Abgeordnetenhaus von Berlin

Drucksache 12 / 2819

12. Wahlperiode

Bericht

des Berliner Datenschutzbeauftragten zum 31. Dezember 1992

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 25. März 1992 vorgelegten Jahresbericht 1991 an und deckt entsprechend der Intention des Gesetzgebers den Zeitraum zwischen 1. Januar und 31. Dezember 1992 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] sowie § 55 Abs. 1 Kabelpilotprojektgesetz[2] nach[3].

1 GVBl. 1991, S. 309 f.
2 Für den Zeitraum bis zum 6. Mai 1992, in dem dieses Gesetz noch galt.
3 vgl. 5.1

Die Veröffentlichungen des Abgeordnetenhauses sind beim Kulturbuchverlag Berlin, Sprosserweg 3, 1000 Berlin 47, Telefon 6 61 84 84, zu beziehen.

Inhaltsverzeichnis

Anlagen

1. Rechtliche Rahmenbedingungen

1.1 Datenschutz in Deutschland und Europa

Das Grundrecht auf informationelle Selbstbestimmung geht davon aus, daß jeder über die Preisgabe und Verarbeitung seiner Daten selbst bestimmen kann. Es kann nicht unbeschränkt gelten: Soweit höherstehende Allgemeininteressen dies gebieten, muß es dem Staat einerseits, aber auch privaten Institutionen andererseits ohne Beteiligung oder gar gegen den Willen der Betroffenen möglich sein, Daten über sie zu erheben und zu verarbeiten. Soweit besteht ein allgemeiner Konsens in der Gesellschaft.

Werden Informationsstrukturen geschaffen, die ohne die Beteiligung der Betroffenen entstehen sollen oder gar gegen diese gerichtet sind, tritt an die Stelle des insoweit aufgegebenen Prinzips der Selbstbestimmung das Prinzip der Verhältnismäßigkeit. Der Gesetzgeber ist gehalten, Regelungen so auszugestalten, daß der Verlust an informationeller Selbstbestimmung durch die angestrebten Zwecke und die mit der Regelung verbundenen Erfolgsaussichten aufgewogen wird. Am ehesten wird dies erreicht durch informationelle Sparsamkeit: Der Gesetzgeber sollte also nur die Verarbeitungsstrukturen zulassen, die für den Verwaltungsablauf unverzichtbar sind.

Die großen Gesetzgebungsvorhaben des Bundes, die im vergangenen Jahr abgeschlossen wurden, zeigen, daß der Bundesgesetzgeber nicht bereit war, der informationellen Selbstbestimmung in dem Maße Rechnung zu tragen, das die Datenschutzbeauftragten des Bundes und der Länder für angemessen hielten.

Bundesgesetzgebung

Das vom Bundesrat initiierte *Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität* vom 15. Juli 1992[4] läßt die Einwände der Datenschutzbeauftragten, die sie bereits im vergangenen Jahr erhoben hatten[5], unberücksichtigt. Mit diesem Gesetz erhalten die Strafverfolgungsbehörden Befugnisse, die weit über das zur Bekämpfung der organisierten Kriminalität erforderliche Maß hinausgehen. Statt die Strafprozeßordnung insgesamt den verfassungsrechtlichen Erfordernissen nach dem Volkszählungsurteil anzupassen, hat es der Bundesgesetzgeber vorgezogen, die Voraussetzungen für schwerwiegende Eingriffe in die Privatsphäre auch unbeteiligter Personen in einem Teilbereich der Verbrechensbekämpfung zu schaffen. Es wird die Aufgabe der Datenschutzbeauftragten sein, bei der Anwendung dieses Gesetzes im Rahmen ihrer Zuständigkeiten auf eine verfassungskonforme, restriktive Auslegung zu achten, soweit diese überhaupt möglich ist. Auch wird aufmerksam zu beobachten sein, inwieweit die neuen geheimen Ermittlungsmethoden und technischen Fahndungsmittel zur Bekämpfung spezieller, organisierter Formen der Kriminalität geeignet sind, und ob sie, falls sich ihre Nichteignung erweist, auch zur Bekämpfung anderer Straftaten verwendet werden, was der Intention des Gesetzgebers eindeutig zuwiderliefe[6].

Auch das neue *Asylverfahrensgesetz* vom 26. Juni 1992[7] enthält eine – in der Öffentlichkeit weitgehend unbeachtet gebliebene – Regelung (§ 16), die in unverhältnismäßiger Weise in das Grundrecht auf informationelle Selbstbestimmung eingreift. So sollen generell alle Asylbewerber auch dann erkennungsdienstlich behandelt werden, wenn ihre Identität feststeht. Nach dem bisher geltenden Recht diente die erkennungsdienstliche Behandlung von Asylbewerbern ausschließlich der Identitätsfeststellung in Zweifelsfällen. Die neue Regelung soll verhindern, daß bereits abgelehnte Asylbewerber unter falschem Namen erneut einreisen und wiederum Asyl beantragen. Diese generelle und undifferenzierte Erhebung personenbezogener Daten in einem Verfahren, das sonst nur bei Personen angewandt wird, die einer Straftat verdächtigt werden, ist von den Datenschutzbeauftragten des Bundes und der Länder noch vor ihrer Verabschiedung kritisiert worden[8]. Sie kann nur als zusätzliche Abschreckungsmaßnahme verstanden werden, die zur Senkung der Asylbewerberzahlen beitragen soll.

Mit dem *9. Gesetz zur Änderung dienstrechtlicher Vorschriften* vom 11. Juni 1992[9] hat der Bundesgesetzgeber erstmals detaillierte Vorschriften über die *Führung von Personalakten* von Beamten, Richtern, Soldaten und Zivildienstleistenden erlassen. Dieses Gesetz, das am 1. Januar 1993 in Kraft getreten ist, greift zwar eine Reihe von Forderungen auf, die die Datenschutzbeauftragten des Bundes und der Länder bereits seit Jahren erhoben hatten[10], geht jedoch insgesamt noch nicht weit genug.

Für die Länder bedeutsam ist die Änderung des Beamtenrechtsrahmengesetzes, die zu einer Anpassung der Landesbeamtengesetze zwingt. In Berlin steht eine entsprechende Änderung des Landesbeamtengesetzes noch aus[11]. Auch wenn die neuen Vorschriften über das Personalaktenrecht formal nicht für Angestellte im öffentlichen Dienst gelten, sollten sie auch vor einer Anpassung des Bundesangestelltentarifvertrags entsprechend angewandt werden. Es darf keinen Datenschutz zweiter Klasse für Angestellte des öffentlichen Dienstes geben. Die Änderung des Beamtenrechts sollte zugleich als erster Schritt in Richtung auf ein einheitliches Arbeitnehmerdatenschutzgesetz verstanden werden, das trotz aller Absichtserklärungen der Bundesregierung noch immer auf sich warten läßt. Die Datenschutzbeauftragten des Bundes und der Länder haben die Notwendigkeit eines solchen Gesetzes in ihrer Entschließung vom 24. März 1992[12] unterstrichen.

Ebenfalls zum 1. Januar 1993 ist das Gesetz zur Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung *(Gesundheitsstrukturgesetz)* vom 21. Dezember 1992[13] in Kraft getreten. Auch wenn bestimmte Regelungen dieses Gesetzes erst stufenweise in zwei bis drei Jahren wirksam werden, wird der bereits mit dem Gesundheitsreformengesetz eingeschlagene problematische Weg der verstärkten Erhebung und Auswertung patientenbezogener Informationen fortgesetzt[14]. Die Kritik der Datenschutzbeauftragten[15] ist nur zu einem geringen Teil berücksichtigt worden.

Mit dem *Zinsabschlaggesetz* vom 9. November 1992[16] hat der Bundesgesetzgeber die Konsequenz aus der Entscheidung des Bundesverfassungsgerichts zur Besteuerung von Einkünften aus Kapitalvermögen[17] gezogen. Es wird abzuwarten sein, wie sich die komplizierten Regelungen dieses Gesetzes in der Praxis bewähren werden.

Schließlich sind zur Vorbereitung des Europäischen Binnenmarktes das *Umsatzsteuer- und das Verbrauchssteuer-Binnenmarktgesetz*[18] erlassen worden. Datenschutzrechtlich bedeutsam ist in diesem Zusammenhang, daß zur Umsetzung der entsprechenden EG-Richtlinien zur Steuerharmonisierung das EG-Amtshilfe-Gesetz ergänzt worden ist. Dadurch werden die zuständigen Finanzbehörden verpflichtet, elektronische Datenbanken mit Identifikationsnummern und anderen personenbezogenen Daten von Betriebsinhabern einzurichten, denen die steuerfreie Versendung oder der Empfang bestimmter Waren bewilligt worden ist. Diese Daten werden in regelmäßigen Abständen an die zuständigen Finanzbehörden anderer Mitgliedstaaten übermittelt. Das Gesetz verpflichtet deutsche Finanzbehörden zur Geheimhaltung und zweckgebundenen Verwendung von Auskünften, die sie von den Finanzbehörden anderer EG-Mitgliedstaaten erhalten.

---

4 BGBl. 1992 I, S. 1302 ff.; siehe dazu 4.3
5 vgl. Jahresbericht 1991, Anlage 2.3
6 Ausgeklammert wurde die ursprünglich ebenfalls im Entwurf enthaltene Regelung des „Großen Lauschangriffs"; vgl. hierzu unten 4.2.1
7 BGBl. 1992 I, S. 1126 ff.
8 vgl. Anlage 2.3
9 BGBl. 1992 I, S. 1030 ff.
10 vgl. Entschließung der 42. Konferenz zum Datenschutz im Recht des öffentlichen Dienstes, Jahresbericht 1991, Anlage 2.4
11 vgl. dazu 4.2.7
12 vgl. Anlage 2.1
13 BGBl. 1992 I, S. 2266 ff.
14 vgl. 4.1
15 vgl. Anlage 2.5
16 BGBl. 1992 I, S. 1853 ff.
17 vgl. Jahresbericht 1991, 1.1
18 BGBl. 1992 I, S. 1548 ff. bzw. 2150 ff.

Rechtsprechung

Erneut[18a] hat sich das *Bundesverfassungsgericht* in einer grundlegenden Entscheidung mit der Reichweite des *Fernmeldegeheimnisses* beschäftigt. In einem Beschluß vom 25. März 1992[19] hatte das Gericht über die Verfassungsbeschwerde einer Frau zu befinden, deren Telefonanschluß von der Deutschen Bundespost TELEKOM in eine Zählervergleichseinrichtung *(„Fangschaltung")* einbezogen worden war. Dies geschah auf Antrag einer anderen Telefonkundin, die wiederholt anonyme Anrufe erhalten hatte und vermutete, diese gingen von der Beschwerdeführerin aus, mit deren früherem Bekannten sie befreundet war. Die Beschwerdeführerin war auf Grund der Ergebnisse der Zählervergleichseinrichtung, bei der jeweils nur festgehalten wird, zwischen welchen Telefonanschlüssen ein Gespräch zustande gekommen ist, durch ein Zivilgericht zur Unterlassung verurteilt worden. Sie berief sich gegenüber dem Bundesverfassungsgericht darauf, das Zivilgericht hätte die Ergebnisse der Fangschaltung nicht gegen sie verwerten dürfen.

Die Begründung enthält grundlegende Ausführungen zur Bedeutung des Fernmeldegeheimnisses. Die Einrichtung von Fangschaltungen bedeutet stets einen Eingriff in dieses Grundrecht. Für diesen Eingriff fehlt bisher die erforderliche gesetzliche Grundlage. Das Bundesverfassungsgericht hat darauf hingewiesen, daß das Postverfassungsgesetz lediglich eine Ermächtigung zum Erlaß von Datenschutzvorschriften enthält, „soweit" personenbezogene Daten erhoben und verarbeitet „werden". Daraus läßt sich keine Ermächtigung zum Erlaß von Vorschriften über die Erhebung der Daten selbst z. B. durch Fangschaltungen und Zählervergleichseinrichtungen ableiten.

„Wenn das Grundgesetz die Einschränkung von grundrechtlichen Freiheiten und den Ausgleich zwischen kollidierenden Grundrechten dem Parlament vorbehält, so will es damit sichern, daß Entscheidungen von solcher Tragweite aus einem Verfahren hervorgehen, das der Öffentlichkeit Gelegenheit bietet, ihre Auffassungen auszubilden und zu vertreten, und die Volksvertretung anhält, Notwendigkeit und Ausmaß von Grundrechtseingriffen in öffentlicher Debatte zu klären. Diese Funktion kann der Gesetzesvorbehalt aber nur erfüllen, wenn die Ermächtigung zum Freiheitseingriff im Gesetz nicht bloß unausgesprochen vorausgesetzt, sondern ausdrücklich offengelegt wird."[20]

Diese Formulierungen haben grundsätzliche Bedeutung auch für Eingriffe in das Recht auf informationelle Selbstbestimmung außerhalb des Telekommunikationsbereichs und bedeuten eine konsequente Weiterentwicklung der Rechtsprechung des Bundesverfassungsgerichts seit dem Volkszählungsurteil von 1983.

Der Fangschaltungsbeschluß gibt Anlaß dazu, die Regelungen der Verarbeitung von Verbindungsdaten in der TELEKOM-Datenschutzverordnung und der Teledienstunternehmen-Datenschutzverordnung völlig neu zu überdenken[21].

Während das Bundesverfassungsgericht im Fangschaltungsbeschluß die Frage ausdrücklich offen gelassen hat, inwieweit aus einem Grundrechtsverstoß bei der Beweiserhebung ein *Beweisverwertungsverbot* folgt, hat der *Bundesgerichtshof* für das Strafprozeßrecht seine Rechtsprechung insoweit entscheidend korrigiert. Bisher war es in der Bundesrepublik zulässig, die Aussage eines Angeklagten, die er vor einem Polizeibeamten gemacht hatte, in der Hauptverhandlung auch dann zu verwerten, wenn er vor Gericht schwieg und von dem Polizeibeamten nicht auf sein Aussageverweigerungsrecht hingewiesen worden war. In seinem Beschluß vom 27. Februar 1992[22] hat der Bundesgerichtshof diese Rechtsprechung ausdrücklich aufgegeben und festgestellt, daß in diesem Fall Äußerungen des Beschuldigten im weiteren Verfahren auch vor Gericht nicht verwertet werden dürfen. Der Bundesgerichtshof begründet dies damit, daß der Grundsatz, daß niemand im Strafverfahren gegen sich selbst auszusagen braucht, also ein *Schweigerecht* hat, zu den anerkannten Prinzipien des Strafprozesses gehört und der Achtung vor der Menschenwürde entspricht.

Unter Hinweis auf die Rechtsprechung in anderen Ländern, insbesondere in den Niederlanden, behandelt der Bundesgerichtshof auch die Frage, wann der Betroffene auf sein Schweigerecht spätestens hingewiesen werden muß. Oft ist nämlich zweifelhaft, wann eine bloße Informationssammlung durch den Polizeibeamten in eine Beschuldigtenvernehmung übergeht. Hierbei hat der Beamte zwar einen Beurteilungsspielraum. Der Bundesgerichtshof betont aber, daß es polizeiliche Verhaltensweisen gibt, die schon nach ihrem äußeren Befund belegen, daß der Polizeibeamte dem Befragten als Beschuldigten begegnet. Das gilt etwa für Gespräche, die der Beamte mit einem Verdächtigen führt, den er im Polizeiwagen mit zur Wache nimmt. Hier muß selbst bei einem vergleichsweise geringen Grad des Verdachts vor jeder Befragung auf das Schweigerecht hingewiesen werden. Das gleiche gilt bei vorläufiger Festnahme des Betroffenen oder bei einer bei dem Verdächtigen vorgenommenen Durchsuchung.

Erneut hat sich der Bundesgerichtshof im vergangenen Jahr mit dem *Schutz von Patientendaten* befaßt. Während er in der Vergangenheit bereits die Offenbarung von Patientendaten gegenüber einer gewerblichen Verrechnungsstelle ohne Einwilligung der Betroffenen als Verstoß gegen die ärztliche Schweigepflicht bezeichnet hat[23], hatte er diesmal zu klären, ob Patientendaten im Rahmen eines Praxisverkaufs offenbart werden dürfen. Er hat diese Frage im Urteil vom 11. Dezember 1991[24] im Gegensatz zu seiner bisherigen Rechtsprechung verneint. Der Verkauf einer Patientenkartei mit dem gesamten Inventar einer Arztpraxis verstößt ebenfalls gegen die ärztliche Schweigepflicht. Ein entsprechender Kaufvertrag ist wegen Verstoßes gegen ein gesetzliches Verbot nichtig. Das Gericht hebt hervor, daß es dem Arzt obliegt, die Zustimmung des Patienten zu einer Weitergabe seiner Daten beim Verkauf der Arztpraxis in eindeutiger und unmißverständlicher Weise einzuholen. Die Annahme eines stillschweigend oder schlüssig erklärten Einverständnisses des Patienten mit der Weitergabe seiner Unterlagen scheide im Regelfall aus.

Ein ausdrückliches Einverständnis muß der Patient mit der Weitergabe seiner Daten an den Praxisübernehmer nur dann nicht erklären, wenn er seine Zustimmung dadurch zum Ausdruck bringt, daß er sich auch dem Übernehmer zur ärztlichen Behandlung anvertraut. In allen anderen Fällen muß die ausdrückliche Zustimmung des Patienten eingeholt werden. Dies hält der Bundesgerichtshof mit Recht für praktikabel, da Patienten in laufender Behandlung mündlich, die übrigen schriftlich befragt werden können. Äußert sich der angeschriebene Patient nicht oder ist sein Aufenthalt nicht mehr zu ermitteln, so müssen die Unterlagen beim ausscheidenden Arzt verbleiben. Suchen diese Patienten später den Arztnachfolger auf, so bereitet eine Beschaffung der Behandlungsdaten vom Praxisvorgänger keine größeren Schwierigkeiten als bei einem vom Patienten veranlaßten Arztwechsel. Sie können außerdem dadurch vermieden werden, daß der Praxisübergeber oder die ärztlichen Standesorganisationen Vorsorge für die leicht erreichbare Aufbewahrung solcher Unterlagen treffen.

Europas Datenautobahnen – immer noch ohne Leitplanken

Mit dem Inkrafttreten des *Europäischen Binnenmarktes* am 1. Januar 1993 ist ein entscheidender Schritt zur Verwirklichung des freien Verkehrs von Personen, Kapital, Gütern und Dienstleistungen in den 12 Mitgliedstaaten der Europäischen Gemeinschaft getan worden. Allerdings ist es nicht gelungen, entsprechend dem EWG-Vertrag bis zum 31. Dezember 1992 den vollständig freien Personenverkehr zwischen den Mitgliedstaaten zu verwirklichen. Statt dessen haben lediglich 9 der 12 EG-Mitgliedstaaten (Belgien, die Niederlande, Luxemburg, Deutschland, Frankreich, Italien, Spanien, Portugal und Griechenland) das sogenannte *Schengener Übereinkommen* mit einem Durchführungsübereinkommen unterzeichnet, die beide ursprünglich

18a vgl. Jahresbericht 1991, 1.1
19 1 BvR 1430/88, NJW 1992, S. 1875 ff.
20 BVerfG NJW 1992, S. 1877
21 vgl. 5.2
22 5 StR 190/91
23 vgl. Jahresbericht 1991, 1.1
24 VIII ZR 4/91

bereits am 1. Januar 1992 in Kraft treten sollten[25]. Das Europäische Parlament hat in einer Entschließung vom 19. November 1992[26] Kritik daran geübt, daß auf der Grundlage des Schengener Übereinkommens der freie Personenverkehr nur in einem Teil der Gemeinschaft verwirklicht werden soll und daß es bisher keine internationale gerichtliche Kontrolle der Ausführung des Durchführungsübereinkommens gibt. Das Europäische Parlament hält den Europäischen Gerichtshof in Luxemburg für die dafür geeignete Instanz, der jedoch bisher keine Zuständigkeit zur Überwachung des Schengener Übereinkommens hat. Eine internationale Kontrollinstanz ist umso wichtiger, als der Schutz des persönlichen Lebensbereichs und der Rechtsschutz der Personen, deren Daten in das *Schengener Informationssystem* aufgenommen werden sollen, durch die Unklarheit und Auslegungsfähigkeit zahlreicher Begriffe in diesem Übereinkommen beeinträchtigt wird. Auch hierauf hat das Europäische Parlament zu Recht hingewiesen.

Die Datenschutzbeauftragten haben schon 1989 betont, daß deutsche Stellen (insbesondere Polizei und Staatsanwaltschaft) nur dann personenbezogene Daten in das Schengener Informationssystem eingeben dürfen, wenn die Staaten, an die diese Daten übermittelt werden sollen, nationale Regelungen für die Erhebung und Nutzung solcher Daten erlassen haben. Dies gilt auch für die Bundesrepublik selbst, in der zwar mittlerweile die meisten Polizeigesetze der Länder entsprechende Regelungen enthalten, wo jedoch die Strafprozeßordnung nach wie vor in wesentlichen Bereichen nicht die erforderlichen bereichsspezifischen Grundlagen für das Erheben und Nutzen von Daten aufweist. Es erscheint deshalb optimistisch, wenn die Bundesregierung davon ausgeht, daß das Schengener Übereinkommen mit Durchführungsübereinkommen nach der Änderung des Art. 16 Grundgesetz Mitte 1993 ratifiziert werden kann. Daß die Anpassung der Strafprozeßordnung an die Vorgaben des Bundesverfassungsgerichts seit Jahren hinausgezögert wird, erweist sich jetzt als Hemmschuh beim Aufbau eines grenzüberschreitenden Informationssystems zur Verbrechensbekämpfung.

