992/7, 128
Bundesverfassungsschutzgesetz 1990/105, 106; 1992/57
Bundeszentralregister, unbeschränkte Auskunft 40, 56, 88, 120; 1984/28
Bußgeldverfahren 1984/22; 1989/39
Bündelfunknetz Chekker 1990/32
Bürokommunikationssysteme 1988/3, 24; 1989/13; 1990/17
BVG 104; 1986/9; 1988/31; 1990/85; 1993/37, 51

CD-ROM 1992/131
Charité 1991/30
Chemikaliengesetz 1992/119
Chipkarte 1985/14; 1986/4; 1993/23, 35, 163
Client-Server-Architektur 1992/116; 1993/24
Codes 34, 60, 77, 101; 1984/6
COISTRA s. Staatsanwaltschaft
Computerkriminalität 1984/5; 1986/4; 1989/19
Computermißbrauch 1984/4
Cyberspace 1991/19; 1992/28

Datei 25, 31, 49, 55, 58; 1985/18; 1991/57; 1992/140
Dateienregister 12, 24, 26, 27, 30, 43, 57, 64, 86, 88, 105, 120, 121; 1985/24; 1986/29; 1987/30; 1988/34; 1989/41; 1991/57, 103; 1992/97, 137, 139; 1993/143
Dateienrichtlinien nach ASOG 1993/78
Datenangst 99
Datenaustausch, Bezirke 1992/116, 117
Datenaustausch Ost/West 1990/25
Datenbankabfragesprache 1992/118
Datenbeschreibungspflicht 1992/97
Datenerhebung, heimliche 1991/77
Datenfernübertragung 1992/73
Datengeheimnis 55
Datenscheckheft 50; 1993/150
Datenschutzbeauftragter, behördlicher 1991/57, 121; 1992/96, 141, 142
Datenschutzbeauftragter, Kontrollrechte 120; 1988/10; 1993/101
Datenschutzbeauftragter, Rolle 99; 1989/3
Datenschutzbeauftragter, Zuständigkeit 25
Datenschutzrichtlinie s. Europäische Datenschutzrichtlinie
Datenlöschungs- und -vernichtungsverbot 1991/84; 1992/72
Datenschutzprogramme 1990/89
Datensicherung bei manuellen Datensammlungen 114
Datensicherung 37, 42, 57, 58, 64, 93, 116; 1984/5; 1992/117, 118
Datenspeicher Wohnungspolitik 1991/28
Datenträgervernichtung 1990/93
Datenträgerverwaltung 1992/41
DATEX 1987/11
DDR 1990/68, 103, 104; 1991/6, 24; 1992/124, 146; 1993/17, 74, 89
Demonstrationsteilnehmer 1993/81
Denkmalschutz 1990/54
Deregulierung 1993/20
Deutsche Dienststelle s. WASt
Deutsche Klassenlotterie Berlin 85
Deutsche Oper Berlin 105
Deutsches Bibliotheksinstitut 105; 1991/107
Dezentralisierung 1986/3; 1988/3; 1989/36
Diagnosestatistik 1986/10; 1988/19
Dialogorientiertes Recherche- und Auskunftssystem (DORA) 1991/25
Dialogsysteme 1990/16
Dienststelle, Aufbau 16, 24, 33, 50, 121; 1991/120
digitale Telekommunikation 1991/7; 1992/127, 131
Digitalisierung 1988/12
Direkteinleiter 1992/120
Diskriminierung 1990/85; 1991/100
Disziplinarstelle 1988/24

Disziplinarverfahren 1992/64
DNA-Analyse s. Genomanalyse
Dokumentation 1984/6
DORA s. Dialogorientiertes Recherche- und Auskunftssystem
Downsizing 1992/21; 1993/24, 25
EDV-Politik 1990/17
EG-Arbeitskräftestichprobe 1984/23
EG-Kommission s. Kommission der Europäischen Gemeinschaft
EG-Statistikverordnung 1990/101
Ehescheidungsakten 1993/106
Ehrenausschüsse 1991/36
Eichgebühren 1992/79
Eigenbetriebe 104; 1993/19, 124
Eigentumsübertragungsansprüche 1991/105
Einbürgerung 1992/85
Einheitliche Patientendatenverarbeitung 63
Einigungsvertrag 1990/22; 1993/86, 91
Einkommensnachweise 1991/93
Einladungskarteien 105
Einsichtsrecht 25, 41, 59, 66, 100; 1985/20; 1993/40
Einsichtsrecht, medizinische Daten 100; 1986/11; 1987/18; 1988/5, 19
Einsichtsrecht, Schülerbogen 41
Einwilligung 24, 26, 31, 51, 57, 59, 67; 1985/22
Einwohnerwesen 1990/62; 1993/33
Einzelentgeltnachweis 1991/41; 1993/129
Elektronische Autobahnmaut s. Autobahnmaut
Elektronische Geldbörse 1993/37
Elektronische Post 1991/139
Elektronischer Lotse 1987/27
Elektronisches Telefonbuch 1987/16
ELSY, s. Einsatzleitsystem
Emissionskataster 1986/26; 1990/81; 1993/19
Entmündigung 1986/5; 1988/5
Einsatzleitsystem 1990/58
Einwohnerdatenbank, s. Melderegister
Embryonenschutzgesetz 1989/23; 1990/77
Epidemiologie, s. Forschungsprojekte
Erfolgskontrolle bei der Polizei 1993/72
Erforderlichkeit 25, 41, 58, 61; 1991/52
Erhebung 40, 51, 56, 110
erkennungsdienstliche Maßnahmen 1990/61; 1991/82; 1992/59, 84
erkennungsdienstliche Unterlagen 1984/11; 1990/61; 1991/78, 82
Ermittler, verdeckte 1991/76
Erziehungs- und Ordnungsmaßnahmen 1988/29
EUROCAT 50
Europa 1988/6, 12; 1990/14, 106; 1992/131, 132
Europarat 28, 46; 1985/3, 35; 1987/37; 1989/4; 1990/14; 1992/10
Europäische Datenschutzrichtlinie 1992/10; 1993/13
Europäische Gemeinschaft 28, 50; 1988/16, 12; 1989/4, 29; 1990/14, 100, 101, 106; 1991/8; 1992/131, 132
Europäische Union 1993/13
Europäischer Binnenmarkt 1992/9
Euroscheck 1987/13
Evaluation der Lehre 1992/123
externe Schreibkräfte 1984/9