Bereits jetzt führt der Europäische Binnenmarkt, der in naher Zukunft zum Europäischen Wirtschaftsraum erweitert wird, zu einer starken Zunahme der personenbezogenen Datenströme, die nationale Grenzen überschreiten. Dies geschieht gegenwärtig noch ohne die erforderlichen Begrenzungen und Kontrollen auf der Grundlage eines harmonisierten europäischen Datenschutzrechts. Der von der EG-Kommission vorgelegte Entwurf einer Richtlinie des Rates zur Harmonisierung der allgemeinen Datenschutzgesetzgebung ist nicht mehr rechtzeitig zum Inkrafttreten des Binnenmarktes vom Ministerrat beschlossen worden. Allerdings hat die EG-Kommission am 15. Oktober 1992 ihren *„Geänderten Vorschlag für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr"* vorgelegt[26a], nachdem das Europäische Parlament bereits im März 1992 umfangreiche Änderungsvorschläge zum 1. Entwurf der Kommission gemacht hatte. Der geänderte Kommissionsvorschlag greift einen Teil dieser Änderungsvorschläge auf. Insbesondere entspricht er auch der Forderung der 1. Europäischen Datenschutzkonferenz vom November 1991, auf eine Unterscheidung zwischen den Datenschutzvorschriften für den öffentlichen und den privaten Bereich zu verzichten. Im Grundsatz sieht der geänderte Vorschlag die gleichen Regeln für private und öffentliche Datenverarbeiter vor, wobei eine Reihe von zusätzlichen Vorschriften für die öffentliche Datenverarbeitung geplant ist.

Dies ist ein entscheidender Schritt zum Abbau des auch in Deutschland noch vorherrschenden Datenschutzgefälles zwischen dem öffentlichen und dem privaten Bereich. Allerdings muß sichergestellt werden, daß der einheitliche europäische Datenschutzstandard nicht auf dem niedrigeren Niveau festgelegt wird, das gegenwärtig für private Datenverarbeiter in der Bundesrepublik gilt.

Der geänderte Richtlinienvorschlag verbietet es den Mitgliedstaaten nicht, in ihrer nationalen Gesetzgebung das jeweilige Datenschutzrecht weiterzuentwickeln. Allerdings darf der Export personenbezogener Daten in ein anderes Land der Europäischen Gemeinschaft dann nicht unterbunden werden, wenn in diesem Land der Datenschutzstandard der Richtlinie eingehalten wird.

Die Sonderbestimmungen zur Verarbeitung personenbezogener Daten und Meinungsäußerungsfreiheit (Art. 9 des geänderten Vorschlags) hat die Kommission auf Grund eines Vorschlags der Arbeitsgruppe Telekommunikation und Medien der internationalen Datenschutzkonferenz unter dem Vorsitz des Berliner Datenschutzbeauftragten in der Weise geändert, daß die Mitgliedstaaten Ausnahmen von der Datenschutzrichtlinie für die Verarbeitung personenbezogener Daten durch Presseorgane, audiovisuelle Medien und Journalisten zu *journalistischen Zwecken* vorsehen können. Damit wird auf europäischer Ebene einem Gesichtspunkt Rechnung getragen, der bereits in mehreren deutschen Landesdatenschutzgesetzen, so auch im Berliner Datenschutzgesetz, seinen Niederschlag gefunden hat. Soweit Rundfunkanstalten personenbezogene Daten im nichtredaktionellen Bereich zu wirtschaftlich-administrativen Zwecken verarbeiten (z. B. im Zusammenhang mit der Erhebung von Rundfunkgebühren), unterliegen sie in vollem Umfang dem allgemeinen Datenschutzrecht.

Der geänderte Richtlinienentwurf der Kommission wird gegenwärtig vom Ministerrat beraten, der einen gemeinsamen Standpunkt formuliert und diesen dem Europäischen Parlament zur 2. Lesung übermittelt. Erst danach entscheidet der Ministerrat endgültig über den Richtlinienentwurf. Mit dieser Entscheidung ist nicht vor Mitte 1993 zu rechnen. Der geänderte Vorschlag der Kommission sieht vor, daß die Mitgliedstaaten bis zum 1. Juli 1994 ihre innerstaatlichen Bestimmungen der Richtlinie anzupassen haben. Nach Ablauf dieser Anpassungsfrist können sich die Bürger in allen Staaten der Europäischen Gemeinschaft unmittelbar auf solche Bestimmungen der Richtlinie berufen, die ihnen weitergehende Rechte (z. B. auf Auskunft, Berichtigung oder Löschung) einräumen als die jeweilige nationale Gesetzgebung.

Ob der Europäische Unionsvertrag von Maastricht, den der Deutsche Bundestag im Dezember 1992 ratifiziert hat, in Kraft treten wird, ist gegenwärtig noch offen und hängt von der Zustimmung Dänemarks und Großbritanniens ab. Dieser Vertrag wird im Falle seines Inkrafttretens die gemeinschaftsweite Datenverarbeitung in den verschiedenen Stufen der Bildung der Europäischen Union weiter intensivieren. Auch sieht der Unionsvertrag die Einrichtung eines europäischen Bürgerbeauftragten vor. Das Europäische Parlament hat in seiner Entschließung vom 19. November 1992 die Forderung erhoben, daß dieser Bürgerbeauftragte der Gemeinschaft auch für den Datenschutz zuständig wird[27].

Am Beispiel der *Richtlinie* des Ministerrats über den *freien Zugang zu Informationen über die Umwelt*[28] läßt sich anschaulich machen, wie kurzfristig das europäische Informationsrecht in den Mitgliedstaaten Geltung erlangen kann. Die Richtlinie über den freien Informationszugang wurde am 7. Juni 1990 vom Ministerrat der Europäischen Gemeinschaft erlassen und verpflichtete die Mitgliedstaaten dazu, ihre nationale Gesetzgebung bis Ende 1992 den Bestimmungen der Richtlinie anzupassen. In der Bundesrepublik reichte der Zeitraum von zweieinhalb Jahren für diese Anpassung nicht aus. Der Bundesminister für Umwelt und Reaktorsicherheit leitet seinen Entwurf eines Umweltinformationsgesetzes den Ländern erst Anfang 1992 zur Stellungnahme zu[29]. Dies hat zur Folge, daß nach der Rechtsprechung des Europäischen Gerichtshofs diejenigen Bestimmungen der Richtlinie des EG-Ministerrates, die den Bürgern Rechte auf Akteneinsicht bzw. Auskunft einräumen, ab dem 1. Januar 1993 in der Bundesrepublik und damit auch im Land Berlin unmittelbar geltendes Recht sind. Die Verwaltung hat auch vor dem Inkrafttreten eines Umweltinformationsgesetzes des Bundes sicherzustellen, daß der Bürger sein Recht auf freien Zugang zu Umweltinformationen ausüben kann.

---

25 vgl. Jahresberichte 1989, 4.4, und 1990, wo irrtümlich davon ausgegangen wurde, das Durchführungsübereinkommen sei bereits in Kraft getreten

26 BR-Drs. 899/92, auch veröffentlicht in EuGRZ 1992. S. 578 ff.

26a KOM 92/422 endg.

27 vgl. EUGRZ 1992, S. 578 ff.

28 vgl. Jahresbericht 1990, 1.2

29 vgl. Jahresbericht 1991, 1.1; siehe auch unten 4.6

1.2 Datenschutz in Berlin

Neue Rechtsgrundlagen für den Datenschutz

In Berlin ist eine Reihe wichtiger Landesgesetze zur Verarbeitung personenbezogener Daten nach zum Teil jahrelangen Beratungen in Kraft getreten.

Noch vor Ablauf der verlängerten Übergangsfrist des § 34 Berliner Datenschutzgesetz (BlnDSG) am 31. März 1992 wurden das novellierte *Allgemeine Sicherheits- und Ordnungsgegetz (ASOG)*[30] und das *Ausführungsgesetz zum Gerichtsverfassungsgesetz (AGGVG)*[31] verabschiedet. Die einmalige Verlängerung der Übergangsfrist des Berliner Datenschutzgesetzes reichte allerdings nicht aus, um die Vielzahl weiterer bereichsspezifischer Verarbeitungsbefugnisse Gesetzeskraft erlangen zu lassen. Daraufhin verlängerte das Abgeordnetenhaus mit dem Zweiten Gesetz zur Änderung des Berliner Datenschutzgesetzes[32] zunächst bis zum 31. Oktober 1992 und durch das Dritte Gesetz zur Änderung des Berliner Datenschutzgesetzes[33] bis zum 31. Januar 1993.

Vor Ablauf der zweiten Verlängerung der Übergangsfrist trat am 21. Oktober 1992 das *Gesetz über die Informationsverarbeitung bei der allgemeinen Verwaltungstätigkeit (Informationsverarbeitungsgesetz – IVG –)*[33a] in Kraft.

Die Forderung nach einer gesetzlichen Grundlage für die Verarbeitung personenbezogener Daten im Rahmen der amtlichen Statistik im Land Berlin hat der Berliner Datenschutzbeauftragte bereits vor zehn Jahren erhoben[34]. Die Verabschiedung des *Landesstatistikgesetzes,* das im November 1991 bereits zum dritten Mal als Entwurf in das Parlament eingebracht worden war[35], entspricht daher einer der ältesten Forderungen des Datenschutzes. Das Land Berlin hat sich unter den alten Bundesländern am meisten Zeit für diese Regelung gelassen. Es hat allerdings für den speziellen Bereich des Statistischen Informationssystems auch eine Regelung getroffen, der eine Vorreiterfunktion im Verhältnis zum Bundesstatistikgesetz und zu anderen Landesgesetzen zukommt[36].

Gleichzeitig mit dem Landesstatistikgesetz hat das Abgeordnetenhaus in 2. Lesung ein neues *Verfassungsschutzgesetz* verabschiedet[36a], das fast alle Verbesserungsvorschläge des Datenschutzbeauftragten außer Acht gelassen hat.

Der Entwurf eines *Gesetzes über die Schaffung bereichsspezifischer Regelungen für die Verarbeitung personenbezogener Daten („Artikelgesetz")*[37] konnte erst in der zweiten Hälfte des Jahres 1992 im Unterausschuß „Datenschutz" beraten werden. Dabei gelang es nicht, diese Beratungen rechtzeitig vor Ablauf der verlängerten Übergangsfrist am 31. Oktober 1992 abzuschließen, so daß diese Übergangsfrist zum dritten und letzten Mal bis zum 31. Januar 1993 verlängert werden mußte.

Die bereits im vergangenen Jahr kritisierten Lücken und Widersprüche des Entwurfs konnten im wesentlichen in den Beratungen bereinigt werden.

Nach vielfältigen, teils hektischen Bemühungen vor allem im Unterausschuß „Datenschutz" ist es gelungen, das Gesetz so weit zu beraten, daß es am 21. Januar 1993 verabschiedet werden konnte.

Mit dem Inkrafttreten des Artikelgesetzes entfällt die Übergangsvorschrift des § 34 Abs. 1 BlnDSG, und das Berliner Datenschutzgesetz wird für die Bereiche, in denen bereichsspezifische Regelungen weiterhin fehlen, erstmals in seiner ganzen Strenge Anwendung finden. Dies bedeutet, daß die Verarbeitung personenbezogener Daten, für die es keine bereichsspezifische Rechtfertigung gibt, zukünftig nur noch auf die informierte Einwilligung der Betroffenen gestützt werden kann. Das Datenschutzgesetz selbst bietet hierfür keine Grundlage mehr.

Trotz der langwierigen Diskussionen über den Entwurf des Artikelgesetzes kann man sich des Eindrucks nicht erwehren, daß diese harte Auswirkung des Berliner Datenschutzgesetzes in manchen Behörden noch immer nicht verstanden worden ist. Für sie bleibt nur der Ausweg, so schnell wie möglich die erforderlichen bereichsspezifischen Verarbeitungsbefugnisse zu formulieren und dem Parlament zuzuleiten, wenn die Einwilligung der Betroffenen keine praktikable Verarbeitungsgrundlage darstellt. Auch ist davor zu warnen, eine Einwilligung vorschnell zu unterstellen oder die Anforderungen an ihre Wirksamkeit zu senken. Das Datenschutzgesetz enthält detaillierte Aussagen darüber, wann die Einwilligung des Betroffenen in die Verarbeitung seiner Daten wirksam ist.

Das Artikelgesetz enthält eine Vielzahl von *Rechtsgrundlagen für die Datenverarbeitung in Fachgesetzen,* die der Datenschutzbeauftragte seit langem gefordert hat.

Im einzelnen sind dies

- das Zweckentfremdungsbeseitigungsgesetz,
- das Gesetz über das Vermessungswesen in Berlin,
- die Landeshaushaltsordnung,
- das Berliner Stiftungsgesetz,
- das Ausführungsgesetz zum Bürgerlichen Gesetzbuch,
- das Gesundheitsdienst-Gesetz,
- das Berliner Kammergesetz,
- das Gesetz über Pflegeleistungen,
- das Berliner Hochschulgesetz,
- das Erschließungsbeitragsgesetz,
- das Lehrerbildungsgesetz,
- das Schulgesetz für Berlin,
- das Gesetz über die Bewährungshelfer für Jugendliche und Heranwachsende,
- das Eigenbetriebsgesetz,
- das Friedhofsgesetz,
- das Berliner Wassergesetz,
- das Gesetz zur Ausführung des Baugesetzbuches,
- das Gesetz über die Verarbeitung personenbezogener Daten bei der Deutschen Dienststelle (WASt) für die Benachrichtigung der nächsten Angehörigen von Gefallenen der ehemaligen Deutschen Wehrmacht,
- das Gesetz über die Datenverarbeitung im Bereich der Kulturverwaltung,
- das Gesetz über die Stadtreinigung,
- das Ausführungsgesetz zum Bundesimmissionsschutzgesetz,
- das Stadtreinigungsgesetz,
- das Gesetz über die Berufsbildung im öffentlichen Dienst und
- das Landesabgeordnetengesetz.

Dabei ist der Gesetzentwurf bei den Beratungen im Unterausschuß „Datenschutz" dahingehend verändert worden, daß die jeweiligen Fachgesetze lediglich um eine generelle Aufgabenzuweisung und Befugnis zur Verarbeitung personenbezogener Daten ergänzt werden sollen, der Umfang der Verarbeitung personenbezogener Daten jedoch aufgrund einer *Verordnungsermächtigung* durch die jeweilige Senatsverwaltung per Rechtsverordnung näher beschrieben werden soll. Es wurde nicht in das Belieben der jeweiligen Verwaltung gestellt, wann eine derartige Rechtsverordnung erlassen wird, sondern sie ist *verpflichtet,* bis zum 31. Dezember 1993 die erforderlichen Rechtsverordnungen zu erlassen.

Offen geblieben ist die Frage, wie bei *Bundesgesetzen* zu verfahren ist. Das Berliner Datenschutzgesetz fordert für jede Verarbeitung personenbezogener Daten entweder eine bereichsspezifi-

30 GVBl. 1992, S. 119 ff., in Kraft seit dem 26. 4. 1992
31 GVBl. 1992, S. 73 ff., in Kraft seit dem 29. 3. 1992
32 GVBl. 1992, S. 81
33 GVBl. 1992, S. 312
33a GVBl. 1992, S. 305; s. dazu 6.2
34 Jahresbericht 1983, Materialien zum Datenschutz 2, 2.2
35 Jahresbericht 1991, 3.4.4, S. 90; vgl. 4.2.6
36 vgl. dazu 4.2.6
36a GVBl. 1993, S. 33 ff. Das Gesetz trat am 31. 1. 1993 in Kraft, vgl. dazu 4.2.3
37 Jahresbericht 1991, 2.1

sche Rechtsgrundlage oder die Einwilligung des Betroffenen. Dabei unterscheidet es nicht zwischen der Anwendung von Bundesrecht oder Landesrecht durch die Behörden des Landes Berlin. Deshalb ist der Landesgesetzgeber gehalten, zu solchen Bundesgesetzen, die keine besonderen Rechtsgrundlagen für Eingriffe in das informationelle Selbstbestimmungsrecht enthalten, selbst Ausführungsgesetze zu erlassen. Dem hält der Senat entgegen, der Landesgesetzgeber könne dort nicht tätig werden, wo der Bund die Gesetzgebungskompetenz hat „und sogar im Begriff ist, von dieser Gebrauch zu machen".[38] Die Senatsverwaltungen für Justiz und Inneres halten darüber hinaus auch landesrechtliche Regelungen in solchen Bereichen für verfassungswidrig, in denen Bundesgesetze die Verarbeitung personenbezogener Daten zwar voraussetzen, aber nicht ausdrücklich regeln. Das Abgeordnetenhaus ist demgegenüber der Auffassung des Berliner Datenschutzbeauftragten gefolgt und hat zu drei Bundesgesetzen (Bundesdatenschutzgesetz, Baugesetzbuch und Bundesimmissionsschutzgesetz) Datenverarbeitungsbefugnisse in das Landesrecht aufgenommen. Damit werden Berliner Behörden in Übereinstimmung mit dem Grundsatz der Bundestreue in die Lage versetzt, Bundesgesetze datenschutzgerecht durchzuführen.

Wiederholt wurde im Berichtszeitraum die Gelegenheit verpaßt, bei der ohnehin anstehenden Änderung von Berliner Fachgesetzen (z. B. des Kita-Kostenbeteiligungsgesetzes) die *erforderlichen Datenverarbeitungsbefugnisse* zu regeln. Nur ausnahmsweise (z. B. beim 7. Änderungsgesetz zum Wassergesetz) ist es uns gelungen, noch während der parlamentarischen Beratungen die Gesetzentwürfe entsprechend ergänzen zu lassen. Auch nach der bevorstehenden Verabschiedung des Artikelgesetzes wird es Bereiche der Berliner Verwaltung geben, in denen personenbezogene Daten ohne die erforderliche bereichsspezifische Rechtsgrundlage verarbeitet werden. Es bleibt deshalb die Aufgabe der Verwaltung, diese Regelungsdefizite festzustellen und dem Parlament so schnell wie möglich Gesetzentwürfe vorzulegen, mit denen die Regelungslücken geschlossen werden können.

Datenschutzrechtlich bedeutsam war im Berichtszeitraum schließlich das *4. Gesetz zur Änderung des Personalvertretungsgesetzes*[39], mit dem die Mitbestimmungsrechte der Personalräte bei der Einführung und Änderung von Verfahren der IUK-Technik in der Berliner Verwaltung erheblich ausgeweitet worden sind. Das Mitbestimmungsrecht der Personalräte hängt nicht mehr - wie nach bisherigem Recht - davon ab, ob die Technik objektiv geeignet ist, die Leistung und das Verhalten der Beschäftigten zu kontrollieren. Damit wird die in der Vergangenheit oft streitige Frage an Bedeutung verlieren, ob eine Leistungs- und Verhaltenskontrolle der Beschäftigten mit den vorhandenen Programmen möglich ist oder nicht. Mit den erweiterten Mitbestimmungsmöglichkeiten der Personalräte wird zugleich die Datenschutzkontrolle in den öffentlichen Stellen Berlins intensiviert. Der Berliner Datenschutzbeauftragte hat stets der Beratung von Personalräten große Bedeutung beigemessen. Auch der Meinungsaustausch und die Zusammenarbeit mit dem Hauptpersonalrat wurden im vergangenen Jahr verstärkt.

Noch immer fehlt in Berlin ein *Landesarchivgesetz*, das der Berliner Datenschutzbeauftragte seit zehn Jahren fordert. Mittlerweile gehört Berlin insoweit bundesweit zu den Schlußlichtern der Rechtsentwicklung. Sogar in einigen neuen Bundesländern sind entsprechende Gesetze schon verabschiedet worden. Immerhin wurde an dem Tag der Verabschiedung des Artikelgesetzes, dem 21. Januar 1993, der Senatsentwurf für ein Landesarchivgesetz[40] im Abgeordnetenhaus eingebracht.

Das Berliner Datenschutzgesetz von 1990, das den bereichsspezifischen Verarbeitungsregeln den Vorrang einräumt, ist bereits wiederholt mit dem Hinweis kritisiert worden, es verstärke die *„Normenflut"* und laufe der rechtspolitischen Tendenz der Deregulierung zuwider. Diese Kritik geht fehl. Jährlich wird eine Vielzahl von Rechtsvorschriften verabschiedet und in Kraft gesetzt, über deren Sinn man durchaus streiten kann. Seit dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 ist allerdings klar, daß Eingriffe in das Recht auf informationelle Selbstbestimmung nur durch Gesetz oder auf Grund eines Gesetzes im überwiegenden Allgemeininteresse vorgenommen werden dürfen. In seinem Fangschaltungsbeschluß von 1992[41] hat das Bundesverfassungsgericht nochmals betont, daß es Sache des Parlaments sei, Notwendigkeit und Ausmaß von Grundrechtseingriffen in öffentlicher Debatte zu klären. Dem trägt das Berliner Datenschutzgesetz konsequent Rechnung, indem es den mit jeder Verarbeitung personenbezogener Daten verbundenen Eingriff in das Recht auf informationelle Selbstbestimmung nur auf Grund einer besonderen Rechtsvorschrift zuläßt, soweit der Betroffene nicht in die Verarbeitung eingewilligt hat. Das Berliner Datenschutzgesetz und die bereichsspezifischen Regelungen in den Fachgesetzen konkretisieren deshalb das Grundrecht auf Datenschutz und seine Grenzen.

Zusammenarbeit mit dem Land Brandenburg

Bereits vor der Empfehlung der gemeinsamen Regierungskommission, bis zum Jahre 1999 eine Vereinigung der Länder Berlin und Brandenburg anzustreben, traten am 7. Mai 1992 der *Staatsvertrag* über die Zusammenarbeit zwischen Berlin und Brandenburg im Bereich des Rundfunks[42] und der *Staatsvertrag über die Berlin-Brandenburgische Akademie der Wissenschaften*[43] in Kraft. Für die Medienanstalt Berlin-Brandenburg (MABB) und die Berlin-Brandenburgische Akademie der Wissenschaften, die beide ihren Sitz in Berlin haben, wurde auf Grund unserer Empfehlung[44] neben der Geltung des Berliner Datenschutzgesetzes die Durchführung der Datenschutzkontrolle in Zusammenarbeit mit dem Brandenburgischen Landesbeauftragten für den Datenschutz vorgesehen. Dies ist ein gutes Modell für die zahlreichen Zweiländeranstalten, die jetzt entstehen.[44a] Der Entwurf eines entsprechenden Staatsvertrags über die von Berlin und Brandenburg getragene *Akademie der Künste*[45] enthält keine entsprechende Regelung der kooperativen Datenschutzkontrolle. Wir werden gleichwohl die erforderlichen Kontrollen etwa im Archiv der Akademie der Künste in enger Abstimmung mit dem Brandenburgischen Landesbeauftragten für den Datenschutz durchführen.

Auch in anderen Bereichen - insbesondere bei der Überprüfung des Zentralen Einwohnerregisters - haben wir im Berichtszeitraum eng mit dem *Brandenburgischen Datenschutzbeauftragten* zusammengearbeitet. Auch bei den jetzt bevorstehenden Verhandlungen über einen Neugliederungsstaatsvertrag und andere Vereinbarungen zwischen den beiden Bundesländern sowie bei der intensiver werdenden Zusammenarbeit zwischen den Polizeibehörden Berlins und Brandenburgs werden wir diese Zusammenarbeit mit dem Brandenburgischen Datenschutzbeauftragten fortsetzen. Eine gute Grundlage dafür bietet die ähnliche Struktur der Datenschutzgesetze in beiden Ländern.

1.3 Grundrecht auf Datenschutz

Im Volkszählungsurteil hat das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung, das mit dem Recht auf Datenschutz gleichzustellen ist, als Grundrecht anerkannt. Anfängliche Zweifel in der Wissenschaft wurden durch die Bestätigung des Grundrechtes in einer Reihe nachfolgender Entscheidungen beseitigt. Das Grundrecht gewährleistet nach der Formulierung des Gerichtes „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen". Neben dem darin zum Ausdruck kommenden materiellen Gehalt betont das Gericht die Bedeutung der Beteiligung unabhängiger Datenschutzbeauftragter für einen effektiven Schutz des Rechts auf informationelle Selbstbestim-

38 Stellungnahme des Senats zum Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1991. Drs. 12/1760, S. 16
39 GVBl. 1992, S. 210 ff.
40 Drs. 12/2302

41 siehe unten 5.2
42 GVBl. 1992, S. 150 ff., S. 176; siehe dazu unten 5.1
43 GVBl. 1992, S. 226 ff., 270
44 vgl. Jahresbericht 1991, 2.1
44a vgl. z. B. den Entwurf eines Staatsvertrages über die Feuersozietät Berlin-Brandenburg und die Öffentliche Lebensversicherung Berlin-Brandenburg
45 Drs. 12/1991

mung. Ein verfassungsrechtlich zureichender Rechtsschutz sei darüber hinaus nur gegeben, wenn der Bürger Kenntnis davon erlangen kann, wer wo über welche seiner personenbezogenen Daten in welcher Weise und in welchen Zwecken verfügt.

So klar diese Aussagen des Bundesverfassungsgerichts sind, so wenig kann der rechtsunkundige Bürger sie der Lektüre des *Grundgesetzes* entnehmen. Schon dies spricht dafür, diese selbst oder deren Inhalt in das Grundgesetz aufzunehmen. Zudem sind sie erst dann für die zukünftige Rechtsentwicklung gesichert: Erst die ausdrückliche Formulierung in der Verfassung erzeugt den der Bedeutung der informationellen Selbstbestimmung in der „Informationsgesellschaft" angemessenen Respekt.

Die in Bundesrat und Bundestag aufgenommenen Beratungen umfaßten so auch konsequenterweise die Frage, ob das Grundgesetz um ein ausdrückliches Grundrecht auf den Schutz personenbezogener Daten sowie um Bestimmungen zu einem Datenschutzbeauftragten und zu Akteneinsichts- und Auskunftsrechten ergänzt werden soll.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung entsprechende Vorstellungen begrüßt und einen eigenen Formulierungsvorschlag zum Recht, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen, sowie zum Recht auf Auskunft aus und Einsicht in amtliche Unterlagen entwickelt[46]. Sie empfahl, die unabhängige Datenschutzkontrolle, die für die Verwirklichung des Grundrechts auf Datenschutz im Alltag von entscheidender Bedeutung ist, in der Verfassung zu verankern.

Im zuständigen Arbeitsausschuß der Kommission des Bundesrates fanden die Vorschläge zwar eine einfache, nicht aber die erforderliche Zweidrittel-Mehrheit. Daraufhin verabschiedete das Plenum der Kommission lediglich einen Diskussionsbericht, jedoch keine eigene Empfehlung. In den nunmehr folgenden Beratungen der Gemeinsamen Verfassungskommission von Bundestag und Bundesrat wurde die Problematik kontrovers diskutiert. Am Ende der Diskussion stand leider auch hier eine Ablehnung. Besonders bedauerlich ist, daß sich der Berliner Senat nur zu einer Enthaltung entschließen konnte.

Diese Entscheidung entspricht nicht der Berliner Verfassungssituation: Art. 21 b der am 11. Januar 1991 beschlossenen *Gesamtberliner Verfassung* sieht das Grundrecht auf Datenschutz in der Formulierung der Verfassungsgerichtsentscheidung vor. Darüber hinaus gewährleistete die von der Stadtverordnetenversammlung am 11. Juli 1990 beschlossene Verfassung, die bei der anstehenden Überarbeitung Berücksichtigung finden soll (Art. 88 Abs. 2 Gesamtberliner Verfassung), auch den Zugang zu Daten und Akten sowie die Institution des Datenschutzbeauftragten. Die Berliner Verfassungskommission bleibt aufgefordert, das Versäumnis des Bundes auf Landesebene wettzumachen.

Einen weiteren Schritt hat das Land Brandenburg unternommen: In ihrer Entschließung hatte die Konferenz der Datenschutzbeauftragten es für erforderlich gehalten, u. a. auch die Probleme der Aktenöffentlichkeit und der Informationsfreiheit, also den Zugang von jedermann zu den (nicht personenbezogenen) Unterlagen der Verwaltung in die Diskussion mit einzubeziehen. Als erste hat die *Verfassung des Landes Brandenburg* vom 22. April 1992 jedem nach Maßgabe des Gesetzes das Recht auf Einsicht in Akten und sonstige amtliche Unterlagen der Behörden und Verwaltungseinrichtungen des Landes und der Kommunen eingeräumt, soweit nicht überwiegende öffentliche oder private Interessen entgegenstehen.

Auch dieser Diskussion wird sich das Land Berlin - spätestens wenn die Einigung der beiden Länder konkret umgesetzt werden soll - nicht entziehen können.

[46] vgl. Anlage 2.2; diese Entschließung wurde gegen die Stimme des Bayerischen Landesbeauftragten gefaßt

2. Technische Rahmenbedingungen

2.1 Entwicklung der Informationstechnik

Bei der Informationstechnik halten die bereits mehrfach in Jahresberichten dargestellten Entwicklungstrends unvermindert an:

- *Miniaturisierung* der Hardware: Laptops und Notepads werden immer leistungsfähiger.
- *Komplexitätssteigerung der Software:* Software wird immer komplexer und leistungsfähiger, benutzerfreundlicher und anspruchsvoller hinsichtlich der Anforderungen an die Hardware. Gleichzeitig nimmt ihr Anteil an den Gesamtkosten der Informationstechnik zu.
- Dennoch Verbesserung des *Preis-/Leistungsverhältnisses:* Arbeitsplatzcomputer bzw. lokale Netze mit Standard-Betriebssystemen werden immer billiger und ihre Leistungsfähigkeit ermöglichen ihren Einsatz für immer mehr Einsatzgebiete. Marktübliche Großrechner („Mainframes" mit herstellerspezifischen - „proprietären" - Betriebssystem wie z. B. MVS von IBM oder BS 2000 von Siemens-Nixdorf) erreichen Leistungen, die bisher speziellen Systemen mit paralleler Rechnerarchitektur vorbehalten waren.
- *Vernetzung* im Kleinen und im Großen: Die Vernetzung von Personalcomputern zu lokalen Netzen ist längst zur Routine geworden. Dies wird noch dadurch verstärkt, daß noch einfachere Vernetzungstechniken als bisher üblich angeboten werden (sog. Peer-to-peer-Netze). Die regionale bis weltweite Vernetzung mittels digitaler Kommunikationsinfrastrukturen ist ebenfalls längst keine Utopie mehr.

Diese Entwicklungen haben mittlerweile dazu geführt, daß generell über die Strategie der Organisation des Einsatzes von Informationstechnik neu nachgedacht wird: Zwei Stichworte, die in der anwendernahen Fachpresse zu den mittlerweile meistgebrauchten Begriffen gehören, charakterisieren den Wandel: Downsizing und Outsourcing.

Diese offenkundig gegensätzlichen Begriffe hängen miteinander zusammen und stehen für das Auseinanderdriften zweier unterschiedlicher Welten beim Einsatz von Informationstechniken: der Welt der standardisierten Arbeitsplatzsysteme und der Welt der Rechenzentren mit proprietären Rechensystemen.

Downsizing bedeutet die Umstellung von Anwendungen von teuren Großrechnern auf dezentrale billige Arbeitsplatzsysteme. Wenn die Anwendungsverfahren selbst nicht im gleichen Maße mitwachsen, führt die starke Verbesserung der Leistungskapazitäten von Arbeitsplatzsystemen dazu, daß der Einsatz von solchen preisgünstigen Systemen wesentlich wirtschaftlicher ist, zumal die Vorhaltung speziell ausgebildeten Personals bei Standardsystemen nicht im vergleichbaren Umfang wie bei Großrechnern nötig ist. Die Bereithaltung arbeitsteilig organisierter Rechenzentren wird entbehrlich, wenn eine Organisation vollständig auf Standard-Arbeitsplatzsysteme umstellen kann.

Es bedeutet aber auch

- den vermehrten Einsatz von Systemen, deren informationstechnische Sicherheit relativ gering einzuschätzen ist;
- die Übertragung sicherheitsrelevanter Aufgaben der Systemverwaltung aus arbeitsteilig organisierten Rechenzentren in die Anwendersphäre;
- verstärkten Bedarf an externer Beratung, Administration und Wartung, die sich nicht mehr nur auf Systemfragen beschränkt, sondern auch in Anwendungen und organisatorische Strukturen beim Anwender eingreifen können.

Downsizing ist also zwar aus wirtschaftlicher Sicht konsequent, aber mit erhöhten Risiken für den Datenschutz, die Datensicherheit und die Ordnungsmäßigkeit der Datenverarbeitung verbunden. Mit der Umstellung der Verfahren auf Standardsysteme werden deren bekannte Risiken übertragen, die bisher bei Kleinanwendungen hinzunehmen waren, die von jeher mit solchen Systemen verarbeitet wurden.

Die beschriebene Tendenz zum Downsizing wird durch die scheinbar gegensätzliche Tendenz zum *Outsourcing* ergänzt. Einerseits macht die Verbesserung des Preis-/Leistungsverhältnisses bei Standardsystemen diese für immer mehr und größere Anwendungen erschließbar. Andererseits führt die gleiche Tendenz bei Großsystemen dazu, daß diese durch die typischen Großverfahren immer mehr unterfordert werden. So liegt der Gedanke nahe, viele Großverfahren auf einzelne Rechenzentren zu konzentrieren, damit die Leistungsfähigkeit der Rechner auch dann wirtschaftlich erschlossen werden kann, wenn die Anforderungen der Verfahren nicht im gleichen Maße steigen. Aus diesem Grunde steht der Dezentralisierungstendenz bei Arbeitsplatzsystemen eine Zentralisierungstendenz bei Großrechnern gegenüber. Da einzelne Organisationen Großrechnerverfahren benötigen, die Rechner aber nicht allein auslasten können, bieten sich für die Auslagerung der Datenverarbeitung in Rechenzentren sogenannte Outsourcing-Unternehmen an, die die Bereithaltung von Rechnerleistung samt technischer Betreuung und Beratung der Anwender als „Rundum-Service" leisten wollen.

Im Gegensatz zum Outsourcing, das zwar in Ansätzen in der Berliner öffentlichen Verwaltung bereits erkennbar ist - vor allem bei Eigenbetrieben und im Krankenhauswesen - und in den nächsten Jahren aus datenschutzrechtlicher Sicht der genauen Beobachtung bedarf, findet Downsizing in der Berliner Verwaltung verstärkt statt.

Downsizing in öffentlichen Stellen Berlins

In der Berliner Verwaltung werden im großen Umfang Arbeitsplatzsysteme als isolierte Personalcomputer (PC) mit dem Betriebssystem MS-DOS, als PC-Netze mit NOVELL-Netzbetriebssystem oder als Mehrplatzsysteme mit UNIX-Derivaten als Betriebssysteme eingesetzt. Nimmt man die von den Anwendern zu vertretenden Mängel des Einsatzes solcher Systeme einmal aus, die als Hauptrisiken anzusehen sind, so weist ein Blick in die Evaluationsberichte des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) deutlich aus, daß selbst die Produkte, die hinsichtlich der Sicherheit optimiert der Evaluation gestellt wurden, auf außerordentlich niedrigem Niveau zertifiziert wurden. Dies gilt sowohl für das in der Berliner Verwaltung verbreitet eingesetzte Sicherheitstool für PC (Safeguard Professional) als auch für die in Berlin bisher nicht vorgefundene Sicherheitsversion eines in Berlin ansonsten häufig verwendeten UNIX-Derivats (SINIX von Siemens-Nixdorf).

Prüfungen des Einsatzes von Standardsystemen haben in den letzten Jahren gezeigt, daß für den sach- und ordnungsgemäßen Betrieb und die Verwaltung der Standardsysteme im unmittelbaren Anwendungsbereich häufig die erforderliche *Qualifikation* fehlt. Dies schlägt sich nieder in mangelhaftem *Sicherheitsbewußtsein*. Wer die Eigenschaften der Systeme nicht kennt, kennt auch ihre Risiken nicht und setzt daher auch keine Schutzmaßnahmen sinnvoll um. Sachverstand ist meist nur in den zentralen Organisationsstellen zu finden, die es ihrerseits meist aber ablehnen, die sicherheitsrelevante Systemadministration bei eingeführten Verfahren zu übernehmen. Bereits früher haben wir für UNIX-Systeme empfohlen, eine zentrale und anwendungsferne Systemadministration durch die für Datenverarbeitung und Organisation zuständigen Stellen einzurichten[47].

Wie Einsparungen sich bei den Qualifikationskosten systemverantwortlich auswirken können, zeigen die Prüfergebnisse beim Landesamt für offene Vermögensfragen[48].

Auch zur *Fernwartung* haben wir uns bereits mehrfach kritisch, aber konstruktiv geäußert[49]. Unsere bisherigen Äußerungen zur Fernwartung bezogen sich aber auf die systemnahe Fernwartung bei Großrechnern, die nur in Ausnahmefällen Risiken für personenbezogene Daten in sich birgt. Durch das Downsizing entsteht auch ein Bedarf an Wartung für Anwendungsverfahren, die bei proprietären Systemen meist von Mitarbeitern der Rechenzentren selbst geleistet werden konnte, jetzt aber für fernwartende Firmen den unmittelbaren Zugang an Anwenderdaten erforderlich macht.

Fernwartung wird zwar von den Herstellern von Hard- und Software aus Rationalisierungsgründen als fortschrittlich deklariert, ist jedoch angesichts des sich ausbreitenden geschärften Bewußtseins für die Sicherheit der Informationstechnik eher ein Schritt rückwärts. Die Vorteile der Fernwartung für die Systemverfügbarkeit werden durch unberechenbare Risiken für die Vertraulichkeit der Daten und die Integrität der Systeme und Daten mehr als abgebaut. Aus diesem Grunde sollte die Verfügbarkeit der Systeme durch vertraglich festgelegte schnelle Reaktionszeiten der Wartungsfirmen der Fernwartung vorgezogen werden.

Fernwartung ist dann besonders problematisch, wenn es sich bei den erreichbaren Daten um solche handelt, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen und bei denen nicht nur die Übermittlung im datenschutzrechtlichen Sinne, sondern bereits die reine Offenbarung, etwa zu Zwecken der Auftragsdatenverarbeitung unzulässig ist.

2.2 Sicherheit der Informationstechnik

Nicht die datenschutzrechtlichen Risiken der organisatorischen Einbettung der Informationstechnik und auch nicht die des nachlässigen Umgangs mit ihr, sondern die Stärken und Schwachstellen der informationstechnischen Produkte bei der Abwehr von Risiken der Verfügbarkeit und Intregität der Systeme, Programme und Daten und der Vertraulichkeit der Daten werden bislang mit dem Begriff „IT-Sicherheit" umrissen.

IT-Sicherheitskriterien

Die Bewertung der informationstechnischen Produkte ist seit dessen Gründung 1991 Aufgabe des *Bundesamtes für Sicherheit in der Informationstechnik (BSI)* oder von autorisierten Prüfstellen an Hand von IT-Sicherheitskriterien, die - abgeleitet aus dem sogenannten Orange Book des amerikanischen Verteidigungsministeriums - vom BSI entwickelt und veröffentlicht worden sind[50].

Im Rahmen der Europäischen Gemeinschaft stehen derzeit *gemeinsame harmonisierte Kriterien* für die Bewertung der Sicherheit von Systemen der Informationstechnik vor der Verabschiedung. Gegenüber den deutschen Kriterien kennen sie sieben Evaluationsstufen (E0 - E6) anstelle der acht deutschen Qualitätsstufen (Q0 - Q7) sowie zehn nur beispielhaft dargestellte Funktionalitätsklassen, die sich teils hierarchisch an den Kriterien des Orange Book, teils an Funktionen spezialisierter Systeme orientieren. In der Fachöffentlichkeit besteht noch ein engagiert verfochtener Meinungsstreit über die harmonisierten Kriterien, da sie in den Augen vieler Fachwissenschaftler nicht ausreichen und wesentliche Risikobereiche nicht abdecken.

Ob derartige Sicherheitskriterien in der Praxis des Datenschutzes viel verändern werden, bleibt abzuwarten. Es gibt selbstverständlich einen Bedarf an unabhängigen Bewertungen und Vergleichen von Systemen, die der höheren Sicherheit in der Datenverarbeitung dienen. Es ist auch den Datenschutzbeauftragten ein sicheres Urteil kaum möglich, welche Systeme und Verfahren sie empfehlen und vor welchen sie warnen sollen, denn den in den Werbeschriften gepriesenen Vorzügen stehen meist versteckte Schwachpunkte gegenüber. Dennoch gibt es nur wenige Produkte, die der zeitraubenden und kostspieligen Evaluation durch das BSI ausgesetzt worden sind. Daher - und weil die Zertifikate meist keineswegs hochrangig sind - können wir zur Zeit nicht auf den Einsatz unabhängig geprüfter Systeme drängen.

47 „Empfehlungen für den datenschutzgerechten Einsatz von UNIX-Systemen", Jahresbericht 1989, Anlage 3
48 Abschnitt 3.3
49 z. B. in den Jahresberichten 1985, Anlage 7 (Empfehlungen zur datenschutzgerechten Fernwartung) und 1986, 4.1 (zur Fernwartung bei medizinischen Systemen)

50 „IT-Sicherheitskriterien", hrsg. vom BSI, Bundesanzeiger Verlagsges. Köln, 1989. Siehe auch Jahresbericht 1991, 1.2

IT-Sicherheitshandbuch

Mit dem IT-Sicherheitshandbuch hat das BSI ein weiteres Werk herausgebracht, das sich von der angesprochenen Definition löst, da es sich nicht vorwiegend mit der Sicherheit der Informationstechnik, sondern vor allem mit den Risiken in der Organisation der Datenverarbeitung und des riskanten Umgangs mit der Informationstechnik beschäftigt. Es soll dazu dienen, Bedrohungs- und Risikoanalysen durchzuführen und Sicherheitskonzepte zu erarbeiten.

Bereits im letzten Jahresbericht haben wir kritisch über einen Entwurf des IT-Sicherheitshandbuches berichtet[51]. Wir hatten Mängel in der Ausdrucksweise und inhaltliche Oberflächlichkeit sowie die unangemessen allumfassenden Ansprüche an eine Anwendbarkeit kritisiert. In der veröffentlichten Fassung wurden die Mängel weitgehend beseitigt und die Ansprüche auf ein vertretbares Maß zurückgenommen.

Jedoch hatten wir auch methodische Mängel angesprochen:

- den Verzicht auf die ganzheitliche Betrachtung der IT einsetzenden Organisationen;
- die pauschalisierenden, dennoch nicht nachvollziehbaren numerischen Werteskalen für ideelle Anforderungen;
- die mangelnde Berücksichtigung gesetzlicher Rahmenbedingungen;
- das Fehlen eines Aktualisierungs- und Fortschreibungskonzeptes;
- den zur Größenordnung des IT-Einsatzes häufig unverhältnismäßig großen Aufwand.

Die Kritik an der Methodik muß aufrechterhalten bleiben, da sich insoweit kaum etwas gegenüber dem Entwurf geändert hat. Es ist davon auszugehen, daß ohne intensive Begleitung durch das BSI eine praktische Anwendung des Sicherheitshandbuches kaum möglich ist.

Diese Unterstützung durch das BSI wird jedoch *Landesbehörden* nicht gewährt, da das BSI insoweit keine Zuständigkeit besitzt. Die von der Berliner Verwaltung an uns gestellte Frage nach der Verwendbarkeit des Handbuches ist also differenziert zu beantworten:

Zur systematischen Durchführung von Bedrohungs- und Risikoanalysen sowie für die systematische Erarbeitung von Sicherheitskonzepten erscheint das IT-Sicherheitshandbuch wenig geeignet, weil das Verfahren zumindest bei kleineren IT-Anwendungen zu aufwendig, dennoch aber in allen Fällen zu pauschal und wenig nachvollziehbar ist, und weil es die stetige Fortschreibung der Sicherheitskonzepte nicht unterstützt.

Soweit inhaltliche Anforderungen an die sichere Anwendung von informationstechnischen Systemen beschrieben werden, sind sie zutreffend und beachtenswert, wenn auch nicht immer präzise genug und vollständig.

Insgesamt halten wir es jedoch durchaus für angebracht, das IT-Sicherheitshandbuch unter Benennung unserer Vorbehalte breiter bekannt zu machen. In jedem Fall wird es dazu anregen, über Sicherheitskonzepte nachzudenken.