Fahndung, Kraftfahrzeuge 79; 1992/66
Fahrerlaubnisakten 1992/80
Fahrerlaubnisregister, bundesweites 1993/122
Fahrscheinkontrolle 1993/51
Fahrzeugregister 1984/22; 1987/4
Falsch verstandener Datenschutz 1993/142
Familienbuch 1992/82
Familienkrankenhilfe 72
Fangschaltung 1992/7, 129, 130; 1993/137
Farbbänder 1988/42
Fehlbelegungsabgabe 72, 75; 1990/44
Fehleintragung 54
Fehlspeicherung 107
Fehlzeitenaushang 1993/91
Fehlzeitenerfassung 1991/55
Fehlzustellung 1987/29
Fensterbriefumschläge 43
Fernerkundung 1992/133
Ferngespräche, Erfassung, s. Telefondatenerfassung
Fernmeldeanlagengesetz (FAG) 1991/46; 1992/130; 1993/13, 130
Fernmeldegeheimnis 1990/108; 1992/7, 126, 128; 1993/83
Fernmeldeordnung 1984/12
Fernmeldesatelliten 1992/132, 133
Fernmeßdienste 1992/133
Fernwartung 63; 1985/34; 1986/15; 1990/74
Fernwirkdienste 101, 102; 1984/16; 1985/14; 1986/13; 1987/17; 1988/14; 1992/133
Feuersozietät 1984/16; 1993/21
Feuerwehr 79; 1993/132
Finanzämter 1990/45, 48; 1991/68
Finanzverwaltung 88; 1991/68
Fingerabdruckverfahren, automatisiertes 1991/89
Flughafen 1985/4
Flottenmanagement 1992/133; 1993/166
Föderales Konsolidierungsprogramm 1993/155
Formulare 26
Forschung 33, 50, 59, 61, 82, 87, 112, 117; 1987/25, 26, 37; 1988/19, 29; 1989/11, 22, 23, 33; 1990/78; 1991/117; 1992/108; 1993/126
Forschungsnetz 1987/12, 14
Forsten 1985/5
Fotos 1986/11
Frauenförderplan 1991/54
Frauenvertreterin 1990/86; 1991/54; 1993/56
Freiwilligkeit 1988/11, 21; 1991/118
Fremdenpaß 1992/86
Fremdfirmen 63, 84, 86
Friedhöfe 1985/5; 1992/15; 1993/19
FÜDA s. Führerscheine
Führerscheine 1988/30; 1993/33, 122
Führungsinformationen 1988/15
Führungszeugnis 57; 1987/28
Funk 42
Funksprechverkehr s. Sprechfunkverkehr
Funktelefon 1990/32
Funkbetriebszentrale der Polizei 1992/62
Funktionstrennung 86, 101, 114; 1984/6
Funktionsübertragung 1993/51

GASAG 36, 104
„Gauck"-Behörde s. Bundesbeauftragter für die Unterlagen des Ministeriums für Staatssicherheit
Geburtsdaten 41; 1985/18; 1986/6
Gebühreneinzugszentrale (GEZ) 1993/134, 158
Gebührenfreiheit bei Auskünften 1990/9
Gebührenpflicht bei Auskünften 28
Geldautomaten 1986/27
Geldwäschegesetz 1993/10
Gemeinsame Ermittlungsgruppe Schwarzarbeit (GES) 1992/50
Gemeinsame Geschäftsordnung für die Berliner Verwaltung 89, 106; 1985/3, 10
Gemeinsames Landeskriminalamt (GLKA) 1991/25
genetischer Fingerabdruck 1988/6; 1989/9, 12; 1990/76; 1992/101; 1993/99
Genomanalyse 1990/76, 102; 1992/102; 1993/55
Gentechnologie 1987/4; 1988/6; 1989/9
Geräteverzeichnis 1991/57
Gerichtsverfassungsgesetz 1991/102
Gesamtberliner Verfassung
s. Verfassung von Berlin
Geschäftsverteilungsplan 115
Gesetz über Abbau der Fehlsubventionierung, s. Fehlbelegungsabgabe
Gesetz über die Datenverarbeitung für Zwecke der räumlichen Stadtentwicklung 1992/120; 1993/119
Gesetz über psychisch Kranke 121; 1985/3
Gesetz zur Bekämpfung der illegalen Beschäftigung 1992/51
Gesetz zur Bekämpfung der Organisierten Kriminalität s. OrgKG
Gesundheitsakten 1992/51
Gesundheitsdaten, s. medizinische Daten
Gesundheitsdienstgesetz 1991/72
Gesundheitsstrukturgesetz 1992/6, 49
Gesundheitsstrukturreform 1988/5, 6, 37; 1989/22
GEWDAT, s. Gewerbedatenbank
Gewerbeanmeldung 1991/65
Gewerbeanzeige 1987/28
Gewerbedatenbank 1990/84; 1993/34

Gewerbeordnung 62, 87
Gewerberegister 31, 62, 87, 88
GGO, s. Gemeinsame Geschäftsordnung
GIBES s. Grundlagen der Ausstattung mit IT-Infrastruktur für die Bezirks- und Senatsverwaltungen
Glaubwürdigkeit kindlicher Zeugen 36
Gleitzeitbogen 1992/94
GLKA, s. Gemeinsames Landeskriminalamt
grenzüberschreitende Datenverarbeitung 1989/3, 4; 1991/8
„Großer Lauschangriff" 1992/56, 58, 69; 1993/6
Grundbuch 1987/24; 1991/105
Grundlagen der Ausstattung mit IT-Infrastruktur für die Bezirks- und Senatsverwaltungen (GIBES) 1993/29
Grundrecht auf Datenschutz 28; 1991/4; 1992/19 f.; 1993/8
Grundrecht auf Informationsfreiheit 1991/5
Grundrechte 30
Gruppenberechtigung 1990/90
GSD 1987/13; 1988/17; 1989/39