Virenbefall

Im Frühjahr warnte das BSI vor dem sog. *Michelangelo-Virus*. Damit rückte das Thema Computer-Viren in die Schlagzeilen der Presse und in den Mittelpunkt des Interesses von Computeranwendern und -fachleuten. Dieses öffentliche Interesse wurde dem Michelangelo-Virus zuteil, obwohl er eigentlich zu den relativ harmlosen Viren zu rechnen ist. Zwar verfügt er über eine Schadensroutine, die Daten von der Testplatte unwiederbringlich verschwinden läßt, jedoch verfügt er wie nicht gefährlichere Computerviren über Tarnmechanismen, die seine Bekämpfung erheblich erschweren würden. Ferner war er seit längerem bekannt und war daher von den meisten aktuellen Virenbekämpfungsprogrammen erkennbar und beseitigbar.

Wir nahmen dennoch die Warnung des BSI zum Anlaß, selbst Hinweise zum Michelangelo-Virus, seinen typischen Identifikationsmerkmalen und Maßnahmen zu seiner vorbeugenden Bekämpfung an die öffentlichen Stellen des Landes zu senden.

Der Geburtstag Michelangelos am 6. März stellt jedes Jahr das Auslösekriterium für diesen Virus dar. An diesem Tag überschreibt er mit einem zufällig aus dem Arbeitsspeicher gewählten Zeichen einzelne Festplattenbereiche. Die ursprünglich in diesen Bereichen gespeicherten Daten gehen verloren.

Eine von uns durchgeführte Umfrage ergab, daß Michelangelo nur in zwei Senatsverwaltungen entdeckt wurde. In einem Fall konnte er rechtzeitig beseitigt werden, im anderen Fall vernichtete er die erste Partition der Festplatte des befallenen Rechners. Die betroffene Verwaltung führte den Virenbefall auf neu beschaffte PC zurück. Offensichtlich übte die Lieferfirma nicht die notwendige Sorgfalt bei der Installation der Rechner, denn alle von dieser Firma gelieferten Rechner waren mit dem Virus infiziert.

Es wurden jedoch diverse *andere Viren* entdeckt, deren Bedrohungspotential zum Teil weitaus größer ist als das des Michelangelo. So wurden zum Beispiel die Viren plr, 5120, Stoned, 1704 und Tequila gefunden. Letzterer gehört zu jenen Viren, die nicht von allen Suchprogrammen entdeckt werden können.

Auf Grund der zunehmenden Bedrohung führen wir seit Beginn des Jahres bei allen datenschutzrechtlichen Überprüfungen von Personalcomputern, die mit dem Betriebssystem MS-DOS (PC-DOS) betrieben werden, auch eine *Virenprüfung* durch. Erfreulich ist, daß dabei bisher keine Viren gefunden wurden.

In der Fachliteratur werden allerdings Computerviren mit einem ganz neuen Bedrohungspotential beschrieben. Bisher arbeiten Virenbekämpfungsprogramme dadurch erfolgreich, daß sie die Festplatte oder Diskette absuchen und eventuell gefundene Dekodieralgorithmen von Viren mit einer in die Bekämpfungsprogramme integrierten Tabelle vergleichen. Diese Algorithmen, die zur Tarnung benötigt werden, sind für jeden Virus spezifisch und erlauben damit seine Identifikation.

Die neueste Virengeneration ist allerdings nach ersten bestätigten Tests in der Lage, nach jeder „Infektion" diesen Algorithmus selbständig zu verändern. Daraus folgt, daß eine Identifikation und ein Erkennen dieser Viren mit den bisherigen Möglichkeiten nicht mehr möglich sein wird.

Besondere Brisanz erhält dies durch die Tatsache, daß in Europa bereits sog. *Viren-Baukästen* verbreitet werden, die eine individuelle Konstruktion von derart gefährlichen Viren-Programmen zulassen und softwaremäßig unterstützen. Mit handelsüblichen Virenerkennungsprogrammen sind derart konstruierte Viren bisher nicht erkennbar.

Die derzeit einzige Schutzmöglichkeit gegen diese Arten von Viren sind Hardware-Einsteckkarten, die bereits vor dem Laden des Betriebssystems destruktive Rechneraktivitäten überwachen. Sollte es danach zu einer Virenaktivität kommen, die beispielsweise ein Löschen, Überschreiben oder Verändern bewirkt, unterbricht diese Einsteckkarte den Manipulationsversuch und öffnet ein Bildschirmfenster mit einer entsprechenden Sicherheitsabfrage, die der Systembenutzer entsprechend seinen Aktivitäten beantworten muß. So ist zum Beispiel ein Virus zu erkennen, falls eine Rückfrage hinsichtlich einer Festplattenformatierung bei der Erstellung eines Dokumentes in einer Textsoftware erscheint.

Da diese besonders gefährliche Art der Computerviren noch nicht in der Praxis aufgetreten ist, können sich *Präventionsmaßnahmen* derzeit noch auf das aktuell bekannte Bedrohungspotential, also die herkömmlichen Virentypen, konzentrieren. Dies bedeutet, daß in jedem Bereich, in dem PC eingesetzt werden, zwei Virenscanner zur Überwachung der Systemsicherheit eingesetzt werden sollten. Zwei Scanner sind ratsam, um eine gegenseitige Überprüfung dieser Programme zu ermöglichen und um programmseitige Schwächen der Virenscanner auszugleichen.

[51] Jahresbericht 1991, 1.2

Die ungleich bessere Lösung gegenüber einer Virenbekämpfung nach einer Infektion stellt jedoch eine wirkungsvolle Prävention gegen Virenbefall dar. Viren dringen normalerweise über Disketten oder offene Schnittstellen in ADV-Systeme ein. Da es in der Vergangenheit gelegentlich auch zu Vireninfektionen über Originalsoftware gekommen ist, sollte jede Diskette, die in ein System eingespielt wird, vorher mit einem Viren-Scanner auf ihre Integrität überprüft werden. Rechner mit offenen Kommunikationsschnittstellen für beispielsweise Datex-P/Datex-J sollten nicht in einem Netzwerk betrieben werden, um im Infektionsfalle den Schaden so gering wie möglich zu halten.

Das weitaus größte Risiko geht von dubiosen *Disketten* aus, deren Ursprung nicht genau bekannt ist. Vordringlich Computerspiele, Public-Domain-Software und indizierte Software (Spiele mit antisemitischem Hintergrund, gewaltverherrlichende Spiele, pornographische Spiele) sind Überträger von Computerviren. Je schlechter ein Programm verfügbar ist (beispielsweise durch Indizierung o. ä.), desto höher ist erfahrungsgemäß das Interesse an ihr und damit das Verlangen, in den Besitz solcher Software zu gelangen. Das Vorführen dieser Software im Büro gegenüber vertrauten Kollegen ist häufig der nächste Schritt. Im ungünstigen Fall ist der Virus zu diesem Zeitpunkt dann bereits im dienstlichen PC-Bereich aktiviert und hat sich eingenistet.

Die Einspielung nicht offiziell beschaffter Software muß daher nicht nur aus urheberrechtlichen Gründen unterbleiben.

Ferner ist zu empfehlen, daß Diskettenlaufwerke, die nicht unbedingt erforderlich sind, weil sie in Netzen betrieben werden, ausgebaut oder gesperrt werden, sofern nicht ohnehin Diskless-Workstations eingesetzt werden. Dies unterbindet neben dem Einspielen dubioser Programme auch das unbefugte Kopieren von Daten auf externe Datenträger.

2.3 Neue Dimensionen durch Cyberspace

Die informationelle Selbstbestimmung als wesentliche Voraussetzung für die freie Entfaltungsmöglichkeit der Bürger wird durch die Datenschutzgesetze vor dem zügellosen Einsatz der Informationstechnik bewahrt. Es scheint, daß in Zukunft die persönliche Selbstbestimmung durch technische Entwicklungen erheblichen Risiken ausgesetzt wird, denen noch keine gesetzlichen Dämme entgegenstehen. Die Manipulation des menschlichen Willens, die Erzeugung suchthafter Abhängigkeiten, hervorgerufen durch die faszinierende Ambivalenz von Realität und Schein, könnte durch die computergesteuerte Versetzung in Scheinwelten möglich werden.

Datenschutz muß sich auch mit den Problemen befassen, die solche Formen des Einsatzes von Informationstechnologie für die menschliche Anatomie mit sich bringen können.

Cyberspace ist eine solche dreidimensionale computergesteuerte Scheinwelt, in die der Mensch mit Hilfe von speziell entwickelter Hardware eintauchen kann. Diese Welten werden mit leistungsstarken Grafikrechnern vorgegaukelt und ermöglichen den ersten Schritt weg von der überkommenen Vorstellung, an einem Bildschirm oder einer Leinwand zu spielen, hin zu einem Spiel inmitten einer künstlichen Welt.

Eine kalifornische Firma beschäftigte sich zuerst mit dieser elektronisch erzeugten künstlichen Welt und hat, um in diese Welt eintauchen zu können, besondere Geräte entwickelt: Das Eyephone (Datenbrille) ist eine Art Helm, der mit Kopfhörern und zwei kleinen Farbbildschirmen ausgerüstet ist, die dem Benutzer einen scheinbar dreidimensionalen Blick ermöglichen. Der *Data-Glove* (Datenhandschuh) ist entfernt einem Motorradhandschuh mit Stulpe vergleichbar, der die Handbewegungen auf den Computer überträgt. Der *Data-Suit* (Datenanzug) ähnelt einem Druckausgleichsanzug militärischer Überschallpiloten, der mit einer großen Anzahl kleiner, aufblasbarer Luftpolster ausgerüstet ist, die in Sekundenschnelle rechnergesteuert voll aufgeblasen werden können und dem Träger des Datenanzugs so das Gefühl eines Stoßes oder eines Schlages vortäuschen.

Alle drei Hilfsmittel sind mit kleinen Sensoren ausgestattet, die sämtliche Bewegungen des Benutzers an den Computer weiterleiten, dort in ein Punkteraster übertragen und mit der festgefügten, softwareseitig vorhandenen Computerwelt verglichen werden. Danach schickt der Computer dem Benutzer seiner Handlung entsprechende „Antwortbilder". Dem Benutzer können mehr als 350 Bilder pro Sekunde vor Augen geführt werden.

Die Genauigkeit der Antworten, z. B. auf ein Tasten, hängt natürlich stark von der Präzision der Bilder in der Datenbrille und von der verwendeten Technologie ab. Ebenso ist die Bewegungsfreiheit des „Cybernauten" momentan noch stark durch den notwendigen „Kabelsalat" und das Gerätegewicht eingeschränkt. Die Qualität der virtuellen Realität selbst, also die Genauigkeit der per Computer erzeugten Bilder, erinnert noch stark an eine Computergrafik. So sind zwar Räume, z. B. Flughafenhalle, höchst detailliert mit Rolltreppen, Schaltern, Transportbändern u. ä. abbildbar, allerdings fehlt der letzte Eindruck der Realität, da eine echte Dreidimensionalität mit einem zweidimensionalen Darstellungsmedium wie dem Eyephone nicht nachbildbar ist.

Erste Versuche zeigen jedoch, daß diese Mängel nicht so entscheidend für den Benutzer sind. Bereits die ersten Versuchspersonen waren von den ersten Bildschirmen mit LCD-Technik mit ruckelnden Bildübergängen so beeindruckt, daß sie sich ohne weiteres mit der minderen Qualität zufriedenstellen ließen und in Interviews angaben, bereits erste *Suchterscheinungen* zu diagnostizieren.

Bei einer Messe in Monte Carlo stellte 1991 eine englische Firma das weltweit erste serienreife Cyberspace-System vor.

Dieses System wird in drei Baureihen produziert. Das erste und auch das kostengünstigste ist das *Unterhaltungsmodell,* welches aus einem Eyephone, zwei Joysticks und einem futuristischen Sessel besteht. Der Benutzer kann so unbegrenzt im „Computer-Universum" umherreisen. Bei diesem Modell besteht außerdem die Möglichkeit, daß mehrere Systeme miteinander verknüpft werden können, d. h. es wird ein aggressives Gegeneinanderspielen und ein harmonisches Zusammenspielen ermöglicht.

Zwei weitere Modelle der gleichen Firma sind auf den *wissenschaftlichen* und den militärischen Sektor abgestimmt. Diese Modelle verfügen zusätzlich noch über den Data-Suit. Cyberspace ermöglicht hier z. B. Chemikern die Reise in das Innere von Molekülen, Ärzte können zuvor „eingescannte" (eingelesene) Patienten von innen untersuchen und so zu neuen Erkenntnissen und Therapieverfahren gelangen. Reißbrettskizzen könnten in den Computer zusammen mit planungstechnischen Daten eingegeben werden, und ein Architekt könnte bereits vor dem Hausbau einen „Rundgang durch das Gebäude" machen.

Militärische Versionen der Cyberspace-Technologie sind derzeit bereits im Einsatz. So werden zum Beispiel Helme von US-Militärpiloten mit der notwendigen Technik ausgestattet, um die üblicherweise in Kampfflugzeugen erforderlichen Cockpit-Anzeigen auf das Helmvisier zu projizieren. Einsätze etwa im Golfkrieg wurden in Simulatoren mit Cyberspace-Technologie trainiert.

Ein japanischer Konzern befaßt sich derzeit mit der Entwicklung sog. *Bodytops,* Computern und Computerperipherie, die am Körper getragen werden. Erste Vorläufer dieser Technologie sind Armbanduhren mit Taschenrechner oder elektronischem Telefonbuch. Die derzeitigen Versuche befassen sich mit „Körperzusätzen", wie man sie eher von Captain Kirk vom Raumschiff Enterprise her kennt: Sprechende und Sprache verstehende Eyephones, verbunden mit einer Art Tracking Ball in einer Hand erlauben den Zugriff auf Computersysteme nahezu von jedem Ort innerhalb einer bestimmten Reichweite.

So harmlos und hilfreich diese Systeme auf den Betrachter wirken mögen, darf man nicht die *Gefahren* übersehen, die in dieser Weiterentwicklung der Computertechnik stecken. Doch die Möglichkeit, eine „heile" Welt zu erschaffen, in der man alle Probleme lösen, man alles beherrschen kann und man immer als Sieger hervorgeht, werden viele Menschen nutzen wollen, um dem Alltag zu entfliehen.

Es ist bekannt, daß bereits normale Video- und Computerspiele Suchtwirkungen entfalten können. Wer sich allzu intensiv und häufig in die abstrakten Spielwelten hineinversetzt, wird vielleicht immer schwerer davon loskommen, muß immer neue Versuche machen, um zum Ziel seines Spieles zu gelangen. Am Ende vernachlässigt er sich, negiert seine Umwelt und versäumt es, die wichtigeren Dinge zu erledigen.

All diese Effekte könnten bei Cyberspace in verschärfter Form auftreten: Die direkte Einwirkung der Scheinbilder über das Eyephone blendet alle Reste von Umgebungseinflüssen noch aus, die den normal mit einem Computer spielenden an die Existenz der realen Umgebung erinnern. Die realen Sinneswahrnehmungen aus der Scheinwelt mittels des Data-Suits können die Grenzen zwischen der realen und der virtuellen Welt immer verschwommener machen.

Darüber hinaus ist nicht auszuschließen, daß mit Cyberspace eine unkontrollierbare Manipulation von Personen über *unterbewußte Botschaften* (subliminal messages) möglich ist. Dabei handelt es sich um Impulse, die gezielt außerhalb der menschlichen Wahrnehmung auf das Unterbewußtsein wirken. Testversuche, die in den USA Ende der 70er Jahre in einem Kino in New York durchgeführt wurden und die die Beeinflußbarkeit durch diese Methode nachgewiesen haben, lassen sich mit Sicherheit hierher übertragen.

3. Erbe der DDR

3.1 Aufarbeitung der Vergangenheit

Mit der Verabschiedung *des Gesetzes über den Landesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR im Land Berlin* vom 20. November 1992[52] hat Berlin als drittes Land nach Sachsen und Mecklenburg-Vorpommern von der Möglichkeit Gebrauch gemacht, die der Bundesgesetzgeber in § 38 des Stasiunterlagengesetzes den neuen Bundesländern und Berlin eröffnet hat. Der Berliner Datenschutzbeauftragte hatte sich im Gesetzgebungsverfahren für das Stasiunterlagengesetz für die Einrichtung von Landesbeauftragten eingesetzt[53]. Dieser Beauftragte hat in Berlin vor allem die Aufgabe, die historische Aufarbeitung der Unterlagen des Ministeriums für Staatssicherheit, soweit sie sich auf das Land Berlin beziehen, voranzutreiben. Er soll aber auch Bürger beraten, die Einsicht in die Stasiunterlagen beim dafür zuständigen Bundesbeauftragten genommen haben und des fachkundigen – auch psychologischen – Rates bedürfen. Allerdings hat der Landesbeauftragte kein eigenes Einsichtsrecht in Stasiunterlagen in der Behörde des Bundesbeauftragten („Gauck-Behörde"), auch dann nicht, wenn der Betroffene ihm eine Vollmacht zur Einsichtnahme erteilt. Einsicht in Stasiunterlagen kann nach Bundesrecht nur der Betroffene selbst oder ein von ihm bevollmächtigter Rechtsanwalt nehmen. Das Einsichtsrecht des Landesbeauftragten bezieht sich demgegenüber auf alle Auskünfte, die die „Gauck-Behörde" in schriftlicher Form Bürgern oder Behörden des Landes Berlin erteilt.

Schließlich hat der Landesbeauftragte die Aufgabe, die Behörden des Landes Berlin bei der Bewertung von Auskünften der „Gauck-Behörde" zu beraten. Diese Aufgabe ist in einem späten Stadium des Gesetzgebungsverfahrens wieder in den Gesetzentwurf aufgenommen worden. Dagegen ist die Regelung eines früheren Entwurfs, daß der Landesbeauftragte auch einheitliche Richtlinien über den Umgang, die Verwendung und die Aufbewahrungsdauer von Auskünften der „Gauck-Behörde" bei öffentlichen Stellen des Landes Berlin erarbeiten sollte, nicht mehr im Gesetz enthalten. Derartige landeseinheitliche Richtlinien fehlen in Berlin nach wie vor, auch wenn die Koordinierungsstelle bei der Senatsverwaltung für Inneres eine Reihe von Informationen z. B. zur Zumutbarkeit der Weiterbeschäftigung von Personen, die für das Ministerium für Staatssicherheit tätig waren, für die Verwaltung entwickelt hat.

Im Gegensatz zur Koordinierungs- und Beratungsstelle verfügt der Landesbeauftragte allerdings über eine klare gesetzliche Aufgabenzuweisung und eine bereichsspezifische Befugnis zur Verarbeitung personenbezogener Daten.

Der Landesbeauftragte wurde *im Geschäftsbereich des Berliner Datenschutzbeauftragten* eingerichtet. Diese Zuordnung ist eine Berliner Besonderheit. Hintergrund dieser Regelung war, daß für den begrenzten Zeitraum von fünf Jahren keine eigene oberste Landesbehörde geschaffen werden sollte, der Landesbeauftragte aber dennoch mit einem Höchstmaß an fachlicher Unabhängigkeit ausgestattet werden sollte. Er untersteht zwar selbst der Dienstaufsicht des Berliner Datenschutzbeauftragten, ist allerdings in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Der Berliner Datenschutzbeauftragte übt weder eine Rechts- noch eine Fachaufsicht über ihn aus.

Am 26. November 1992 hat das Abgeordnetenhaus *Herrn Martin Gutzeit* zum Landesbeauftragten für die Unterlagen des Ministeriums für Staatssicherheit der ehemaligen DDR im Land Berlin gewählt. Herr Gutzeit bringt auf Grund seiner persönlichen Geschichte und als Mitglied der Enquetekommission des Deutschen Bundestages für die Aufarbeitung der DDR-Vergangenheit die besten Voraussetzungen für dieses Amt mit. Er hat sein Amt am 6. Januar 1993 angetreten. Wir werden ihm beim Aufbau seiner Dienststelle jede nur mögliche Unterstützung zuteil werden lassen.

Mit der Öffnung der Stasiunterlagen am 1. Januar 1992 trat auch die *Überprüfung* der übernommenen Mitarbeiterinnen und Mitarbeiter von Dienststellen der ehemaligen DDR in den öffentlichen Dienst des Landes Berlin in eine neue Phase.

Bereits 1991 hatte der Senat die Einrichtung einer *Koordinierungs- und Beratungsstelle für die Aufarbeitung der DDR-Vergangenheit in der Berliner Verwaltung* bei der Senatsverwaltung für Inneres beschlossen. Sie hatte anfangs unter anderem folgende Aufgaben:

- Beratung der Behörden bei der Überprüfung des Personals aus dem Beitrittsgebiet nach dem Einigungsvertrag;
- Beratung der Behörden bei der Bewertung von Staats- und Parteifunktionen im Rahmen der Neueinstellung von Bewerbern aus dem Beitrittsgebiet;
- Entwicklung von generellen Hinweisen für die Weiterbeschäftigung und Neueinstellung von Personal aus dem Beitrittsgebiet (auch für die Prozeßführung vor den Arbeitsgerichten);
- Beratung und Unterstützung der Bürger bei Abbau vergangenheitsbedingten Mißtrauens gegenüber der Verwaltung;
- Entgegennahme und Weiterleitung von Bürgerhinweisen auf Stasi-Mitarbeiter, Parteifunktionäre und ehemals repressiv handelnde Personen in der Berliner Verwaltung mit dem Ziel, das Ansehen des öffentlichen Dienstes nicht zu gefährden;
- Entgegennahme – eventuelle Ergänzung – und Weiterleitung von sonstigen Bürgerinformationen zur Hinterlassenschaft des DDR-Regime;
- Bewertung von Indizien für das Fortbestehen von Stasi- und Partei-Seilschaften in der Berliner Verwaltung und für das wirtschaftliche Zusammenwirken derartiger Organisationen in Verwaltung und Wirtschaft. Unterrichtung und Beratung der zuständigen Behörden.

Die Koordinierungsstelle ist damit nicht Teil der Personalverwaltung; soweit sie personenbezogene Daten für ihre Aufgabenstellung benötigt, kann sie sich nicht auf die allgemeinen Rechtsgrundlagen für die Verarbeitung von Personaldaten (§ 34 Abs. 2 BlnDSG, dienstrechtliche Spezialvorschriften) berufen, vielmehr bedarf sie insoweit jedenfalls nach Ablauf des Übergangsbonus einer ausdrücklichen Rechtsgrundlage, soweit nicht die Einwilligung der Betroffenen vorliegt.

Dies gilt sowohl für personenbezogene Daten von Bürgern, die sich ratsuchend oder mit Informationen an die Innenverwaltung wenden, als auch für Personaldaten von Mitarbeitern der öffentlichen Verwaltung. Der Senat hat zwar beschlossen, daß zu Senatsvorlagen, mit denen Bewerber aus dem Beitrittsgebiet im Bereich der Hauptverwaltung für Funktionen, die dem höheren Dienst entsprechen, berücksichtigt werden sollen, bis zum Ablauf der Legislaturperiode bei der Prüfung der Eignung für die Tätigkeit in einer demokratischen Verwaltung die Senatsverwaltung für Inneres – II – zu befragen ist. Das Ergebnis dieser Befragung

[52] GVBl. 1992, S. 335
[53] vgl. Jahresbericht 1991, 1.1

ist in der Senatsvorlage darzustellen[54]. Darin liegt aber weder eine gesetzliche Aufgabenzuweisung noch eine bereichsspezifische Befugnis zur Verarbeitung von Personaldaten durch andere öffentliche Stellen als die jeweiligen Dienstbehörden.

Eine Verarbeitungsbefugnis fehlt auch für Informationen, die Bürger an die Senatsverwaltung für Inneres weitergeben. Dabei handelt es sich naturgemäß um äußerst sensible Informationen, die zum Teil auch den Charakter von bloßen Vermutungen oder Verdächtigungen haben, was zunächst nicht erkennbar sein wird. Umso sorgfältiger muß die Erhebungs- und Speicherungsbefugnis formuliert sein. Die Einwilligung des Bürgers, der die Information liefert, kann die Speicherung jedenfalls nicht rechtfertigen, soweit die Informationen Dritte betreffen.

Soweit die Koordinierungs- und Beratungsstelle Behörden bei der Überprüfung des Personals und bei der Bewertung von Staats- und Parteifunktionen im Rahmen der Neueinstellung von Bewerbern aus dem Beitrittsgebiet beraten soll, werden eine Offenbarung von Personaldaten an die Koordinierungs- und Beratungsstelle und eine Verarbeitung der Daten bei dieser Stelle nicht erforderlich sein. Vielmehr kann die Beratung auch in nicht-personenbezogener Form durchgeführt werden.

Die Senatsverwaltung für Inneres stimmt mit uns darin überein, daß es nicht Aufgabe der Koordinierungs- und Beratungsstelle ist, eine zentrale „schwarze Liste" über ehemalige Mitarbeiter des Ministeriums für Staatssicherheit oder Funktionäre der SED zu führen.

Sie hält allerdings im Gegensatz zu uns auch keine bereichsspezifische gesetzliche Regelung der Tätigkeit der Koordinierungs- und Beratungsstelle für erforderlich. Wir hatten drei Alternativen aufgezeigt, wo diese Befugnis geregelt werden könnte, nämlich im Rahmen des Artikelgesetzes, im Gesetz über den Landesbeauftragten für die Stasiunterlagen oder in einem Gesetz zur Bewältigung der DDR-Vergangenheit, in dem sämtliche in diesem Zusammenhang entstehenden datenschutzrechtlichen Probleme hätten geregelt werden können. Die Senatsverwaltung für Inneres hat keinen dieser Vorschläge aufgegriffen.

Bereits im vergangenen Jahr hatten wir die Notwendigkeit betont, daß auch in Berlin landesgesetzlich zu regeln ist, unter welchen Voraussetzungen Dienstbehörden *Anfragen an den Bundesbeauftragten für die Stasiunterlagen* richten dürfen. Dies ist bisher nicht geschehen, obwohl auch für diese Frage das Gesetz über den Landesbeauftragten ein geeigneter Regelungsort gewesen wäre. Vielfach herrscht immer noch das Mißverständnis vor, das Stasiunterlagengesetz des Bundes regele die Frage, in welchen Fällen öffentliche Bedienstete durch eine Anfrage beim Bundesbeauftragten für die Stasiunterlagen überprüft werden dürfen. Tatsächlich enthält das Stasiunterlagengesetz nur Vorschriften darüber, für welche Zwecke Informationen aus den Stasiunterlagen verwendet und an wen sie weitergegeben werden dürfen.

Die Frage ist von erheblicher praktischer Bedeutung. Im Berichtszeitraum erreichten uns zahlreiche Beschwerden aus einem östlichen Bezirk, für den das Bezirksamt die generelle Überprüfung aller Mitarbeiterinnen und Mitarbeiter unabhängig von ihrer jetzigen Funktion durch Anfrage beim Bundesbeauftragten für die Stasiunterlagen beschlossen hatte. Alle diese Personen waren zuvor mit dem bekannten Zusatzfragebogen[55] befragt worden. Wir haben die *generelle Überprüfung* aller bezirklichen Bediensteten durch Anfrage beim Bundesbeauftragten für die Stasiunterlagen als unverhältnismäßig beanstandet. Unabhängig davon, ob man die Anfrage beim Bundesbeauftragten für die Stasiunterlagen auf Vorschriften des Einigungsvertrages oder auf das Bundesdatenschutzgesetz stützt, hat die Dienstbehörde in jedem einzelnen Fall zu prüfen, ob eine solche Anfrage gerechtfertigt ist. Dies ist zweifellos dann der Fall, wenn die Dienstbehörde Hinweise darauf hat, daß die Angaben des Beschäftigten im Zusatzfragebogen falsch waren. Man wird auch eine Überprüfung aller Angehörigen einer bestimmten Berufsgruppe wie z. B. Lehrer, Richter oder Inhaber von herausgehobenen Funktionen in der allgemeinen Verwaltung als zulässig ansehen müssen. Eine undifferenzierte, pauschale Überprüfung aller Angehörigen des öffentlichen Dienstes in einem Bezirksamt von der Putzfrau bis zum Bezirksbürgermeister ist jedoch eine Datenerhebung, die über das erforderliche Maß hinausgeht und damit unzulässig ist. Der Bezirk, dessen Praxis wir beanstandet haben, teilt unsere Rechtsauffassung nicht und setzt seine generelle Überprüfung fort. Wir haben Hinweise darauf, daß andere östliche Bezirke Berlins ähnlich verfahren.

Zwischenzeitlich bereitet der Senat einen Beschluß vor, nach dem in der Hauptverwaltung übernommene Mitarbeiterinnen und Mitarbeiter aus der ehemaligen DDR nur dann durch Anfrage beim Bundesbeauftragten für die Stasiunterlagen überprüft werden sollen, wenn sie Stellen des gehobenen und höheren Dienstes innehaben. Andere Mitarbeiterinnen und Mitarbeiter der Verwaltung sollen ausschließlich auf freiwilliger Basis überprüft werden, wobei der Senat einen Appell an die westlichen Bediensteten richten will, sich aus Gründen der Gleichbehandlung ebenfalls überprüfen zu lassen. Damit will der Senat im Gegensatz zu den östlichen Bezirken zumindest derzeit von einer generellen Überprüfung aller übernommenen Mitarbeiterinnen und Mitarbeiter absehen. Zwar führt der Senat hierfür in erster Linie Praktikabilitätsgründe an, weil der Bundesbeauftragte für die Stasiunterlagen die Masse der ihm vorliegenden Anfragen von Dienstbehörden ohnehin nicht in überschaubarer Zeit wird beantworten können. Auch wenn der Senat die Rechtsauffassung des Berliner Datenschutzbeauftragten nicht ausdrücklich teilt, würde das von ihm vorgesehene Verfahren im Ergebnis zu einer Beschränkung der Datenerhebung auf das erforderliche Maß führen.

Auch zum *Umgang mit den Fragebögen*[56] erreichten uns im vergangenen Jahr erneut Beschwerden. In einem Fall wurde festgestellt, daß beim Polizeipräsidenten in Berlin entgegen der ausdrücklichen Zusage an die Betroffenen, den Fragebogen im verschlossenen und versiegelten Umschlag bei der Personalakte aufzubewahren, sich der Fragebogen offen bei den Personalunterlagen befand. Dies haben wir gegenüber der Senatsverwaltung für Inneres beanstandet, die daraufhin eine Versiegelung des Fragebogens veranlaßt hat. Der Hinweis der Senatsinnenverwaltung, daß während der laufenden Personalüberprüfung ständig auf den Fragebogen zurückgegriffen werden müsse, rechtfertigt kein Abweichen von dem Verfahren, das dem Betroffenen vorab eingehend erläutert worden ist. Es muß auch während der laufenden Überprüfung vermieden werden, daß der Personalsachbearbeiter, der z. B. den Urlaubsantrag eines Polizisten zu bearbeiten hat, stets zwangsläufig auch den ausgefüllten Zusatzfragebogen bei der Personalakte offen vorfindet. Um dies zu vermeiden, wäre es auch denkbar, den Überprüfungsvorgang einschließlich des ausgefüllten Fragebogens bis zum Abschluß der Überprüfung völlig getrennt von der Personalakte unter Verschluß zu halten.

Der Bundesangestelltentarifvertrag-Ost enthält detaillierte Regelungen darüber, welche *Vordienstzeiten* von übernommenen Mitarbeiterinnen und Mitarbeitern aus der ehemaligen DDR von den Dienstbehörden anzuerkennen sind und sich damit vergütungssteigernd auswirken. Diese Regelungen schließen sogenannte „systemnahe" Beschäftigungen von der Anrechnung als Vordienstzeit aus. Wir haben der Senatsverwaltung für Inneres empfohlen, die Betroffenen eingehend über das Verfahren der Anerkennung von Vordienstzeiten aufzuklären. Es steht jedem öffentlichen Bediensteten frei, die Anerkennung von Vordienstzeiten zu beantragen oder darauf zu verzichten. Er darf auf diesem Wege auch nicht dazu veranlaßt werden, „systemnahe" Vordienstzeiten zu offenbaren, die ohnehin nicht anrechnungsfähig sind.

Zum Zweck der Anfrage beim Bundesbeauftragten für die Stasiunterlagen erheben die Dienstbehörden bei den betroffenen Bediensteten stets auch die *Personenkennzahl* (PKZ). Dies geschieht allerdings häufig ohne den erforderlichen Hinweis auf die Freiwilligkeit dieser Angabe. Die Personenkennzahl ist ein Datum, das dem Bundesbeauftragten die Erschließung der Stasiunterlagen und damit die Erteilung der Auskunft erleichtert und dieses Verfahren unter Umständen sehr beschleunigt. Wir haben

[54] Rundschreiben über die Zusammensetzung und den Aufgabenkatalog der Personalkommission des Senats vom 17. Juni 1991, Dienstblatt, Teil I, S. 111 f.

[55] vgl. Jahresbericht 1990, 3.5; 1991, 2.2

[56] Jahresbericht 1991, 2.2

deshalb einigen Dienstbehörden empfohlen, die Betroffenen darauf hinzuweisen, daß der Bundesbeauftragte, dessen Dateien nach der PKZ sortiert sind, einzelne Anfragen sehr viel schneller beantworten und Verwechselungen zuverlässiger ausschließen kann, wenn ihm die PKZ zur Verfügung gestellt wird. Falls dies nicht möglich ist – etwa weil der Betroffene die PKZ vergessen hat –, genügt aber auch die Angabe des Geburtsdatums, wie der Bundesbeauftragte selbst betont hat.

Hinzu kommt, daß die PKZ nach den eindeutigen Vorgaben des Einigungsvertrages in allen Datensammlungen, in denen sie enthalten ist, bis zum 31. Dezember 1992 gelöscht werden mußte. Um dem Bundesbeauftragten für die Stasiunterlagen eine Nutzung dieses Datums auch über diesen Zeitpunkt hinaus zu ermöglichen, haben wir deshalb eine ausdrückliche Klarstellung im Stasiunterlagengesetz als wünschenswert bezeichnet. Der Innenausschuß des Deutschen Bundestages hat demgegenüber die Auffassung vertreten, daß der Bundesbeauftragte für die Stasiunterlagen die Personenkennzahlen auch über den 31. Dezember 1992 hinaus nutzen darf. Eine Novellierung des Stasiunterlagengesetzes hat der Ausschuß zur Zeit nicht für erforderlich gehalten.

3.2 Abwicklung des Zentralen Einwohnerregisters (ZER)

Nach dem Einigungsvertrag war das Zentrale Einwohnerregister der früheren DDR zunächst weiterzuführen, soweit es Aufgaben des Meldewesens wahrzunehmen hatte und solange die örtlichen Melderegister ihre Aufgaben nicht ohne das zentrale Register erfüllen konnten. Es war zum frühestmöglichen Zeitpunkt, spätestens am 31. Dezember 1992, aufzulösen.

Alle Daten, die nicht zu den Meldedaten gehörten und die nicht für die Aufgabenerfüllung anderer Fachbereichsverwaltungen erforderlich waren, waren zu löschen. Sofern Fachverwaltungen Ansprüche äußern würden, wären solche Daten von den Meldedaten getrennt zu speichern und zum frühestmöglichen Zeitpunkt, aber spätestens bis zum 31. Dezember 1992 in die Datenbestände der jeweiligen Fachbereichsverwaltungen zu überführen und danach im Zentralen Einwohnerregister unverzüglich zu löschen. Die Verarbeitung neu anfallender Daten, die zur Aufgabenerfüllung der Fachbereichsverwaltungen erforderlich waren, war bis zur Überführung der Daten in diese Bereiche zulässig. Auskünfte durften nur durch die zuständige Fachbereichsverwaltung nach Maßgabe des für sie geltenden Rechts erteilt werden.

Diese Bestimmungen waren im zurückliegenden Jahr umzusetzen.

Melderechtsfremde Projektdateien

Sie beziehen sich jedoch ausschließlich auf das Zentrale Einwohnerregister, ohne zu berücksichtigen, daß das ZER nur einen – wenn auch sehr wesentlichen – Bestandteil der im Rechenzentrum des ehemaligen Ministeriums des Innern (MdI) der DDR vorgehaltenen Datensammlungen darstellte. So wurden in diesem Rechenzentrum, das für damalige Verhältnisse mit ESER-Rechentechnik recht großzügig ausgestattet war, auch *DV-Projekte* abgearbeitet, die mit dem Meldewesen nur sehr wenig zu tun hatten.

Zu diesen Projekten gehörten statistische Verfahren (Fahndungsstatistik, Brandstatistik der Feuerwehr, Medizinalstatistik zum Gesundheitszustand Strafgefangener und Verhafteter, Medizinalstatistik zum MdI-Personal, Kriminalstatistik, Verkehrsunfallstatistik), Ordnungswidrigkeiten im Transitverkehr, MdI-interne Projekte (Personal/Kader, Bekleidung/Ausrüstung, Kfz-Ersatzteile, Führungskennziffern) und Daten zum Strafvollzug (Strafgefangenen- und Verhaftetendatei, Inhaftiertenbestand einschließlich dessen ökonomischer Abrechnung).

Bis auf einige wenige (Verkehrsunfallstatistik, Kriminalstatistik, Personalbestand, Datenbank des Gemeinsamen Landeskriminalamtes der neuen Bundesländer) wurden die Verfahren mit oder kurz nach der Vereinigung eingestellt. Anders als bei den vielfältigen, elektronisch gespeicherten Datensammlungen des MfS wurden hier jedoch die Dateien weder gelöscht noch gar die Datenträger physisch vernichtet.

Nach dem Einigungsvertrag waren diejenigen Daten nicht zu löschen, deren Kenntnis nach Bundesrecht für die speichernde Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben erforderlich ist.

In ergänzender Auslegung sollte die Löschung ebenfalls unterbleiben, soweit nach landesgesetzlichen Regelungen die Speicherung dieser Datenbestände für die Aufgabenerfüllung von Landesbehörden, die gem. Art. 13 des Einigungsvertrages die Verantwortung für die auftraggebende Behörde übernehmen, erforderlich war. Die Projektdaten waren in diesem Fall an die jeweiligen Landesbehörden herauszugeben.

Diese gesetzlichen Anforderungen sowie die sich zuspitzende Situation im Rechenzentrum selbst – das nahe Ende der Einrichtung vor Augen verließen immer mehr qualifizierte Mitarbeiter das ZER – führten zu einer *Sicherstellungsaktion,* die sowohl die Datenträger als auch die zugehörigen Projektunterlagen betrafen. Vom Innenministerium des Landes Brandenburg als dienstaufsichtsführender Behörde im Auftrag der anderen Bundesländer wurde im Juni 1992 veranlaßt, alle Projekte möglichen Manipulationen durch Mitarbeiter zu entziehen.

Die zuständigen Fachverwaltungen des Bundes sowie der Länder wurden über die mannigfaltigen Datensammlungen des ehemaligen MdI der DDR informiert und gebeten, eventuelle Ansprüche hinsichtlich der weiteren Nutzung anzumelden. Bis auf die Kriminalstatistik, die im Auftrag aller neuen Bundesländer vom Landeskriminalamt Sachsen ohne Personenbezug aufbereitet werden soll, hat bisher nur die Strafgefangenendatei das Interesse des Bundesarchivs geweckt.

Im Ergebnis wurden die sichergestellten Datenbestände gesperrt und dem Bundesarchiv zur Sicherstellung überantwortet. Dabei war insbesondere zu prüfen, ob das Datenmaterial ohne die seinerzeit genutzte Rechentechnik und ohne das Spezialwissen der ehemaligen Mitarbeiter des MdI-Rechenzentrums überhaupt noch nutzbar ist.

Überprüfung vor Ort

Im Auftrag der Datenschutzbeauftragten der neuen Bundesländer führten wir in Zusammenarbeit mit dem Brandenburgischen Datenschutzbeauftragten eine datenschutzrechtliche *Überprüfung des ZER* durch, die sich auf die Aspekte konzentrierte, die für die nur noch kurze Zukunft des ZER von Bedeutung waren, im wesentlichen also mit der ordnungsgemäßen, planvollen Abwicklung und Auflösung der Einrichtung bis zum 31. Dezember 1992.

Das Berliner Landeseinwohneramt (LEA) hatte zwar bereits im April 1991 die Übernahme der Berliner Daten abgeschlossen und nutzte die ZER-Datenbank nur noch zu gelegentlichen Abgleichen durch Online-Zugriffe, deren Häufigkeit ständig abnahm. Wegen der Belegenheit in Berlin wurden wir dennoch beteiligt.

Das Hauptproblem lag darin, daß das personelle Ausbluten des ZER die ordnungsgemäße Abwicklung der Restaufgaben des ZER, insbesondere die Meldedatenübergabe an die restlichen Kommunen, sehr gefährdete. Sofortige Anpassungen an neue Rahmenbedingungen, etwa bei Inkrafttreten von Meldegesetzen, konnten auf Grund von Kapazitätsengpässen bei der Programmierung nicht mehr erfolgen. Es gab zum Prüfzeitpunkt nur noch einen qualifizierten Programmierer, der für eventuell notwendige Programmpflegearbeiten zur Verfügung stand.

Für das Landeskriminalamt Brandenburg bestand ein Zugriff auf die gesamten Meldedaten der fünf neuen Länder und Berlins. Dabei handelte es sich um den Online-Zugriff des derzeit in Auflösung begriffenen *Gemeinsamen Landeskriminalamtes.* Diese umfassende Zugriffsmöglichkeit war unzulässig. Soweit die Meldedaten an die neuen Länder übergeben wurden und diese die Meldeaufgaben unabhängig vom ZER wahrnahmen, durften Auskünfte und Datenübermittlungen durch Online-Zugriffe nur noch bei den örtlich zuständigen Meldebehörden nach Maßgabe des jeweiligen Landesmeldegesetzes erfolgen.

Ein Online-Zugriff beim ZER käme allenfalls in Betracht für Meldedaten, bei denen das ZER wegen der noch nicht funktionsfähigen Meldebehörden die Meldeaufgaben noch durchführte.

Anfragen, die *Berliner Bürger* betrafen, wurden zum Teil vom ZER beantwortet. Zwar wurden keine Melderegisterauskünfte erteilt, wenn bereits aus der Anfrage ersichtlich war, daß es sich um einen Berliner Einwohner handelte. In diesem Fall erfolgte die Auskunft durch das LEA Berlin. Wenn jedoch aus der Anfrage selbst nicht ersichtlich war, daß es sich um einen Berliner Einwohner handelte, erteilte das ZER eine Auskunft.

Auch die Erteilung von Melderegisterauskünften an Dritte durch das ZER war unzulässig. Auskünfte sind nur vom LEA Berlin als zuständiger Meldebehörde nach dem Berliner Meldegesetz zu erteilen. Bei diesem Verfahren war zudem nicht sichergestellt, daß Auskunftssperren, die nach Übergabe der Daten (April 1991) verfügt wurden, beim ZER berücksichtigt werden konnten.

Das ZER hielt es weiterhin für zulässig, die Datensätze mit dem Ordnungsmerkmal *Personenkennzahl* zu führen. Insbesondere wegen personeller Probleme sei es nicht möglich gewesen, eine umfassende Umstellung dieses für das ZER maßgeblichen Ordnungsmerkmals durchzuführen.

Laut Auskunft des ZER fand die PKZ allerdings nur noch interne Verwendung. Im Verkehr mit den Meldebehörden wurde die PKZ weiterhin zur Aktualisierung des Datenbestandes verwandt, da anderenfalls in vielen Fällen ein Auffinden des Datensatzes nicht möglich gewesen wäre. Bei der Übergabe der Meldedaten an Gemeinden wurde die PKZ nicht mitgeliefert. Die Daten wurden mit einem eigenen Ordnungsmerkmal versehen, das im ZER nicht gespeichert wurde.