Hacking 1989/4; 1987/11
Häftlingsüberwachung 1991/101
Haftpflichtversicherung 1988/19
Handels- und Gaststättenzählung 1985/11; 1993/87
Handelsregister 1988/28; 1989/31; 1990/73
Handelsstatistikgesetz s. Handels- und Gaststättenzählung
Handfunkterminals 1989/25
HAREG, s. Handelsregister
Hausbesetzungen 80, 120
Hausbücher 1991/27
Haushaltsbegleitgesetz 100
Haushaltsstrukturgesetze 72
Haushaltswesen 1987/18; 1988/17; 1989/21
Herangabeanspruch nach Antragsrücknahme 1993/59
Herstellerfirmen 63
HIV, s. AIDS
Hochschularchiv 1992/124
Hochschuldaten-Verordnung 1992/122
Hochschulen 25, 32, 50, 57, 63; 1986/11; 1988/32; 1990/86; 1992/122 ff.; 1993/114
Hochschulgesetz 1986/22; 1989/33; 1990/86; 1991/118; 1992/122 f.
Hochschulstatistikgesetz 58; 1984/24; 1989/29, 34; 1990/87; 1992/122
Hotelmeldepflicht 1990/109
home-banking 60; 1987/12
HUK-Verband 1992/66
Humangenetik 1989/11
s. auch Genomanalyse

Identitätsfeststellung 1984/11
IDN 1987/11
illegale Beschäftigung, Bekämpfung 72
Immatrikulationszeiten 1993/114
Impfliste 1988/30
in-camera-Verfahren 90
Indienreise 1986/18; 1987/29
Industrie- und Handelskammer 45, 61; 1988/31
Information des Bürgers 27
Information des Datenschutzbeauftragten 26, 43, 64, 113
informationelles Selbstbestimmungsrecht 25; 194/3; 1990/5, 7, 59; 1991/4, 6, 14, 31; 1992/120, 131
Informationsfreiheitsgesetz 1990/10, 82; 1991/7
Informationsgesellschaft 49; 1989/3; 1991/4; 1992/19
Informationsgesetzbuch 1990/10
Informationsgleichgewicht 15, 30; 1990/11
Informationssicherheit 1990/15; 1991/8
Informationssystem Verbrechensbekämpfung 36, 79, 108; 1984/10; 1985/8; 1986/16; 1987/23; 1989/2; 1990/55; 1993/48, 70, 77
Informationsverarbeitungsgesetz (IVG) 1991/23; 1992/13, 135; 1993/31
Informationsverarbeitung, Entwicklung 49; 1988/3
Inkassobüro 1993/52
INPOL-System 44; 1985/8; 1992/66; 1993/33, 75
Institutionsleihe 44
Integrierte Personalverwaltung (IPV) 1993/27, 32, 93
intelligente Schnittstelle 1985/6

Internationale Fahndung s. Indienreise, Schengener Informationssystem, Schengener Übereinkommen
interner Datenschutzbeauftragter 105, 112, 116
internes Dateienregister 105
Intimbereich 39
Inventarisierung des IT-Gerätebestandes 1993/145
IOC s. Berlin 2000
IPV s. Integrierte Personalverwaltung
isolierte Rechner 63, 114; 1985/5; 1990/16
ISDN-Datenschutzrichtlinie 1991/47; 1993/138
ISDN 1986/3; 1989/5, 12, 47; 1990/14, 17, 29, 100, 108, 111; 1991/9, 40; 1993/137
ISVB, s. Informationssystem Verbrechensbekämpfung
IT-Gesetz 1991/22
IT-Sicherheitshandbuch 1991/16; 1992/25
IT-Sicherheitskriterien 1991/15; 1992/24
IuK-Datenbank 1992/140
IuK-Gesetz 1990/10; 1991/22
IuK-Politik 1990/18; 1993/23
IuK-Systeme 1991/56

Jubiläen 1986/22; 1987/29
Jugendamt 1993/95
Jugendgerichtshilfe 58, 110; 1993/95
Jugendgesundheitsdienst 1991/72
Justizmitteilungsgesetz 1987/24; 1991/98; 1993/97
Justizverwaltung 50, 60
Justizvollzugsanstalten 55, 81, 87; 1985/17; 1991/100; 1992/104 ff.; 1993/74

Kabelfernsehen 1990/111, 114
Kabelkommunikation 33, 37, 39, 46, 67, 102
Kabelpilotprojekt 101; 1984/15; 1985/3, 15; 1986/13; 1987/16; 1988/14; 1989/17, 18; 1990/35
Kabel-Pilotprojekt-Gesetz (KPPG) 1991/38, 40; 1992/126
Kaderpolitik 1990/20
KAI, s. Akademie der Wissenschaften
Kammergericht 1985/5
KAN, s. Kriminalaktennachweis
Kartentelefone 1991/138
Kassenarzt 1986/5, 10
Kaufpreissammlung 119; 1984/27; 1993/31
Kinder- und Jugendhilfegesetz 1990/14, 49; 1991/92
Kindergeld 72, 100; 1984/19
Kirchen 24, 27, 32
Kirchensteuer 1984/17; 1989/20; 1992/78
KITA-Kostenbeteiligungsgesetz 1991/92; 1993/20
Klassenliste 118
Kleingärtner 1993/120
Kleinrechner 84, 114; 1988/41; s. a. Personalcomputer
Klinische Nachsorgeregister 50
Klinisch-medizinische Analysen-Computer System (KLIMACS) 1992/56
Kommunikationsprofile 1991/46
Konfessionszugehörigkeit 1992/78
Konkurrentenklage 1993/90
Konsolprotokolle 63
Konten- und Gehaltspfändung 1988/9
Kontrollen von Amts wegen 11, 24, 25, 26, 32, 50, 68
Kontrollkompetenz 1990/13
Kontrollmitteilungen 1987/18; 1993/60
Konverter 102
Koordinierungsausschuß für innerstädtische Investitionen (KOAI) 1992/45
Koordinierungs- und Beratungsstelle für die Aufarbeitung der DDR-Vergangenheit in der Berliner Verwaltung 1992/33
Koordinierungsstelle Verwaltungseinheit (KVE) - Personalbörse - 1991/61
Kosten- und Behandlungsplan 110; 1984/9, 34
Kostenrechnung 1988/22
Kostenübernahme, Krankenhaus 1986/10; 1987/29
Kostenübernahmescheine 81
KPM 105
KPPG, s. Kabel-Pilotprojekt-Gesetz
KpS-Richtlinien 27, 43, 56, 79, 119; 1984/12, 27; 1993/76
Kraftfahrzeuge 25, 79

Kraftfahrzeughalter 1993/10, 77
Krankenakten, s. medizinische Daten
Krankenbett 1986/11
Krankengeschichtenverordnung 120; 1984/8
Krankenhausmeldepflicht 1990/109
Krankenhausstatistik 1988/19
Krankenhäuser 1987/13; 1993/129; s. a. medizinische Daten
Krankenkassen 1985/21; 1986/10
Krankentransport 1993/18
Krankenversichertenkarte 1992/50; 1993/38
Kreditkarte 1993/36, 122
Krebsregister 50, 88; 1984/8; 1990/50, 110; 1991/31
Kriminalaktennachweis 44
Kriminalpolizeiliche personenbezogene Daten, s. KpS-Richtlinien
Kriminalpolizeiliche Beratungsstelle 1987/24
krw 1987/13; 1988/17
kulturelle Einrichtungen 105

Landesabfallgesetz 1993/19
Landesamt für Elektronische Datenverarbeitung 62, 63; 1988/3; 1990/15
Landesamt für Informationstechnik 1991/23; 1992/140; 1993/26, 94
Landesamt für Verfassungsschutz s. Verfassungsschutz
Landesamt zur Regelung offener Vermögensfragen (LAROV) 1992/43; 1993/52
Landesantidiskriminierungsgesetz s. Landesgleichstellungsgesetz
Landesarchiv s. Archive
Landesbeamtengesetz 1993/88, 124
Landesbeauftragter für die Stasi-Unterlagen 1991/6; 1992/31; 1993/145
Landeseinwohneramt 1986/5; 1987/29; 1991/27
Landesgleichstellungsgesetz 1993/56
Landeskrankenhausgesetz 1984/3, 30, 70
Landesmeldegesetz 35, 45, 53, 64, 77, 107, 12; 1984/3, 2; 1990/63
Landespressegesetz s. Presse
Landesstatistikgesetz 10; 1984/3; 1987/2; 1988/5, 2; 1989/2; 1990/11; 1991/19, 90; 1992/13, 87; 1993/86
Landesversicherungsanstalt 1984/16
Landesverwaltungsamt 1990/68
Landeswahlordnung s. Wahlen
Landwirt, gläserner 1993/120, 162
Laptops 1990/35; 1991/18, 91
Lastschrifteinzug 1984/17
„Lauschangriff" s. „Großer Lauschangriff"
LED
s. Landesamt für Elektronische Datenverarbeitung s. Landesamt für Informationstechnik
Lehrerindividualdatei 11; 1986/2; 1990/78; 1991/110; 1992/111; 1993/34, 94, 111
Lehrer-Informations- und Verwaltungssystem (LIV) s. Lehrerindividualdatei
Leichenschauschein 188/22
Leistungsdaten
s. Schülerunterlagen
Lichtbildsammlung und -vorzeigekartei 1991/82
Liegenschaftskataster 7; 1984/1; 1990/41; 1991/66, 105; 1993/53
Liegenschaftskarte 1990/42
LIT
s. Landesamt für Informationstechnik
Lohnsteuerkarte 43, 54, 5; 1986/2; 1987/30
Lohnsteuerstellen 119
Löschungsanspruch 35; 1989/35
Löschungsfristen s. Prüffristen
Luftbildaufnahmen 1993/120

Maastricht, Vertrag von 1991/10; 1992/132; 1993/13, 138
MADB s. Makrodatenbank
Mahnverfahren 1987/25; 1990/74
Mail-box-Rechner 1988/15
Maklerlisten 1992/43
Makrodatenbank 1993/88
MAN (Metropolitan Area Network) 1993/25, 27
manuelle Datensammlungen 89, 91, 93, 112, 114, 117
Max-Planck-Gesellschaft 61, 87
Medienprivileg 8, 38, 65, 68; 1993/132
medizinische Daten 25, 27, 31, 40, 49, 63, 100, 112, 120; 1984/3, 7; 1985/20; 1986/10; 1987/14, 20; 1988/4, 19; 1989/22; 1990/84; 1991/71, 101, 117; 1992/53; 1993/53, 63, 66, 131
medizinisch-psychologische Gutachten 1992/80; 1993/12, 123
Mehrplatzsysteme 1990/17
Meldegesetz 35, 45, 53, 64, 77, 107, 121; 1984/3; 1985/3, 6, 26; 1986/3, 5, 39; 1988/27; 1989/26; 1990/62; 1992/40
Meldepflicht
s. Meldegesetz, Melderechtsrahmengesetz
Meldepflicht zum Dateienregister
s. Dateienregister
Melderechtsrahmengesetz 27, 31, 44, 100; 1985/26; 1990/109; 1991/26; 1993/136
Melderegister 54, 63, 64, 78, 87, 107; 1984/21; 1985/6, 23; 1986/5; 1988/10, 16, 26; 1992/73, 77; 1993/33
Menschenrechtskonvention 28
Michelangelo-Virus 1992/26
Mieterbefragung s. Mietspiegel
Mieterdaten 1993/113
Mieterlisten 73
Mietobergrenzen 1984/27
Mietspiegel 1988/16; 1989/19; 1993/58
Mietpreisstellen 73
Mikrochips 1992/121
Mikrocomputer 1984/18
Mikroverfilmung 1984/32; 1988/21, 42; 1990/47; 1993/60
Mikrozensus 1984/23; 1985/11; 1986/8; 1987/6, 20; 1989/28; 1990/67; 1991/91; 1992/90
Ministerium für Staatssicherheit 1990/20, 21
Mischverwaltung 44
Mißbrauch von Sozialleistungen 1993/6, 8, 9
MiStra
s. Anordnung über Mitteilungen in Strafsachen
Mithören 1991/11
Mitschneiden 1987/11
Mitteilungsverordnung 1993/61
MiZi
s. Anordnung über Mitteilungen in Zivilsachen
mobile Aktenvernichter 1990/94
Mobilfunk 1990/111, 113; 1992/131; 1993/13, 137, 159
Modellbezirksamt 1993/27, 28
Modellprogramm Psychiatrie
s. psychiatrische Daten
MS-DOS 1990/19; 1991/15, 18, 94; 1992/116
Müllgefäßidentifikation 1992/121
Museum für Verkehr und Technik 121