Unzulässigerweise wurden auf die *Kreismeldekarteikarten* jedoch noch die PKZ ausgedruckt. Dieser Mangel wurde beanstandet und es wurde gefordert, falls es dem ZER technisch nicht anders möglich wäre, dieses Ordnungsmerkmal vor Auslieferung zu schwärzen.

Das ZER vergab für *Neugeborene* in den neuen Ländern immer noch die PKZ. Berlin war hiervon ausgenommen, da der noch vorhandene Berliner Datenbestand nicht mehr aktualisiert wurde. Gemäß Einigungsvertrag durfte die PKZ weiter verarbeitet werden, soweit und solange sie für die Weiterführung des Melderegisters erforderlich war. Allerdings sollten sämtliche Dateien, die nach der PKZ geordnet sind, unverzüglich nach anderen Merkmalen umgeordnet und die PKZ zum frühestmöglichen Zeitpunkt gelöscht werden. Das ZER hatte keine Löschung der PKZ bzw. Umordnung nach einem neuen Ordnungsmerkmal vorgenommen, da dies einen erheblichen programmtechnischen Umstellungsaufwand bedeutet hätte, der bei der sich zuspitzenden Personalsituation ein zu hohes Risiko hinsichtlich der Datenübergabe an die Landesmeldebehörden bedeutet hätte.

Im ZER-Datensatz war immer noch eine ganze Reihe melderechtsfremder Daten gespeichert, die über das gesetzlich zulässige Maß hinausgingen. Wenn auch die meisten dieser Daten (z. B. Personalausweis- und Paßdaten, Abmeldung nach außerhalb, Zugehörigkeit zu den bewaffneten Organen, Haft oder Haftentlassung, Führerscheindaten) für Belange des Meldewesens gesperrt waren, hatte es doch in der Vergangenheit vereinzelte Anfragen von für diese Daten zuständigen Fachbereichsverwaltungen der neuen Länder gegeben. Auch in diesen Fällen fehlten zum Prüfungszeitpunkt Entscheidungen zur weiteren Nutzung des Datenmaterials, obwohl es sich zumindest teilweise um Daten handelt, die bei der Durchsetzung von Rehabilitierungsansprüchen eine Rolle spielen könnten.

Ein wesentlicher Teilaspekt der Prüfung bezog sich auf die ordnungsgemäße *Organisation der Datenträgerverwaltung* im Rechenzentrum, wurden doch von verschiedenen Seiten Befürchtungen dahingehend geäußert, daß möglicherweise bereits Daten unzulässigerweise abgeflossen waren bzw. sogar ganze Datenträger unbemerkt aus dem Archiv entfernt wurden.

Auf einem PC geführt wurde eine Bestandsliste, die neben der Archivnummer u. a. die Kennzeichnung des zugeordneten Projektes und einen Status enthielt, der es ermöglichte, festzustellen, ob sich der jeweilige Datenträger im Haus oder im Zuge eines Datenträgeraustausches außerhalb befand, ob er defekt war oder gar zur Vernichtung freigegeben worden war. Außerdem enthielt die Liste einen Verweis auf den Stellplatz in den Archivschränken.

Es existierten insgesamt ca. 20 000 Disketten, 33 000 Magnetbänder, 250 29-MB-Wechselplatten und 1 200 100-MB-Wechselplatten. Bei diesen Zahlen und angesichts der Tatsache, daß die Datenträgerverwaltung weitgehend manuell erfolgte, ist es sicher nachvollziehbar, daß eine Inventur mit einem erheblichen Aufwand verbunden sein mußte. Bei der letzten Überprüfung der Datenträgerbestände im Jahre 1990 waren 15 Mitarbeiter ca. 4 Tage beschäftigt.

Angesichts des nicht von der Hand zu weisenden Risikos, daß Datenträger mit personenbezogenen Daten dem Archiv unbemerkt entnommen werden könnten, des wirtschaftlichen Interesses an diesen Daten und der in der Regel ungünstigen persönlichen Situation aller Mitarbeiter - Ende September sollten die 198 noch verbliebenen ZER-Beschäftigten ihre Kündigung zum Jahresende erhalten - haben wir dringend empfohlen, vor der Auflösung des ZER eine Inventur unter externer Aufsicht durchzuführen.

Nach Auskunft des ZER sollte nach seiner Auflösung das Gebäude vom Polizeipräsidenten in Berlin übernommen werden, wobei die ESER-Rechentechnik verschrottet und die IBM-Anlage an das Land Brandenburg zurückgeführt werden sollte.

Da zum Prüfungszeitpunkt noch keine klare Konzeption zur Übernahme bzw. Beseitigung der Datenträger sowie zur Löschung ihrer Inhalte vorgelegt werden konnte, war festzustellen, daß eine ordnungsgemäße Auflösung des ZER zu diesem Zeitpunkt nicht gewährleistet war.

Weiteres Schicksal der Datenbestände

Die Datenschutzbeauftragten der neuen Länder und Berlins stellten hinsichtlich der im ZER vorgehaltenen melderechtsfremden Projekten fest, daß diese Datenbestände zur Wahrung schutzwürdiger Belange der Betroffenen und für Zwecke der juristischen und historischen Aufarbeitung bedeutsam sein können. Sie seien deshalb noch nicht zu vernichten, sondern bis auf weiteres in behördliche Obhut zu nehmen und aufzubewahren. Ihre spätere Verwendung sei mit den betroffenen Ländern abzustimmen.

Außerdem wurden die Innen-, Justiz- und Archivbehörden des Bundes und der beteiligten Länder aufgefordert, dies übergangslos sicherzustellen. Dazu empfahlen die Datenschutzbeauftragten die rasche Einrichtung einer Abwicklungsstelle, die auch dazu notwendig sei, die Sicherheit der Daten bei der bereits begonnenen Auflösung des ZER und des Rechenzentrums zu gewährleisten.

Ende Oktober entschieden die Melderechtsreferenten der neuen Bundesländer und Berlins, daß der Rechenbetrieb im ZER Anfang November endgültig eingestellt wird. Dem Wunsch des *Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes* und der *Zentralen Ermittlungsstelle für Regierungs- und Vereinigungskriminalität,* aufbereitete Daten aus dem *Meldebestand* und den Projekten zu erhalten, könne erst nach Schaffung entsprechender Rechtsgrundlagen nachgekommen werden. Dem Bundesarchiv wurden der Meldedatenbestand und die Projektdaten zur Zwischenlagerung überlassen.

Die derzeitige Rechtslage schließt eine Nutzung sämtlicher Daten durch das *Bundesarchiv* aus. Da Melde- und Fachverwaltungsdaten als wesentlicher Bestandteil des ZER mit dessen Auflösung zumindest einem Verwertungsverbot unterliegen, ist ein Zugang zu diesen Daten bzw. eine Übermittlung der Daten an eine andere Stelle nur auf Grund einer ausdrücklichen Rechtsgrundlage möglich.

Hinsichtlich der Projektdaten sind weiterhin die jeweils zuständigen Stellen, in der Regel Stellen der neuen Bundesländer und Berlins, als datenverarbeitende Stellen zu betrachten. Über eine weitere Nutzung kann erst entschieden werden, wenn diese erklären, daß eine Erforderlichkeit für die Nutzung der Daten in ihrem Bereich besteht. Vor einer Löschung dieser Daten sind Löschungsverbote zu beachten.

3.3 Alteigentümer als informationelles Freiwild?

In einer Berliner Zeitung wurde berichtet, daß Anschriften von Alteigentümern und Anwälten, die Rückübertragungsansprüche auf Grundstücke und Häuser im Bezirk Mitte von Berlin gestellt hatten, an Berliner Maklerbüros weitergegeben worden waren. Die von uns noch am gleichen Tag aufgenommene Überprüfung im Landesamt zur Regelung offener Vermögensfragen (LAROV) bezog sich vor allem auf die Herkunft der der Zeitungsredaktion zugespielten Listenausdrucke *(„Maklerlisten")*, von denen uns Kopien übergeben wurden.

Der Überprüfung lagen im wesentlichen zwei Fragestellungen zugrunde:

- Sind die „Maklerlisten" im LAROV erstellt worden bzw. stammten die darin enthaltenen Daten aus dem LAROV?
- Begünstigten die vom LAROV getroffenen technisch-organisatorischen Maßnahmen den Mißbrauch der Daten?

Technische Prüfung des LAROV

Das seit Herbst 1989 existierende LAROV erledigte anfänglich seine Aufgaben auf bis zu 30 nicht miteinander vernetzten Personalcomputern. Auf jedem PC waren immer nur Teildatenbestände gespeichert. Später wurde eine DV-Herstellerfirma vom Bundesminister für Justiz beauftragt, die entsprechende Hardware und die erforderlichen Programme sowohl für den Bund als auch für Berlin und die fünf neuen Bundesländer zu entwickeln und bereitzustellen, um die Einzeldatenbestände zu einem Gesamtdatenbestand vereinigen zu können. Im LAROV wurden daraufhin zwei Rechner mit dem Betriebssystem UNIX installiert und die PC-Daten auf die Plattenspeicher der neuen Rechneranlage übertragen.

Die vorher nur zur Datenerfassung eingesetzten PCs wurden nach der Datenzusammenführung im wesentlichen als Endgeräte genutzt.

Die *Prüfung der UNIX-Systeme* ergab, daß zur Zeit der Prüfung keine Programme vorhanden waren, mit denen aus der Datenbank ein Ausdruck der Listen in der gesuchten Form möglich gewesen wäre. Einzelabfragen waren aber von jedem Terminal in unbegrenzter Anzahl möglich. Wegen der fehlenden Dokumentationen und der fehlenden Schulung der Mitarbeiter wurde jedoch keine Protokolldatei geführt bzw. ausgewertet, so daß nicht geprüft werden konnte, ob und wenn ja, in welchem Umfang solche Abfragen getätigt worden waren.

Die Prüfung zeigte insgesamt, daß die vom LAROV getroffenen technisch-organisatorischen Maßnahmen so mangelhaft waren, daß sie einen Mißbrauch der Datenverarbeitung außerordentlich begünstigt hätten:

Für die verschiedenen Systemaufgaben wurden keinerlei Handbücher (z. B. System-, Administrations- und Bedienerhandbuch) vorgefunden. Organisationsabläufe, Programmdokumentationen, Dokumentationen über Sicherungsmaßnahmen sowie Aufstellungspläne für Geräte lagen nicht vor. Die Systemverwalter waren unzureichend geschult.

Zu viele Mitarbeiter hatten hochprivilegierte Systemverwalterkennungen. Von jedem Terminal aus war der Zugriff mit diesen Privilegien möglich. Die für diese Kennungen durchgeführten Kontrollmaßnahmen waren nicht ausreichend, eine Funktionstrennung zwischen diesen hochprivilegierten Benutzern war nicht vorgesehen.

Zur Datenbanknutzung wurde zwar eine umfangreiche Protokolldatei vorgefunden; ein Auswertungsprogramm dafür war jedoch nicht vorhanden. Damit konnten auch mit dieser Protokolldatei keine Erkenntnisse über die veröffentlichten Listen gewonnen werden, da die Datei immer nur für eine Woche gespeichert wurde.

Alle Dateien der LAROV-Datenbank waren allen Benutzern zugänglich. Irgendwelche Zugriffsbeschränkungen auf Teile von Datensätzen, Datentabellen oder einzelne Felder waren nicht realisiert.

Insgesamt ließ sich feststellen, daß mit an Sicherheit grenzender Wahrscheinlichkeit die Maklerlisten nicht im LAROV gedruckt worden sind. Weder dafür geeignete Software noch ein geeigneter Rechner oder Drucker war im Rahmen der PC-Prüfung aufzufinden. Allerdings war auf Grund der mangelnden Sicherungen nicht auszuschließen, daß die Daten in anderer Form aus dem LAROV *herausgegeben* worden waren.

Senatsverwaltung für Finanzen und LAROV haben die Beanstandungen zu technischen und organisatorischen Aspekten im vollen Umfang akzeptiert und die Beseitigung aller Mängel und die Beachtung unserer Empfehlungen zugesagt. Eine spätere Nachprüfung bestätigte die Umsetzung.

Datenübermittlung an andere Stellen

Auf Grund einer weiteren Zeitungsmeldung wurde bekannt, daß das LAROV im Sommer 1991 ca. 60 Adressen von Antragstellern an einen Investor, der ein Geschäftscenter errichten will, herausgegeben hat. Diese Meldung, die von der Senatsverwaltung für Finanzen bestätigt wurde, nahmen wir zum Anlaß, die Zulässigkeit der Weitergabe von Daten der Alteigentümer an Investoren einer grundsätzlichen Prüfung zu unterziehen.

Das LAROV übermittelte bis Oktober 1991 die Daten von Antragstellern, die Rückübertragungsansprüche nach dem Vermögensgesetz angemeldet hatten, an *private Investoren* im Rahmen von Investitionsgenehmigungsverfahren. Da die nach dem Berliner Datenschutzgesetz erforderliche Befugnisnorm zum damaligen Zeitpunkt fehlte und erst in der Novellierung des Vermögensgesetzes vom Juli 1992 geschaffen wurde, war diese Übermittlung unzulässig.

Bei der Überprüfung wurde festgestellt, daß das LAROV darüber hinaus personenbezogene Daten von Antragstellern an eine Vielzahl weiterer öffentlicher und privater Stellen übermittelt.

Bei den beteiligten Stellen haben wir vor Ort Überprüfungen vorgenommen mit besonderem Augenmerk auf die technisch-organisatorischen Sicherungen der Datenspeicherungen, auch um herauszufinden, ob möglicherweise die in Maklerkreisen kursierenden Listen bei einer dieser Stellen hergestellt wurden bzw. die Daten dorther stammten. Prüfungsgegenstand war ferner die Zulässigkeit der Datenübermittlungen an diese Stellen.

In der Geschäftsstelle des *Koordinierungsausschusses für innerstädtische Investitionen* (KOAI) bei der Senatsverwaltung für Bau- und Wohnungswesen wurden dabei ebenfalls schwerwiegende datenschutzrechtliche Mängel in technisch-organisatorischer Hinsicht festgestellt.

Ungehindert hatten wir Zutritt zu den Räumen, in denen drei PCs installiert waren, die sich nach Einschalten als betriebsbereit erwiesen. Auf einem der PCs befand sich eine Datenbank mit 1548 Daten von Anspruchsberechtigten. Der Zugang hierzu war zwar durch ein Paßwort gesichert, dieses war jedoch durch geschicktes Probieren leicht herauszufinden. Auf der Gehäuserückseite steckte der Schlüssel in einem Schloß, das eigentlich den manuellen Zugriff auf Hardware-Bauteile des Gerätes verhindern soll. Im Ergebnis hätte diese Situation die unbefugte Herausgabe der Daten erleichtert, wenn auch hier ebenfalls keine konkreten Anhaltspunkte vorlagen.

Wegen der unzureichenden räumlichen Sicherung, der mangelhaften Gerätesicherungen sowie weiterer erheblicher technisch-organisatorischer Mängel bei der Aktensicherung wurde eine Beanstandung ausgesprochen. Die festgestellten Mängel wurden behoben, wie auch eine spätere Nachprüfung ergab.

Zu differenzierten Ergebnissen führte die Prüfung der *Rechtsgrundlagen für die Übermittlungen.* Die einzige Übermittlungsbefugnis im zum Zeitpunkt der Prüfung geltenden Vermögensgesetz ließ Auskünfte aus dem LAROV über Antragstellungen nur an betroffene Rechtsträger, staatliche Verwalter sowie Dritte, deren rechtliche Interessen durch den Ausgang des Restitutionsverfahrens berührt werden, zu (§ 31 Abs. 2).

Eine Ermächtigung zur Übermittlung von Daten an andere öffentliche Stellen enthielt das Vermögensgesetz nicht, es sei denn, diese sind von dem in § 31 Abs. 2 Vermögensgesetz genannten Empfängerkreis erfaßt.

Nach der Neufassung des Vermögensgesetzes im Juli 1992 kam eine weitere Übermittlungsnorm hinzu, wonach jedem, der ein berechtigtes Interesse glaubhaft darlegt, Name und Anschrift von Antragstellern sowie der Vermögenswert mitgeteilt werden darf. Die Antragsteller haben hiergegen ein Widerspruchsrecht. Zielrichtung dieser Vorschrift ist es, nunmehr auch die Weitergabe der personenbezogenen Daten von Anmeldern an Investoren zu ermöglichen. Potentiellen Investoren soll die Möglichkeit zu einer direkten Einigung mit dem Anmelder eingeräumt werden, um im Ergebnis eine Verkürzung des Verfahrens zu erreichen.

Eine Ermächtigung zur Weitergabe von Daten an Makler oder Immobilienfirmen, die nur für die Kundenanwerbung an diesen Angaben interessiert sind, ist diese Vorschrift nach wie vor nicht.

Eine Befugnis zur Datenübermittlung an andere öffentliche Stellen, die nicht unter § 31 Abs. 2 Vermögensgesetz fallen, ist wiederum nicht aufgenommen worden. Soweit für öffentliche Stellen personenbezogene Informationenen über Antragstellungen für die Erfüllung ihrer gesetzlich zugewiesenen Aufgaben erforderlich sind, fehlen entsprechende Rechtsvorschriften.

Ohne gesetzliche Ermächtigung war eine Übermittlung personenbezogener Daten auf Grund der Übergangsvorschrift des § 34 Abs. 1 BlnDSG bis zum 31. Januar 1993 zulässig, wenn die Kenntnis der Daten zur rechtmäßigen Aufgabenerfüllung der anfragenden Stelle erforderlich ist. Nach Ablauf dieser Übergangsfrist ist eine Datenübermittlung an andere öffentliche Stellen auf Grund des BlnDSG nur noch zulässig, wenn die Daten vom Empfänger zur Erfüllung des gleichen Zwecks benötigt werden, zu der sie erhoben wurden (§ 12 Abs. 1 Satz 2 BlnDSG).

Hinsichtlich der einzelnen überprüften Stellen führte dies zu folgender Bewertung:

Die *Geschäftsstelle des Koordinierungsausschusses für innerstädtische Investitionen* bei der Senatsverwaltung für Bau- und Wohnungswesen erfüllt andere Aufgaben als das LAROV, da Investitionsberatung und Anspruchsprüfung verschiedenen Zwecken dienen. Die Rechtmäßigkeit der Übermittlung hätte damit die Einwilligung der Betroffenen vorausgesetzt. Mangels gesetzlicher Aufgabenzuweisung konnte auch der Übergangsbonus nicht in Anspruch genommen werden.

Die in derselben Verwaltung angesiedelte *Geschäftsstelle für die Erteilung von Investitionsbescheinigungen* fällt hingegen Entscheidungen, die in der Rechtsstellung der Antragsteller eingreifen und damit in unmittelbarem Zusammenhang mit der Feststellung der Eigentumsverhältnisse stehen. Entgegen unserer ursprünglichen Einschätzung finden die Übermittlungen hier nicht nur im Übergangsbonus, sondern auch in der Zweckgleichheit ihre Rechtsgrundlage.

Die Übermittlungen an das für *Bodenwirtschaft und Grundstückswertermittlung* zuständige Referat waren hingegen schon deswegen unzulässig, weil ein Personenbezug für diese Aufgaben nicht erforderlich ist.

Ebenfalls nicht mit den rechtlichen Vorgaben in Übereinstimmung stand die Übermittlung der Daten von Alteigentümer an private *Sanierungsträger.* Sie wäre nur auf Grund einer ausdrücklichen Rechtsgrundlage oder mit Einwilligung der Betroffenen zulässig gewesen[57]: § 138 Abs. 1 Baugesetzbuch sieht zwar eine Erhebungsbefugnis vor, geht aber von einer Datenerhebung bei den Betroffenen selbst aus und normiert eine entsprechende Auskunftspflicht. Dies bedeutet, daß bei einer Datenerhebung bei dritten Stellen die Betroffenen um ihre Einwilligung zu bitten sind. Im Hinblick auf eine konkrete Initiative der Senatsverwaltung für Finanzen, das Vermögensgesetz erneut zu ändern, wurden die Übermittlungen allerdings für eine Übergangszeit hingenommen.

Das *Ausgleichsamt* im Geschäftsbereich der Senatsverwaltung für Finanzen erteilte zeitweise ebenfalls Auskünfte und hielt hierfür ca. 100 000 Adressen von Anmeldern und Anschriften von restitutionsbefangenen Grundstücken vor. Zwar ist grundsätzlich eine derartige Datenverarbeitung im Auftrag möglich; die Zulässigkeit der Auskünfte selbst richtet sich jedoch nach den Kriterien für das LAROV, das nach wie vor datenverarbeitende Stelle bleibt.

Unzulässig waren schließlich auch Datenübermittlungen aus dem LAROV an verschiedene *Grundbuchämter.* Für diese waren die Daten nicht erforderlich, da das durch den Antrag auf Rückübertragung nach § 3 Abs. 3 VermG ausgelöste Verbot für den Verfügungsberechtigten, dingliche Rechtsgeschäfte abzuschließen, kein Eintragungshindernis im Sinne des § 18 Grundbuchordnung ist.

In keinem der Fälle war für die Beurteilung der Übergangsbonus des § 34 Abs. 1 BlnDSG letztendlich heranzuziehen. Dessen Ablauf hatte damit keinen Einfluß auf unsere Beurteilung.

Gleichwohl haben wir angeregt, in einem Ausführungsgesetz zum Vermögensgesetz bereichsspezifische Bestimmungen zu schaffen, die in klarerer Weise, als dies bisher der Fall ist, die Datenbeziehungen zwischen der Vielzahl der am Restitutionsprozeß beteiligten öffentlichen und nichtöffentlichen Stellen regeln.