Namensänderung 1992/82; 1993/125
Nachrichtendienstliches Informationssystem (NADIS) 35; 1989/5, 7; 1991/85; 1992/73; 1993/84
Nebenstellenanlagen 1989/12; 1990/17, 34; 1991/11, 31, 48; 1993/31, 129
Nebentätigkeit 1986/11; 1987/29; 1988/23
Netze 1987/4, 11; 1990/17; 1991/18; 1992/21
Neue Medien 23, 37, 45, 59, 67, 75, 91, 100; 1984/12, 28, 30; 1985/31; 1986/12; 1987/15, 31; 1988/12; 198
Neue Medien, Grundsätze 64, 67; 1984/30
Neugliederungsstaatsvertrag 1993/22
nichteheliche Kinder 1988/26
Nomenklaturkader 1991/34
Normenflut 1992/17; 1993/21
Notare 87
Novellierung des Bundesdatenschutzgesetzes
s. Bundesdatenschutzgesetz

Oberfinanzdirektion 1987/8
OECD 28, 46
Öffentliche Lebensversicherung 1984/16
Öffentliche Wirtschaftsunternehmen 1984/16
Öffentlichkeit 1986/19; 1990/94; 1991/120
Öffentlichkeitsarbeit 33, 50, 89, 121; 1984/29
Olympia-Gegner 1993/70
Olympia GmbH
s. Berlin 2000
one-line-Anschlüsse 39, 49, 78, 84, 115
ONGUM 1987/13

Ordnungsmäßigkeit der Datenverarbeitung 114; 1991/96
Ordnungsmerkmal 53, 77; 1985/6
Ordnungsverwaltung 1986/5
OrgKG 1990/74, 107; 1991/47, 77, 97; 1992/4, 58, 100; 1993/98
Organisierte Kriminalität 1991/73
Organleihe 44
Orientierungsrahmen 1988/3; 1989/37
Ortszuschlag 1991/51; 1992/93; 1993/90
Orwell 99
Outsourcing 1993/24, 25

Parteien 1987/26; 1990/65
patientenbezogenes Leistungskonto 1992/49
Patientendaten 1990/84; 1991/6, 12; 1992/8, 50, 53
Patiententelefon 1993/129
Paß 126; 1986/4; 1987/3
Pay-per-View 1990/114
Pay-TV 102; 1985/15; 1987/16; 1988/14; 1989/18; 1992/133
PC-Netze 1990/17
Personalakten 26, 40, 67; 1984/18; 1986/20, 23; 1987/4, 5, 21, 39; 1988/23, 24; 1989/29; 1990/72; 1991/53, 89, 100; 1992/5, 91, 96; 1993/57, 88
Personalausweis 26, 31, 42, 55, 87, 106, 120, 126; 1985/6; 1986/5; 1987/3, 4; 1988/25, 26
Personalausweisgesetz 44, 100, 106; 1984/4; 1986/3
Personalbezügedatei 1984/24; 1988/22
Personalcomputer 1985/4, 32; 1986/3, 7, 14, 17; 1987/7, 22, 24; 1988/3, 22; 1989/15; 1990/15, 56, 89
Personaldaten 25, 32, 40, 45, 49, 56, 66, 67; 1984/9, 18; 1985/5, 18; 1986/3, 15, 20, 28; 1987/21; 1988/23, 29, 32; 1990/68; 1991/5, 49
Personalfragebogen 1984/19; 1990/68
Personalinformationssystem 1986/20; 1987/4
Personalrat 1985/19; 1986/21; 1989/31
Personalüberhangliste 1988/23; 1989/30; 1990/72
Personalvertretungsgesetz 1992/17, 92
Personalverwaltung 1990/90
Personalverzeichnis 41
Personenbeförderungsgesetz 62
personengebundene Hinweise 1988/26; 1989/25
Personenkennzeichen 53; 1984/4; 1990/22; 1991/29
s. auch PKZ/Personennahverkehr 1993/36
Persönlichkeitsprofil 39, 67, 68; 1991/105
Persönlichkeitsrecht 59, 73; 1991/5, 78, 90
Petitionsausschuß 1984/26; 1985/24; 1986/29
Pfändungen 1987/21
Pflegschaft 54
Pinnwand 1987/16
PKZ (Personenkennzahl) 1990/22; 1992/37, 40; 1993/85
Planung 51, 52, 59, 73; 1985/11
Planungsrecht 1992/48
Polizei, Ordnungsaufgaben
s. Allgemeines Sicherheits- und Ordnungsgesetz, Ausländerbehörde, Melderegister, Paß, Personalausweis
Polizei, Strafverfolgung
s. Fahndung, Informationssystem, Verbrechensbekämpfung, INPOL-System, KAN, KpS-Richtlinien, Strafverfolgung, Strafprozeßordnung
Polizeifunk 1992/126
Polizeiliche Beobachtung 1984/11; 1985/7; 1992/60
Polizeiliche Kriminalstatistik 1986/9
Polizeitechnische Untersuchungsstelle 1988/7; 1990/57
POS 1987/12
Postgeheimnis 1990/108; 1993/83
Postreform, zweite Stufe 1993/136
Poststrukturgesetz 1988/12, 39; 1989/17, 44
Postverkehr 43; 1986/25; 1987/28; 1989/38; 1990/94; 1991/64; 1993/139
Presse 1986/19; 1990/5; 1993/132
private Computernutzung 1984/18; 1986/24, 35; 1989/21; 1990/46, 72; 1991/109
private EDV-Unternehmen 84
private Sicherheitsdienste 1993/73
Privatisierung 1988/4, 17; 1990/24; 1993/49, 136, 165
Programmdokumentation 106, 114; 1990/91; 1991/56
Programmtests 86, 113
PROSOZ 1991/111; 1992/116
Prostituierte 1990/60; 1992/61, 67; 1993/74
Protokollierung 1988/27; 1991/105
Protokollisten 116
Prozeßordnungen 1984/25; 1985/22
Prüffristenverordnung 1993/69
Prüfrecht der Datenschutzbeauftragten 1990/13
psychiatrische Daten 53, 66; 1984/8; 1985/20
psychiatrisches Gutachten 41