Massenoffenbarungen bei der Bahnplanung

Auf einen erheblichen Verstoß gegen das Grundrecht auf informationelle Selbstbestimmung durch die Bundesregierung machten wir den Bundesbeauftragten für den Datenschutz aufmerksam:

Im August 1992 leitete die Bundesregierung dem Bundesrat den Entwurf eines Gesetzes über den Bau der *„Südumfahrung Stendal"* der Eisenbahnstrecke Berlin - Oebisfelde (Hochgeschwindigkeitsverbindung Berlin - Hannover)[58] zu. Dabei handelt es sich um ein Investitionsmaßnahmengesetz, mit dem der Zeitraum für die Bauzulassung erheblich verkürzt werden sollte. Der Gesetzentwurf der Bundesregierung enthielt umfangreiche Anlagen, darunter auch ein Grunderwerbsverzeichnis, in dem die Eigentümer der von der Planung betroffenen Grundstücke, Antragsteller auf Rückübertragung nach dem Vermögensgesetz sowie Inhaber dinglicher Rechte (z. B. Altenteil, mietfreies Wohnrecht und monatliche Rente) aufgeführt waren. In einer weiteren Anlage waren Einwendungen von Bürgern gegen das Bauvorhaben in personenbezogener Form dem Gesetzentwurf beigefügt. Die Bundesratsdrucksache wurde in der üblichen hohen Stückzahl gedruckt und verteilt.

In dieser Veröffentlichung sensibler personenbezogener Daten lag ein schwerer Eingriff in das informationelle Selbstbestimmungsrecht der Eigentümer, Rechtsinhaber, Antragsteller auf Rückübertragung und Bürger, die Einwendungen erhoben hatten. Das Bundesverfassungsgericht hat bereits im Jahre 1990 festgestellt, daß die Veröffentlichung von Einwendungen in personenbezogener Form in der Begründung eines Planfeststellungsbeschlusses das Gebot der Zweckbindung personenbezogener Daten verletzt[59]. Bürger, die im Planungsverfahren Einwendungen erheben oder einen Antrag auf Rückübertragung stellen, offenbaren der zuständigen Behörde ihre personenbezogenen Daten zu einem ganz bestimmten Zweck. Werden die Daten anschließend veröffentlicht, so wird dieser Zweck durchbrochen, weil für die Betroffenen nicht mehr feststellbar ist, wer von diesen Daten Kenntnis erhält und zu welchen Zwecken er sie weiterverwendet. Der Bundesbeauftragte forderte die Bundesregierung auf, umgehend alles zu tun, um den rechtswidrigen Eingriff in die Rechte der Bürger zu beenden.

Die Bundesregierung begnügte sich damit, die personenbezogenen Angaben in der Drucksache zur Einbringung in den Bundestag[60] zu verschlüsseln.

[57] § 13 BlnDSG

[58] BR-Drs. 513/92

[59] Beschluß vom 24. 7. 1990, CR 1990, S. 798

[60] BT-Drs. 12/3477

4. Ausgewählte Geschäftsbereiche

4.1 Gesundheit

Gesundheitsstrukturgesetz

Wieder einmal hat in dem Berichtsjahr die Kostendämpfung im Gesundheitswesen im Vordergrund der öffentlichen Diskussion gestanden. Durch das Gesundheitsstrukturgesetz, das trotz aller Kritik am 1. Januar 1993 in Kraft getreten ist[61], soll der explosionsartige Anstieg der Kosten bei den Krankenversicherungen gebremst werden.

Die Datenschutzbeauftragten haben wie schon bei dem Gesundheitsreformgesetz 1988 bezweifelt, daß die vermehrte Anwendung der Datenverarbeitungstechnik und die *vermehrte Erhebung medizinischer Daten durch die Krankenversicherungen* geeignet sind, den beabsichtigten Effekt der Kostendämpfung herbeizuführen. Diese Auffassung ist von der Entwicklung der letzten zwei Jahre bestätigt worden. Mit dem Gesundheitsstrukturgesetz 1993 ist jedoch der problematische Weg, die Kosten im Gesundheitswesen durch mehr Datenverarbeitung zu dämpfen, mit noch größerer Entschiedenheit beschritten worden.

Bereits beim Gesundheitsreformgesetz wurde die Einführung eines *patientenbezogenen Leistungskontos* diskutiert. Der Gesetzgeber hat damals - wegen der erheblichen Gefahren für das informationelle Selbstbestimmungsrecht der Patienten - die Einführung einer solchen Einrichtung abgelehnt.

Besonders problematisch ist in dieser Hinsicht der neue § 303 Abs. 3 Sozialgesetzbuch V. Buch (SGB V). Nach dieser Regelung dürfen Krankenkassen ab dem 1. Januar 1995 Abrechnungen der Leistungserbringer (Ärzte, Krankenhäuser) nur vergüten, wenn die Daten maschinenlesbar oder auf maschinell verwertbaren Datenträgern gespeichert oder übermittelt worden sind. In Verbindung mit den Regelungen in den §§ 234, 285 und 301 SGB V soll hierdurch der Druck auf die Leistungserbringer zur Einführung der *maschinenlesbaren Übermittlungstechnik* von Abrechnungsdaten und ihre maschinelle Auswertung erheblich verstärkt werden. Obwohl das Bundesverfassungsgericht im Volkszählungsurteil 1983 in unmißverständlicher Weise auf die Gefahren, die durch die automatische Datenverarbeitung dem Individuum drohen, hingewiesen und den Gesetzgeber aufgefordert hat, „mehr als früher die organisatorischen und verfahrensrechtlichen Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken", soll das Gesetz hier augenscheinlich genau das Gegenteil bewirken, nämlich eine Entwicklung erzwingen, durch die die Nutzung der automatischen Datenverarbeitung einen wesentlichen Schub erfahren soll, und dies in einem Bereich, der von jedem Individuum als besonders empfindlich angesehen wird.

Wird zusätzlich zu der in § 303 Abs. 4 SGB V vorgesehenen Regelung die *Krankenversichertenkarte* - wie zur Zeit beabsichtigt - *als Chipkarte* eingeführt, so ist damit für die Anwender die technische Option für die Speicherung von Gesundheitsdaten der Versicherten aus den Krankenversichertendaten über die gegenwärtige gesetzliche Grundlage des § 291 SGB V hinaus eröffnet[62]. Zugleich wird die Automatisierung der Datenverarbeitung in der Krankenversicherung es ermöglichen, die Leistungsdaten der Versicherten auf neue Art zu verknüpfen und versichertenbezogen auszuwerten.

Gesundheitsprofile der Versicherten können gerade deshalb leichter erstellt werden als bisher, weil § 284 SGB V jetzt die maschinelle Speicherung aller Leistungsdaten bei den Krankenkassen zuläßt. Zugleich hat der Gesetzgeber die Forderung der Datenschutzbeauftragten nicht berücksichtigt, zumindest ein ausdrückliches Verbot der versichertenbezogenen Auswertung dieser sensiblen Datenbestände festzuschreiben.

Ausnahmslos schreibt das Gesetz jetzt auch die Aufzeichnung der *Diagnosen in den ärztlichen Abrechnungsunterlagen* und ihre Übermittlung an die Krankenkassen vor, obwohl die Zweifel der Datenschutzbeauftragten an der Erforderlichkeit der Diagnose für die Leistungsabrechnung nicht ausgeräumt sind.

Schließlich verpflichtet das Gesundheitsstrukturgesetz die *Krankenhäuser,* sehr viel mehr Patientendaten, als bisher für erforderlich gehalten wurde, an die Krankenkassen zu übermitteln (§ 301 SGB V). Der Umfang der zu übermittelnden Daten soll durch Vereinbarung lediglich dann eingeschränkt werden können, „wenn dadurch eine ordnungsgemäße Abrechnung und die Erfüllung der gesetzlichen Aufgaben der Krankenkassen nicht gefährdet werden" (§ 303 Abs. 1 SGB V). Damit hat der Gesetzgeber eine verfassungsrechtlich bedenkliche Datenübermittlung auf Vorrat angeordnet, deren Beschränkung auf das erforderliche und damit zulässige Maß er den Verbänden der Krankenkassen und Leistungserbringer überläßt.

Einstieg in die Vernetzung von Polizei und Krankenkasse?

Durch den Ausschuß für Arbeit des Abgeordnetenhauses von Berlin, die Senatsverwaltung für Inneres sowie die Staatsanwaltschaft und den Polizeipräsidenten ist der Wunsch an die AOK herangetragen worden, ein Datensichtgerät der AOK Berlin im Rahmen der Zusammenarbeit in der *Gemeinsamen Ermittlungsgruppe Schwarzarbeit (GES)* in den Räumen der Berliner Polizei bereitzustellen. Damit sollten Möglichkeiten der schnellen Information aus den Datenbeständen der Sozialversicherung für Arbeitgeber und Versicherte geschaffen werden. Das Datensichtgerät sollte sich in einem verschließbaren, nur von den Mitarbeitern der AOK benutzten Raum befinden.

Es war zwar gewährleistet, daß die Zugriffsberechtigung nur den Mitarbeitern der AOK Berlin gestattet sein sollte. Gleichwohl haben wir gegen die Planung erhebliche Bedenken geäußert. Sie resultierten weniger aus einer rechtlichen Beurteilung der Befugnisse der geplanten gemeinsamen Ermittlungsgruppe. Die Regelung in § 306 SGB V wird man so zu verstehen haben, daß Angaben über die Tatsachen, die für die Einziehung der Beiträge zur Kranken- und Rentenversicherung erheblich sind (Versichertenstatus, Arbeitgeber) im Einzelfall von der AOK übermittelt werden dürfen, wenn sich konkrete Anhaltspunkte für Verstöße gegen das *Gesetz zur Bekämpfung der illegalen Beschäftigung* ergeben. Ob diese Anhaltspunkte bestehen, wird die AOK allerdings nicht allein mit Hilfe der Daten feststellen können, die über ein Terminal abrufbar sind. Vielmehr ist hierfür der Zugriff auf Akten und andere Unterlagen erforderlich, die nur in den Geschäftsräumen der AOK selbst verfügbar sind.

Von besonderer Bedeutung war ein informationspolitisches Argument: Nicht nur muß vermieden werden, daß in der Öffentlichkeit ein (möglicherweise falsches) Bild über die Vermengung der Datenbestände von Sicherheits- und Sozialbehörden entsteht. Vielmehr kann angesichts der modernen Möglichkeiten der informationstechnischen Vernetzung die vom Bundesverfassungsgericht als Teil des Rechtsstaatsprinzips anerkannte „informationelle Gewaltenteilung" nur aufrechterhalten bleiben, wenn die einzelnen Verwaltungsbereiche mit ihren Datenbeständen auch räumlich klar voneinander getrennt sind. Eine wie auch immer geartete gesetzliche Zusammenarbeitsverpflichtung kann an diesem Erfordernis nichts ändern. Wir haben deshalb empfohlen, auf die Realisierung des Vorschlages in der geplanten Form zu verzichten. Der Senat ist unserem Vorschlag gefolgt[63]

Gesundheitsakten: ein besonderes DDR-Vermächtnis

Ein östliches Bezirksamt fragte an, ob es Untersuchungsdaten aus der ehemaligen zentralen Poliklinik der Bauarbeiter der Bauberufsgenossenschaft Hannover zur Verfügung stellen dürfe. Diese hatte die Herausgabe der Unterlagen gefordert, weil ihr als dem Träger der gesetzlichen Unfallversicherung für die Bauwirtschaft Aufgaben nach dem Sozialgesetzbuch und der Reichsversicherungsordnung zur Prävention sowie der Rehabilitation und gegebenenfalls der Kompensation zur Verhütung bzw. Entschädigung von Arbeitsunfällen und Berufskrankheiten obliegen. Für alle genannten Aufgabenbereiche könnten „verwertbare Untersuchungsdaten gute Hilfe leisten". So könnte es beispielsweise im Rahmen der Prävention möglich sein, durch entsprechende Auswertungen neue arbeitsmedizinische Erkenntnisse zu gewinnen.

---

61 BGBl. 1992 I, S. 2266 ff.

62 vgl. dazu Entschließung der 44. DSB-Konferenz, Anlage 2.5

63 vgl. Mitteilung über Maßnahmen zur effektiveren Bekämpfung der Schwarzarbeit, Drs. 12/2248, S. 3 f.

Die Nutzungsmöglichkeiten ersetzen noch keine Rechtsgrundlage. Die Daten unterliegen der ärztlichen Schweigepflicht. Eine Offenbarung derart geschützter personenbezogener Daten setzt eine gesetzliche Regelung voraus. In Betracht kommen nur die Vorschriften der *Reichsversicherungsordnung (RVO)*. Mitteilungspflichten, die dem Träger der betrieblichen Poliklinika oder den Ärzten nach der RVO auferlegt worden sind, gehen - bei der Auflösung der Einrichtung - auf den Rechtsnachfolger der Einrichtung oder auf diejenige Stelle über, die die datenschutzrechtliche Verantwortung für das verbleibende personenbezogene Informationsmaterial übernimmt. Gemäß § 1543 c RVO ist der Unternehmer verpflichtet, seine Genossenschaft bei der Durchführung der *Unfallversicherung* zu unterstützen und ihr Auskunft über Behandlung und den Zustand des Verletzten zu erteilen. Bei dem dem Schreiben des Bezirksamts Marzahn zugrundeliegenden Fall existierte der Unternehmer jedoch nicht mehr. Wer als Rechtsnachfolger jeweils in Betracht kommt, muß in jedem einzelnen Fall gesondert geprüft werden. § 1543 c RVO betrifft nur den aktuellen einzelnen Krankheitsfall, und regelt keine pauschale Datenübermittlungsbefugnis einer so großen Datenmenge wie bei den hier strittigen Unterlagen. Das gleiche gilt auch für die Auskunftspflicht des Arztes nach § 1543 d RVO oder nach den Vorschriften der Berufskrankheiten-Verordnung, die den behandelnden Arzt verpflichten, dem Träger der Unfallversicherung Auskunft über die Behandlung und den Zustand des Verletzten zu erteilen.

Nach diesen Vorschriften kann zwar in jedem Einzelfall - auch nach Abschluß der Behandlung - das Bezirksamt, soweit es die Patientenunterlagen tatsächlich auch verwaltet, über § 1543 c und d RVO verpflichtet werden, dem Träger der Unfallversicherung oder der jeweils zuständigen Genossenschaft Auskunft zu erteilen. Es kann jedoch nicht daraus abgeleitet werden, daß das gesamte Aktenmaterial an die Genossenschaft herausgegeben wird. Dies ergibt sich auch aus der Auslegung des Begriffs „Auskunft". Die Senatsverwaltung für Gesundheit hat sich der von uns vertretenen Auffassung angeschlossen.

Im Jahresbericht für 1991[63] hatten wir über die *Auflösung des Regierungs- und Diplomatenkrankenhauses* berichtet. Durch die Art der Unterbringung war umfangreiches Patientenmaterial einer außerordentlichen Gefährdung ausgesetzt, da der verantwortliche Träger nicht mehr existierte. Im Wege der ordnungsrechtlichen Ersatzvornahme hat das Bezirksamt Mitte die Akten und den ordnungsgemäßen Transport in vorläufig geeignete Lagerräume veranlaßt.

Dieser Vorfall wies eindringlich auf das grundsätzliche Problem hin, daß durch die Abwicklung zahlreicher DDR-Einrichtungen und der damit zusammenhängenden ärztlichen Behandlungsstätten eine Flut von Patientendokumentationen herrenlos wird, ohne daß geeignete Sicherheitsmaßnahmen und die künftige Verwendung sichergestellt waren.

Wir haben die Senatsverwaltung für Gesundheit und die Bezirksämter auf diese drohende Gefahr aufmerksam gemacht und die Bezirke (Abteilung Gesundheitswesen) aufgefordert, ihre ordnungsrechtliche Verantwortung gegenüber höchst sensiblen medizinischen Unterlagen wahrzunehmen. Wir haben empfohlen, *Richtlinien zur Patientenaktenverwaltung* durch die bezirklichen Gesundheitsämter herauszugeben. Den von uns erhobenen Forderungen zur Verwaltung und Nutzung des Datenmaterials wurde im wesentlichen entsprochen.

Die Richtlinien enthalten insbesondere Anweisungen über die *Lagerung der Patientenunterlagen* in Räumen mit geeigneten Sicherheitsvorkehrungen. Insbesondere ist sichergestellt, daß eine strikte Trennung der Patientenunterlagen von den sonstigen Unterlagen der Gesundheitsämter einzuhalten ist. Es handelt sich hierbei nicht um eine im Gesetz über den öffentlichen Gesundheitsdienst definierte Aufgabe des öffentlichen Gesundheitswesens. Vielmehr nimmt der Bezirk die Verwaltung der Patientenunterlagen im Wege der ordnungsrechtlichen Ersatzvornahme vor und darf Daten aus diesen Unterlagen nicht zur Erfüllung öffentlicher Aufgaben verwenden. Er hat bei der Ersatzvornahme die Einhaltung der ärztlichen Schweigepflicht auch für die Zukunft zu garantieren und dabei zugleich auch das Material zugriffsfähig vorzuhalten, so daß für Zwecke der Weiterbehandlung oder zur persönlichen Einsicht in die Patientenunterlagen durch den Betroffenen selbst jederzeit Zugriff genommen werden kann.

Um die Rechte des Patienten wirkungsvoll zu respektieren, haben wir empfohlen, gegen einen entsprechenden Aushändigungsnachweis auf Wunsch des Patienten dem behandelnden Arzt die Originalakte auf Dauer zur Verfügung zu stellen.

Offenbarung medizinischer Daten

Vom Amts- und Vertrauensärztlichen Dienst eines Gesundheitsamts wurden wir befragt, ob einem Taxi- oder Busfahrer, der sich dem Landeseinwohneramt gegenüber weigert, daß ihn betreffende medizinische Daten vom Gesundheitsamt an das Landeseinwohneramt übermittelt werden, die Verlängerung seines Taxi-/Busscheines versagt werden darf. Denn es müßte dem Landeseinwohneramt genügen, wenn vom Amts- und Vertrauensärztlichen Dienst mitgeteilt wird, daß z. B. eine vorzeitige Nachuntersuchung durchgeführt werden sollte, oder daß der Taxi- oder Busfahrer nicht fahrtauglich ist, ohne dabei medizinische Daten im einzelnen zu offenbaren.

Ausgangspunkt der datenschutzrechtlichen Überlegungen ist § 2 Abs. 5 Berufsordnung der Ärztekammer von Berlin (BOÄ). Danach ist der Arzt auch dann zur Verschwiegenheit verpflichtet, wenn er im amtlichen oder privaten Auftrag eines Dritten tätig wird, es sei denn, daß dem Betroffenen vor der Untersuchung oder Behandlung bekannt war oder eröffnet wurde, inwieweit die von dem Arzt getroffenen Feststellungen zur Mitteilung an Dritte bestimmt sind. Aus dieser Vorschrift haben wir den Schluß gezogen, daß der betroffene Patient allein durch die *Teilnahme an einer Begutachtung* in der Regel nur sein Einverständnis dafür gibt, daß eine Mitteilung über das Ergebnis der Begutachtung in Form eines Kürzels - wie „geeignet" oder „ungeeignet" - übermittelt wird. Im Normalfall kann das Einverständnis zur Offenbarung des Gutachtens auch dann zugunsten des Betroffenen angenommen werden, wenn damit seinen objektiven, rechtlichen oder wirtschaftlichen Interessen gedient ist.

Sollte sich aus der Begutachtung jedoch ergeben, daß das Ergebnis der Untersuchung den Vorstellungen oder den Interessen des Begutachteten zuwiderläuft, so kann nicht von einem Einverständnis i. S. d. § 2 Abs. 5 BOÄ ausgegangen werden. Denn die Vorschrift unterstellt eine Einwilligung, die durch schlüssiges Verhalten erklärt wurde. Eine solche „Erklärung" darf nicht überinterpretiert werden und ist daher einengend auszulegen. Wenn also überraschende oder dem Interesse des Betroffenen zuwiderlaufende Ergebnisse sich aus der Untersuchung ergeben, darf auch der auftraggebenden Stelle hierüber keine Mitteilung gemacht werden, solange nicht der Betroffene dazu ausdrücklich sein Einverständnis erklärt hat. Ihm ist zumindest eine Gelegenheit zum Widerspruch zu geben. Dies bedeutet, daß in dem hier zugrundeliegenden Fall ohne Einverständnis des Betroffenen keine Informationen über den Ausgang der Begutachtung an das Landeseinwohneramt übermittelt werden dürfen. Wohl aber darf übermittelt werden, daß die Begutachtung durchgeführt wurde und daß das Ergebnis aus Gründen, die das Amt nicht zu vertreten hat, an die auftraggebende Stelle nicht weitergegeben werden kann.

Im Ergebnis führt dies zwar dazu, daß die medizinischen Daten beim Arzt verbleiben; jedoch kann dann von der auftraggebenden Stelle ohne weiteres eine Entscheidung zum Nachteil des Betroffenen gefällt werden, wobei dieser in der Pflicht steht, den Gegenbeweis für einen anderen Sachverhalt zu erbringen.

Geschlechtskrankenvorsorge mit den falschen Methoden

Ein zwischenzeitlich aus Berlin weggezogenes Ehepaar beschwerte sich bei uns darüber, daß es von einer bezirklichen Beratungsstelle für Geschlechtskrankheiten unter seiner alten Berliner Anschrift angeschrieben und ein persönliches Beratungsangebot erhalten hatte. Eingeleitet wurde dieses Angebot mit dem Hinweis, daß unter der Telefonnummer des Ehepaares in einem Boulevardblatt geworben werde.

[63] siehe 2.2

Die *Beratungsstelle für Geschlechtskrankheiten* wertet routinemäßig *Kontaktanzeigen von Prostituierten* und anderen Personen, bei denen sie eine Beratung für angebracht hält, aus und fragt bei der Deutschen Bundespost TELEKOM an, wer der Inhaber des in der Anzeige genannten Telefonanschlusses ist. Die TELEKOM teilt daraufhin Namen und Anschrift der Anschlußinhaber mit. Diese Auskunft war in dem genannten Fall falsch, weil die TELEKOM vier Wochen nach dem Umzug des Ehepaares nach Baden-Württemberg und der Ummeldung des Telefonanschlusses ihre Kundendatei noch nicht berichtigt hatte.