Quellabzugsverfahren 57
Querulanten 1990/5

Rahmendienstvereinbarung über den Einsatz und den Betrieb von digitalen Telefonnebenstellenanlagen 1991/48
Rahmendienstvereinbarung über die Personaldatenverarbeitung 1991/49
Rahmenpläne für Schulen 1992/108
Rasterfahndung 33, 35, 43; 1984/11; 1990/74, 107; 1991/79, 98; 1992/101; 1993/10
Rauschgifthandel 1990/107
Razzien unter Hinzuziehung der Presse 1993/132
Reality-TV 1993/132
Rechenzentren, Funktionentrennung 114
Rechenzentrum 62, 114; 1986/27
Rechenzentrum, Datenträgerarchiv 86
Recht am eigenen Bild 1993/133
Recht am eigenen Wort 1991/11
Recht auf Nichtwissen s. Genomanalyse
regelmäßige Übermittlungen 1986/6, 39
Regierungs- und Diplomatenkrankenhaus 1991/30; 1992/52
Regionales Bezugssystem 1988/16, 21
Reichsversicherungsordnung 72; 1992/52
Reiseausweis für Flüchtlinge und Staatenlose 1992/86
Religionsgemeinschaften 24, 27, 32, 45, 64; 1989/27
remote station 62, 84
Rentenversicherungsnummer 1988/19
Rettungsdienstgesetz 1993/18
Richtlinie über den freien Zugang zu Informationen über die Umwelt 1992/12; 1993/15, 118, 157
Richtmikrophone 1992/101
Risikoanalyse 1992/138
road pricing s. Autobahnmaut
Rufname 1988/27
Rufnummernanzeige 1990/112; 1993/137
Rundfunkgebühren 81, 88; 1991/38; 1993/134
Rundfunkstaatsvertrag 1991/38; 1992/126
Rückkanal 102
Rückmeldeverfahren 1986/16; 1987/29; 26

Sachakte 1989/6; 1991/54
Sanierung 74; 1991/29
Satellitenfernsehen 37
Satellitenkommunikation 1992/132, 167; 1993/120
Schadensersatz 24, 28, 32
Scheinehe 1993/106
Scheinwohnung 1992/77
Schengener Informationssystem 1992/10
Schengener Übereinkommen 1989/25; 1990/14, 99; 1992/9; 1993/132
Schlüssel, Aufbewahrung 117
schnurlose Telefone 1993/130
Schufa 61; 1984/7; 1985/3; 1986/4, 5, 27; 1988/31; 1990/85; 1993/105
Schuldatenschutzbeauftragter 1991/109; 1992/141
Schuldatenverordnung 1993/109
Schuldnerverzeichnis 61; 1984/28; 1989/31; 1993/105
Schule, 25, 32, 36, 41, 50, 57, 87, 118, 120; 1984/28; 1985/5, 24; 1986/3; 1988/29; 1993/149
Schüler-Informationssysteme 1992/10
Schülerunterlagen 1986/3, 23; 1987/30; 1988/30; 1990/78, 80; 1991/110; 1992/107, 110; 1993/109
Schülerzeitung 1992/109
Schulfragebogen 36; 1992/109
Schulgesetz 1987/25; 1988/29; 1989/32; 1990/79; 1992/107
Schulgesundheitsdienst 1991/72
Schulpsychologischer Dienst 118; 1987/25, 40; 1988/34, 40; 1992/108
Schulstatistik 1993/110

Schulverfassungsgesetz 1990/79
Schutz des gesprochenen Wortes beim Telefonieren 1991/10
Schutzgemeinschaft für allgemeine Kreditsicherung s. Schufa
Schwangerschaftsabbrüche 1991/80; 1993/11, 61
Schwarzfahrer 1993/51
Schweigerecht 1992/8
Schweiz 65
Schwerbehinderte 1984/26
SED 1991/34
Selbstbezichtigung 1991/34; 1993/44
Selbsthilfeeinrichtungen 1984/26
Senatsinformationssystem (SIS) 1988/14
Sender Freies Berlin 24, 45; 1991/37
Seriennummer
s. Personalausweis
Sicherheit der Informationstechnik 1990/18; 1991/14; 1992/24
Sicherheitsgesetze 1986/30; 1988/4
Sicherheitssoftware 1990/89; 1991/61
Sicherheitsüberprüfungen 1987/22; 1993/79
SITA 1989/4
smart cards 1993/35
sonderpädagogisches Gutachten 1987/26
Sozialbericht 64
Sozialdaten
s. Sozialgesetzbuch X; 1991/5
Soziale Dienste 1990/73
Sozialgeheimnis
s. Sozialgesetzbuch X
Sozialgesetzbuch I, Mitwirkung (§ 60) 26; 1985/22; 1992/114
Sozialgesetzbuch V, 1989/22; 1992/49
Sozialgesetzbuch VIII 1991/92
Sozialgesetzbuch X 25, 26, 27, 31, 44, 50, 58, 64, 72, 81, 109; 1984/25; 1985/22; 1986/25; 1989/24; 1990/27, 48; 1992/114, 115
Sozialgesetzbuch X, Aktenführung 1984/25, 34; 1986/25
Sozialgesetzbuch X, Ausländer 100, 111
Sozialgesetzbuch X, Datenschutzbeauftragte 112
Sozialgesetzbuch X, Offenbarung für Forschung und Planung 59, 82; 1988/20
Sozialgesetzbuch X, Offenbarung für Strafverfahren 82, 100, 111; 1984/26; 1988/20; 1989/24
Sozialgesetzbuch X, Zweckbindung 83
Sozialhilfe, Ausländer 58, 82
Sozialhilfe 58, 87; 1988/20, 1990/52; 1992/114
Sozialhilfeantrag 1992/114
Sozialhilfestatistik 64; 1986/28
Sozialleistungsmißbrauch s. Mißbrauch von Sozialleistungen
Sozialleistungsträger 1984/16
Sozialmedizinischer Dienst 1993/62
Sozialpsychiatrischer Dienst 1989/22; 1993/65
Sozialversicherungsausweis 1988/5, 19
Sozialversicherungsnummer 1988/5, 19
Sozialwissenschaftliche Untersuchungen 33; 1988/18
Sparkasse der Stadt Berlin West 1984/16; 1988/31
speichernde Stelle 62, 109; 1986/24, 38
Speicherschreibmaschine 1993/143
Speicherverschlüsselung 1987/11
Sperrung 1984/22; 1985/6
Spezialgesetze
s. bereichsspezifische Regelungen
Sprachspeicherdienst 1987/16
Sprachverschleierungstechnik 1993/131
SPUDOK
s. Spurendokumentationssysteme
Spurendokumentationssysteme 1984/12; 1986/ 1; 1990/57
Sprechfunkverkehr der Sicherheitsbehörden 1993/131, 161
Staatsanwaltschaft 60, 64, 115; 1984/28; 1988/5, 27; 1990/72; 1993/33, 46, 103
Staatsdienst der DDR 1990/5
Stadtplanungsdatei 1990/81; 1992/120; 1993/19, 34, 119
stand-alone-Rechner 63
Standesamt 1993/32
Stasi 1990/20, 21; 1991/32 f.
Stasi-Unterlagen-Gesetz 1991/6; 1993/86, 92
Statistik 31, 59, 64, 102, 104; 1984/23; 1985/11; 1986/3; 1990/62, 66, 101; 1991/90
Statistikgeheimnis 1992/88, 122
Statistisches Informationssystem 1986/9; 1987/20; 1988/21; 1992/88
Statistisches Landesamt 1988/11; 1990/66, 87; 1991/91; 1992/122; 1993/19
Städtebauförderungsgesetz 74
Sterilisation 1986/10
Steuerdaten-Abrufverordnung 1990/46
Steuerfahndung 88
Steuerverwaltung 88; 1987/18; 1988/9, 17; 1989/20; 1991/68
Strafantragsrecht des Datenschutzbeauftragten 1993/101
Strafgefangene 1992/104, 106
Strafgesetzbuch, § 200, 81; 1989/32
Strafprozeßordnung 1984/10; 1986/4; 1987/24; 1988/4, 5; 1989/43; 1990/74; 1993/68
Straftaten 1988/29, 1990/57
Straftatenkatalog 1991/47, 76, 98; 1992/101; 1993/100
Straftatverdächtige 1992/60, 97
Strafverfahrensänderungsgesetz (StVÄG) 1990/74; 1991/97; 1992/98, 100; 1993/98
Strafverfolgung 37, 79; 1984/10
Strafvollzug
s. Justizvollzugsanstalten
Straßenbenutzungsgebühren s. Autobahnmaut
Straßensperre 1988/26
Straßenverkehrsgesetz 1987/4
Straßenverkehrsunfallstatistik 1990/67
Suchtgefahren 1992/30
„Südumfahrung Stendal" 1992/48
Studentendaten
s. Hochschulen
Studentendatenverordnung 1993/124
StUG
s. Stasi-Unterlagen-Gesetz
Subventionsbetrug 1993/11
Suizid 1987/20
SWIFT 1987/13; 1989/4
Synchronknoten 1986/15

Tageszeitung 1989/5
Taxifahrer 62; 1984/28; 1986/27
Taxi-Genehmigungsbehörde 1992/79
TDSV
s. Telekommunikationsdatenschutzverordnung
Technische Prüfstellen für den Kraftfahrzeugverkehr 64
Technische Universität Berlin 1990/28; 1991/117 f.; 1992/124
Teilhaber-/Teilnehmersysteme 1987/11, 14
Teilnehmerverzeichnisse für die Telekommunikation 1990/32; 1992/131
Telebus 1984/26
Teledienstunternehmen-Datenschutzverordnung (UDSV) 1992/127
Telefaxgeräte 1990/92; 1991/48
Telefon, Benutzung 42
Telefonbuch 1992/130
Telefonaufzeichnung 1986/5; 1988/33
Telefondatenerfassung 63, 87, 120; 1986/5; 1987/5; 1992/127
Telefonkarten 1990/31, 32
Telefonnebenstellenanlagen
s. Nebenstellenanlagen
Telefonnetz, Programmierpanne 1990/34
Telefonüberwachung 1990/77
Telekommunikation 1988/39; 1989/4, 46; 1990/29, 108, 111; 1991/40; 1992/127; 1993/128
Telekommunikationsdatenschutzverordnung (TDSV) 1991/40; 1992/8, 55, 127; 1993/130, 137
Telekommunikationsordnung 1986/14, 32; 1987/16; 1988/12
Telekopierer 1988/21
Telemarketing (Telefonwerbung) 1991/13, 48
Teletex 37, 38
Telex 1988/13
Testdaten 86, 113; 1984/18
Textverarbeitung 84, 85; 1985/5; 1989/36; 1993/54
Teilnehmerverzeichnisse 1990/112
Todesursachenstatistik 104; 1989/40
Tonbandaufzeichnung 1988/6
transeuropäische Netze 1993/138

Transparenz der Datenverarbeitung 30, 86, 104, 114; 1991/80; 1992/122
Transportkontrolle 86; 1992/74, 127
Trennungsgebot, Statistik 1993/87
Treuhandanstalt 1990/25; 1991/123

Umwandlung von Mietwohnungen 73; 1992/118; 1993/58
Umwelt-Informations-Gesetz 1991/7; 1992/118
Umweltschutz 1986/26; 1990/82; 1991/114
unbeschränkte Auskunft, s. Bundeszentralregister
UNESCO 46
Unfallstatistik 1987/28
Unfallversicherung 1992/52
Universitätsklinikum Steglitz 112
UNIX 1989/14, 48; 1990/16, 19, 91; 1991/15; 1992/43, 116
Unterhaltsansprüche 58; 1984/26; 1991/92; 1993/67, 96
Unterricht 1986/24
Unterrichtsbesuch 1993/57
Unterschriftenliste 55
Unterstützungsbetrug 1992/114
Urlaubsreise nach Indien 1986/18; 1987/29
USA 1984/6; 1991/9
Übergangsbonus 1987/22; 1988/4, 38; 1990/58
Übermittlung an nichtöffentliche Stellen 26, 31, 65, 121
Übermittlung nichtöffentlicher Stellen an Behörden 31
Überprüfung von Beschäftigten 1993/91
Überwachungstechniken 1990/108
Überweisungsträger 58, 81, 120

Verbindungsdaten 1990/113; 1992/128, 130; 1993/13, 137
Verbraucherkreditgesetz 1990/85
Verbraucherschutz 1991/43
Verbrauchssteuer-Binnenmarktgesetz 1992/6
verdeckter Ermittler 1992/101
Verfahrensdokumentation 114
Verfahrensentwicklung 113
Verfassung von Berlin 1990/5, 7; 1991/4; 1992/20
Verfassung des Landes Brandenburg 1992/20
Verfassungsreform 1991/4 f.
Verfassungsschutz 25, 35, 80, 108, 120; 1984/3; 1987/5; 1988/34; 1989/5, 45; 1990/61; 1991/84; 1993/43, 79
Verfassungsschutzgesetz 1985/3, 8, 26, 29; 1986/30; 1989/8; 1992/14, 57, 69
Verfassungstreue-Überprüfung 1991/35
Vergleichsmitteilungen s. Ortszuschlag
Verkehrszentralregister 1993/123
Verkehrszählung 1985/11; 1986/9
Verletzlichkeit 1987/11
Vermessungsamt 1985/6; 1993/52
Vermieter 1992/76
Vernetzung
s. Netze
Vernichtung von Datenträgern 63, 115; 1988/42; 1989/38; 1990/93
Veröffentlichung von Verurteilungen 81
Versand von Schriftstücken
s. Postverkehr
Vertraulichkeit 111; 1984/9; 1985/23; 1986/27; 1987/28; 1988/31
Verurteilungen, Veröffentlichung 81
Verwaltungsreform 1993/23, 49
Verwaltungsnetz 1987/11; 1988/3, 15; 1989/40
Verwaltungsprozeßordnung 90
Verwaltungsverfahrensgesetz 1988/5
Verwechslungen 61
Verwertungsverbot 66
Videoaufzeichnungen 1986/13; 1988/14; 1993/103
Vieh- und Schlachthof Spandau 105
Virenbaukästen 1992/27
Virenbefall 1992/26
Virenprüfung 1992/27
Virusprogramme 1988/4
Völkerrechtliche Vereinbarungen 1992/133
Volksbegehren 55
Volkszählung 1983 99, 100, 103, 120; 1984/3, 23
Volkszählung 1987 1984/23; 1985/11; 1986/7; 1987/3, 5; 1988/8, 25, 27; 1989/28; 1990/66
Volkszählungsurteil 1990/9; 1991/74, 91
vorbeugende Straftatenbekämpfung 1990/55; 1991/75, 81; 1992/59
Vordrucke 53, 87; 1986/25; 1987/28; 1988/33; 1989/34

Wachdienste 1993/51, 73
Wahlen 54, 55, 59, 68; 1985/17; 1989/29; 1990/62/65
Wahlstatistik 1992/89
Wahlwiederholung 1993/129
Warnkartei 40
Wählerliste
s. Wahlen
Wählerverzeichnis 1990/66
WAN (Wide Area Network) 1993/25
„Wanzen" 1990/74; 1991/98; 1992/101
Wasserbuch 1990/82
Wassergesetz 1993/119
Wasseruhr 1987/16
WASt 1993/19
Weltbanktagung 1988/25
Werbung 28; 1992/130
Wertkarte 1993/36, 121
Wettbewerbsunternehmen, Krankenhäuser 112
Widerspruchsklausel 1990/13
Wirtschaftskriminalität 77; 1984/6; 1986/4
Wissenschaftsklausel 1990/88; 1991/118; 1992/125; 1993/126
Wohnberechtigungsschein 1990/44; 1991/67; 1993/59
Wohngeldverfahren, Dialogisierung 1990/43
Wohnung 100; 1988/16, 27; 1992/76, 121; 1993/6, 9
Wohnungsamt 1989/19
Wohnungsbau-Kreditanstalt 1985/16
Wohnungsbau-Rechenzentrum 85, 120; 1984/17
Wohnungsbewerber, Fragebögen 1990/43
Wohnungsstatistikgesetz 1993/87
Wohnungsverkauf s. Umwandlung von Mietwohnungen
Wohnungsverlust, drohender 1993/113

Zählervergleichseinrichtungen 1992/129
Zahlungsverkehr 1987/12, 34
Zentrale Bewerberdatei 1990/80
Zentrale Personendatenbank 1990/20, 24
Zentrale Vormundschaftskasse, Unterhaltsvorschußkasse 85
ZER
s. Zentrales Einwohnerregister
Zentrales Einwohnerregister 1990/23; 1991/26, 46; 1992/37, 39; 1993/85
Zentrales Schuldnerverzeichnis s. Schuldnerverzeichnis
Zeugenschutz 1990/75
Zeugnisse 1988/30; 1989/33; 1992/111
Zielrufnummer 1992/127; 1993/129
Zinsabschlaggesetz 1992/6
ZIS (Zollinformationssystem) 1993/14
Zugriffsberechtigung 55; 1990/92
Zugriffskontrolle 86; 1985/8; 1990/91
Zurückgenommene Anträge 1993/59
Zustimmung
s. Einwilligung
Zwangsvollstreckungsankündigungen 1992/107
Zweckbindung 66, 1990/9; 1991/106; 1992/71, 87