Die *Übermittlung der Kundendaten durch die TELEKOM* wäre jedoch auch dann rechtswidrig gewesen, wenn das Ehepaar nicht umgezogen wäre. Die am 1. Juli 1991 in Kraft getretene TELEKOM-Datenschutzverordnung (TDSV)[64] enthält detaillierte und abschließende Regelungen über die Nutzung von Kundendaten. Insbesondere darf die TELEKOM Auskünfte über die Kunden, die über die Rufnummer hinausgehen, nur mit dem schriftlichen Einverständnis der Kunden erteilen (§ 11 Abs. 3 TDSV). Das Bundesgesetz zur Bekämpfung der Geschlechtskrankheiten bestimmt zwar, daß die Gesundheitsämter geeignete Maßnahmen treffen, um geschlechtskranke Personen und solche, bei denen die begründete Befürchtung besteht, daß sie angesteckt werden und Geschlechtskrankheiten weiterverbreiten, festzustellen. Darin liegt jedoch keine Befugnis für die Gesundheitsämter, Daten über die Inhaber von Telefonanschlüssen bei der TELEKOM zu erheben, und ebensowenig eine Befugnis für die TELEKOM, entsprechende Daten zu übermitteln. Diese Auffassung wird vom Bundesbeauftragten für den Datenschutz und vom Bundesminister für Gesundheit geteilt. Der Bundesbeauftragte für den Datenschutz hat in diesem Fall zu Recht darauf hingewiesen, daß die TDSV auch keinen Raum für das sonst übliche *Adreßmittlungsverfahren* läßt, bei dem der Absender (das Gesundheitsamt) der datenverarbeitenden Stelle seinen Brief kuvertiert und frankiert zur Verfügung stellt und die datenverarbeitende Stelle (die TELEKOM) lediglich die Adresse ergänzt und den Brief versendet. Auch hierin wäre eine unzulässige Nutzung von Kundendaten abweichend von der abschließenden Regelung in der TDSV zu sehen. Es gibt andere, datenschutzgerechte Wege für die Beratungsstellen für Geschlechtskrankheiten, um ihre Angebote publik zu machen.

Computerunterstützte AIDS-Behandlung

Ein im Rahmen des Sofortprogrammes der Bundesregierung zur AIDS-Bekämpfung geplantes, rechnergestütztes Informationssystem „Klinisch-medizinische Analysen - Computer System (KLIMACS), betreut durch das Kuratorium AIDS der Paul-Ehrlich-Gesellschaft, ist bisher nicht realisiert worden. Daher ist im Land Berlin das Auguste-Viktoria-Krankenhaus (AVK) dazu übergegangen, im Rahmen eines Pilotprojektes eine eigenständige Lösung zu entwickeln.

Abweichend von der ursprünglichen Planung, nur isolierte Personalcomputer für ein solch sensibles Verfahren einzusetzen, plant das AVK den Einsatz eines *PC-Netzes*. Die zunächst bestehenden Sicherheitsbedenken gegen den Betrieb einer solch sensiblen Datenhaltung in einem Netzwerk konnte das AVK durch eine überzeugende Sicherheitskonzeption ausräumen.

Diese Sicherheitskonzeption sieht vor, Endgeräte ohne Diskettenlaufwerke einzusetzen, die nur über eine Einrichtung zum Starten des PC verfügen. Die normalerweise unverschlüsselte Datenübertragung innerhalb des Netzes wird durch eine spezielle Sicherheitssoftware eines Herstellers, der dieses Verfahren mit dem AVK gemeinsam entwickelt, ersetzt, die eine *Verschlüsselung der Daten* sowohl bei der Übertragung als auch bei der Speicherung gewährleistet.

Die Daten dieses Verfahrens werden mit codierten Querverweisen in mehreren Datenbanken gehalten. Dies bedeutet, daß selbst für den Fall der Entschlüsselung einer Datenbank kein Personenbezug herstellbar ist. Die Planung sieht vor, den Zugriff auf die Endgeräte des Netzes über die üblicherweise praktizierten Zugriffssicherungen (Login-Name und Paßwort) hinaus durch Chipkarten zu sichern, die zur Legitimation eines Nutzers in spezielle, an der Tastatur angebrachte Sensoren gesteckt werden müssen.

4.2 Inneres

4.2.1 Allheilmittel Lauschangriff?

Die sicherheitspolitische Diskussion des vergangenen Jahres ist von einem Thema beherrscht worden, das, wie kaum ein anderes, die Intimsphäre berührt: der Frage, inwieweit unsere Rechtsordnung den „Großen Lauschangriff" als Ermittlungsinstrument für Sicherheitsbehörden zulassen soll. Dieser Begriff, von den Sicherheitsbehörden eingeführt, wenn auch inzwischen von ihnen selbst geschmäht, meint *das heimliche Abhören und Herstellen von Bild- und Tonaufzeichnungen* in und aus Wohnungen mit Hilfe versteckter Mikrofone und Kameras. Sie müssen zuvor in der Wohnung plaziert werden - im Gegensatz zum „Kleinen Lauschangriff", bei dem eine gefährdete Person den Sender selbst mit sich führt, um Hilfe in Notsituationen zu ermöglichen.

In Gefahr gerät damit der vom Bundesverfassungsgericht betonte Grundsatz, daß dem Einzelnen ein unantastbarer Bereich privater Lebensgestaltung bleiben muß, der der Einwirkung der öffentlichen Gewalt entzogen ist. Jedem - auch dem einer Straftat Verdächtigen - muß ein „Innenraum" verbleiben, in dem er „sich selbst besitzt" und „in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt"[65]. Sollen gleichwohl Eingriffe zugelassen werden, müssen die geschützten Rechtsgüter diesem Grundrecht zumindest gleichgeordnet sein.

Anzuerkennen ist nur, daß zum Schutz von Leben und Gesundheit zur Abwehr konkreter Gefahren in diese Sphäre eingegriffen werden darf. Allenfalls das Polizeirecht ist damit die Materie, in der Raum für den „Großen Lauschangriff" ist. Das neue Berliner Allgemeine Sicherheits- und Ordnungsgesetz (ASOG) vom 14. April 1992[66] läßt ihn zu, wenn die Maßnahme zur Abwehr einer gegenwärtigen Gefahr für Leib und Leben oder Freiheit einer Person unerläßlich ist.

Zum erstenmal findet sich allerdings eine Regelung andernorts:

Im *Bundesverfassungsschutzgesetz* vom 20. Dezember 1990[67] hat das Bundesamt für Verfassungsschutz die Befugnis erhalten, Gespräche in Wohnungen heimlich mitzuhören oder aufzuzeichnen und heimliche Bildaufnahmen und -aufzeichnungen vorzunehmen, wenn es im Einzelfall zur Abwehr einer gemeinen Gefahr oder einer gegenwärtigen Lebensgefahr für einzelne Personen unerläßlich ist und geeignete polizeiliche Hilfe für das bedrohte Rechtsgut nicht rechtzeitig erlangt werden kann. Welche Fälle damit gemeint sind, ist unklar. Wie soll eine „Wanze" schneller unbemerkt in einer Wohnung angebracht werden, als z. B. die Polizei eingreifen kann? Sollte davon nur der Schutz von verdeckt eingesetzten Vertrauenspersonen gemeint sein, also der „Kleine Lauschangriff"?

In dem vor kurzem in Berlin in Kraft getretenen *Gesetz über das Landesamt für Verfassungsschutz*[68] vom 26. Januar 1993 ist ebenfalls das heimliche Abhören und Bildaufzeichnen in Wohnungen vorgesehen, wenn auch in begrenzterem Umfang als im Bundesverfassungsschutzgesetz. Auch hier ist nicht ersichtlich, warum das Abhören in Wohnungen zur Gefahrenabwehr nicht der Polizei überlassen bleibt. Aber immerhin: Im Gegensatz zum Bundesgesetz bleibt die Maßnahme bei nichtgewaltbereiten Bestrebungen ausgeschlossen.

Im Mittelpunkt der Diskussion steht nunmehr, ob der „Große Lauschangriff" auch dann eingesetzt werden können soll, wenn eine konkrete Gefahrenlage nicht besteht, wenn es vielmehr darum geht, Straftaten aufzuklären oder gar - Hauptproblem bei der

64 vgl. dazu Jahresbericht 1991, 2.3

65 BVerfGE 27, 1 ff, 6
66 GVBl. S. 119; Jahresbericht 1991, 3.4.1, vgl. 4.2.2
67 BGBl. I S. 2954
68 GVBl. S. 33; vgl. 4.2.3

Bekämpfung der *organisierten Kriminalität* - Straftaten erst einmal auf die Spur zu kommen: Diese Deliktsformen zeichnen sich dadurch aus, daß sie „opferlos" oder, wie es die Kriminologie makabrerweise bezeichnet, „opferverdünnt" sind: Mangels individuell zurechenbaren Schadens oder aus Furcht der Beteiligten werden die Straftaten gar nicht erst angezeigt. Kommunikationstechnik soll an die Stelle treten.

Die Strafverfolgungsbehörden, die sich nur zu gern des Erstarkens mafioser Verbrechensformen als Argument bedienen, rufen nach dem „Großen Lauschangriff" zu einer Zeit, da sie mit dem Inkrafttreten des Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG) vom 15. Juli 1992[69] gerade erst sehr weitreichende Ermittlungsbefugnisse, wie verdeckte Ermittler, Rasterfahndung, den heimlichen Einsatz technischer Mittel zum Abhören des nicht öffentlich gesprochenen Wortes außerhalb von Wohnungen in die Hand bekommen haben. Da im politischen Raum keine Einigung zu erzielen war, wurde der „Große Lauschangriff" aus dem Maßnahmenpaket herausgenommen. Dieses Moratorium könnte dazu genutzt werden, erst einmal diese gar nicht so milden Mittel auf ihre Effektivität hin zu prüfen. Hiervon war wenig zu lesen. Stattdessen desavouieren höchste Beamte das ja schließlich auf ihren eigenen Wunsch in die StPO aufgenommene Instrumentarium mit der Klage, man habe der Polizei „Steine statt Brot" gegeben.

So gefährlich die organisierte Kriminalität für Demokratie und Rechtsstaat ist; der Zweck der Strafverfolgung allein rechtfertigt nicht jedes Mittel: Sehr deutlich hat 1983 auch der Bundesgerichtshof als höchstes Strafgericht festgestellt, daß die Aufzeichnung eines Gesprächs von Eheleuten in der ehelichen Wohnung den unantastbaren Bereich der privaten Lebensgestaltung berührt, der unter den absoluten Schutz des Grundrechts aus Artikel 2 Abs. 1 i. V. m. Abs. 1 GG steht und auf den die öffentliche Gewalt selbst bei überwiegendem Allgemeininteresse nicht einwirken darf[70]. Der Rechtsstaat setzt den Ermittlungsmethoden der Polizei und der Staatsanwaltschaft Grenzen. Die oft geforderte „Waffengleichheit" zwischen Verbrechern und Polizei kann und darf deshalb in einem Rechtsstaat nicht hergestellt werden. Wenn die Bürger nicht mehr sicher sein können, ob sie in ihrer Wohnung heimlich abgehört oder gefilmt werden, verliert der Rechtsstaat sein Gesicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat diese Grundsätze in einer Entschließung betont und damit allen Versuchen eine Absage erteilt, den *Intimbereich der Wohnung* den Strafverfolgungsinteressen preiszugeben. Wahrheitserforschung um jeden Preis dürfe es in der Strafprozeßordnung nicht geben[71].

Dies schließt aber nicht aus, daß überprüft wird, wie weit dieser Schutz reichen muß. Gemäßigte Befürworter des Lauschangriffs weisen darauf hin, daß die Rechtsprechung den grundgesetzlich geschützten Bereich der Wohnung (im jeweiligen Zusammenhang mit guten Gründen) auf Räume ausgedehnt hat, die nicht unbedingt als private Zufluchtsräume gelten können, sondern vielmehr beruflichen und geschäftlichen Tätigkeiten dienen. Die Datenschutzbeauftragten haben betont, daß sie hier einer differenzierenden Sichtweise Verständnis entgegenbringen würden.

4.2.2 Polizei

Rechtsgrundlage für die Informationsverarbeitung

Mit der *Neufassung des Allgemeinen Gesetzes zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin (ASOG),* das am 26. April 1992 in Kraft getreten ist[72], sind auch in Berlin endlich Rechtsgrundlagen für die Informationsverarbeitung der Sicherheits- und Ordnungsbehörden geschaffen worden. Allerdings wäre wünschenswert gewesen, wenn den zum Teil schwerwiegenden Eingriffen in das Recht auf informationelle Selbstbestimmung engere Grenzen gesetzt worden wären.

Von unseren Empfehlungen hierzu[73] wurde nur ein kleiner Teil berücksichtigt. So werden die Voraussetzungen für die *erkennungsdienstliche Behandlung* zur vorbeugenden Straftatenbekämpfung konkreter als ursprünglich vorgesehen aufgeführt, wenn auch nicht in dem Umfang wie von uns angeregt. Weiterhin wird die Erhebung personenbezogener Daten zur vorbeugenden Straftatenbekämpfung auf Straftaten von erheblicher Bedeutung beschränkt.

Der Grundsatz wird nunmehr hervorgehoben, daß die Verarbeitung personenbezogener Daten zur *vorbeugenden Straftatenbekämpfung* nur Personen betreffen darf, bei denen Tatsachen die Annahme rechtfertigen, daß sie Straftaten begehen werden. Durch besondere Regelungen, die die Verarbeitung von Daten unverdächtiger Personen zulassen, wird diese Aussage jedoch teilweise wieder aufgehoben.

Bei *Befragungen* ist der Betroffene nicht - wie im Gesetzentwurf ursprünglich vorgesehen - nur auf sein Verlangen, sondern grundsätzlich auf die Rechtsgrundlage und eine bestehende Auskunftspflicht oder die Freiwilligkeit seiner Auskunft hinzuweisen. Ausnahmen sind nur zulässig, wenn hierdurch die Erfüllung der ordnungsbehördlichen oder polizeilichen Aufgabe erheblich erschwert oder gefährdet würde.

Darüber hinaus wird nunmehr klargestellt, daß bei *erkennungsdienstlichen Maßnahmen* Eingriffe in die körperliche Unversehrtheit unzulässig sind. Damit ist z. B. der genetische Fingerabdruck als erkennungsdienstliche Maßnahme ausgeschlossen.

Bild- und Tonaufzeichnungen bei öffentlichen Veranstaltungen und Ansammlungen sollen nicht, wie ursprünglich vorgesehen, bereits zulässig sein, wenn Tatsachen die Annahme rechtfertigen, daß dabei Ordnungswidrigkeiten begangen werden, sondern nur bei Straftaten. Die Aufbewahrungsfrist für diese Bild- und Tonaufzeichnungen wurde auf zwei Monate herabgesetzt und es wird ausdrücklich klargestellt, daß verdeckte Bild- und Tonaufzeichnungen bei öffentlichen Veranstaltungen und Ansammlungen unzulässig sind.

Die Voraussetzungen für die Ausschreibung zur sogenannten *polizeilichen Beobachtung* wurden verschärft. Diese Maßnahme darf nur eingesetzt werden bei gefährlichen Intensivtätern, bei denen weitere Straftaten zu erwarten sind.

Ferner ist die nach dem Berliner Datenschutzgesetz vorgesehene *Anhörung der Betroffenen* vor der Löschung ihrer Daten nicht völlig entfallen. Wenn die Datenspeicherung von Anfang an unzulässig war, ist weiterhin die Anhörung des Betroffenen vorgeschrieben.

Über die *Auslegung des Gesetzes* gab es erste Meinungsverschiedenheiten. Die wichtigste betrifft den Umfang der Speicherung und Nutzung der *Daten tatverdächtiger Personen.*

Nach § 42 Abs. 1 Satz 1 ASOG kann die Polizei die zur Strafverfolgung erhobenen Daten nur speichern, soweit dies hierfür erforderlich ist. Nach Abschluß des jeweiligen Ermittlungsverfahrens sind die Daten damit grundsätzlich zu löschen. Eine zweckentfremdende Speicherung dieser Daten für die Gefahrenabwehr einschließlich der vorbeugenden Straftatenbekämpfung ist gemäß § 42 Abs. 3 ASOG nur zulässig, soweit dies *hierfür* erforderlich ist.

Voraussetzung für die weitere Registrierung Straftatverdächtiger ist somit, daß in jedem Einzelfall konkrete Tatsachen vorliegen müssen, die die Annahme rechtfertigen, daß die Speicherung der Daten der betroffenen Person zur vorbeugenden Bekämpfung von Straftaten erforderlich ist: Unter Berücksichtigung aller Umstände des Einzelfalles (insbesondere Art, Schwere und Begehungsweise der Tat, Persönlichkeit des Betroffenen, Zeitraum, währenddessen er nicht [mehr] strafrechtlich in Erscheinung getreten ist) müssen Anhaltspunkte die Annahme rechtfertigen, daß die betroffene Person künftig weitere derartige Straftaten begehen wird und daß die Datenspeicherung für die dann zu führenden Ermittlungen erforderlich ist.

---

[69] BGBl. I S. 1302; Jahresbericht 1991, 3.6
[70] BGH vom 16. März 1983 - 2 StR 775/82
[71] Siehe Anlage 2.7. Die Entschließung wurde - zum wiederholten Male im Bereich der Sicherheit - gegen die Stimme des Bayerischen Landesbeauftragten gefaßt, der hier grundsätzlich für einen Nachrang der informationellen Selbstbestimmung plädiert.
[72] GVBl. S. 119
[73] Jahresbericht 1991, 3.4.1

Der Polizeipräsident lehnt dies als zu weitgehend ab. Welche Voraussetzungen er statt dessen berücksichtigen will, ist nicht ersichtlich. Die Tatsache, daß es sich um einen Tatverdächtigen handelt, wird vielmehr offenbar allein schon als ausreichend angesehen, alle im Zusammenhang mit dem Ermittlungsverfahren angefallenen Informationen zu sammeln. Lediglich die Tatsache eines Straftatverdachts ist für eine Speicherung zur vorbeugenden Straftatenbekämpfung nicht ausreichend. Hinzukommen müssen weitere konkrete Umstände, die die Erforderlichkeit und insbesondere Geeignetheit der Speicherung dieser Daten zur Bekämpfung künftig zu erwartender Straftaten belegen. Diese Voraussetzungen wurden vom Bundesverwaltungsgericht für die Aufbewahrung von erkennungsdienstlichen Unterlagen entwikkelt und können auf andere Datenspeicherungen zur vorbeugenden Straftatenbekämpfung übertragen werden[74]. Die besondere Eingriffstiefe der erkennungsdienstlichen Behandlung macht lediglich besonders hohe Anforderungen an den Verhältnismäßigkeitsgrundsatz erforderlich, was z. B. darin seinen Ausdruck findet, daß wegen Bagatelldelikten erkennungsdienstliche Unterlagen nicht zur vorbeugenden Straftatenbekämpfung aufbewahrt werden dürfen[75]. Bei Datenspeicherungen führt dies lediglich zu kürzeren Speicherfristen.

Im ASOG sind nunmehr ausdrücklich die Polizeibefugnisse auf sogenannte *„andere Personen"* ausgedehnt worden. Damit wird das hergebrachte Prinzip aufgegeben, polizeiliche Eingriffe außer in den Fällen des Notstandes nur gegen „Störer" zuzulassen. Hinter diesem Prinzip steht der rechtsstaatliche Grundsatz, daß derjenige, der sich gesetzestreu verhält, das Recht hat, vom Staat in Ruhe gelassen zu werden[76].

In § 43 Abs. 1 ASOG wird zur vorbeugenden Straftatenbekämpfung die bis zu dreijährige Speicherung der Daten von Personen ermöglicht, die sich keiner Straftat verdächtig gemacht haben und nicht als „Störer" in Erscheinung getreten sind.

Hier haben wir mit der Senatsverwaltung für Inneres Einigkeit erzielen können, daß die Speicherung der Daten dieses Personenkreises an besondes strenge Voraussetzungen zu knüpfen ist. So kann die umstrittene Speicherung der Daten von *Prostituierten*[77] künftig nicht mehr mit der Begründung erfolgen, daß ihre Tätigkeit in einem Umfeld erfolgt, das nach polizeilicher Erfahrung erheblichen kriminellen Einflüssen ausgesetzt ist, sondern es müssen darüber hinaus in jedem Einzelfall konkrete Tatsachen vorliegen, die geeignet sind, das Grundrecht auf informationelle Selbstbestimmung hinter das öffentliche Interesse gerade im Umkreis der Betroffenen zurücktreten zu lassen. Die im ASOG für „andere Personen" vorgesehene Speicherfrist hat darüber hinaus dazu geführt, daß die bisher für fünf Jahre vorgesehene Registrierung der Prostituierten in der Kartei „Zuhälterei, Menschenhandel und ähnliche Delikte" erheblich verkürzt wurde und Datenlöschungen vorgenommen wurden[78].

Ein weiterer Problempunkt schafft der Zusammenhang zwischen *Ordnungsverwaltung und Polizeivollzugsdienst.* Wir haben in den Anhörungen darauf hingewiesen, daß nicht nur die Polizei, sondern auch weitere über 150 datenverarbeitende Stellen bei den Ordnungsbehörden des Landes Berlin mit dem ASOG arbeiten werden, was bei den Gesetzesberatungen allerdings kaum Beachtung gefunden hat. Zunehmend „entdecken" Ordnungsbehörden das ASOG, das ihnen weitergehendere Kompetenzen zubilligt als sie zuvor hatten, da dieses auf die Arbeit der Vollzugspolizei zugeschnitten ist[79]. Hier zeigt sich, wie sachdienlich eine stärkere Differenzierung der Befugnisse für Vollzugspolizei und Ordnungsbehörden gewesen wäre.

Funkbetriebszentrale der Polizei

Eine Prüfung der Funkbetriebszentrale beim Polizeipräsidenten ergab, daß alle dort geführten Telefongespräche aufgezeichnet werden. Dies galt für den Zeitpunkt der Prüfung nicht nur für die Anrufe der Bürger, sondern auch für die Gespräche, die die dort eingesetzten Beamten im Zusammenhang mit der Bearbeitung der Notrufe (insbesondere die Unterrichtung anderer Dienststellen, Gespräche mit einzuschaltenden Dienststellen) führen. Gespräche mit der BVG, Feuerwehr und den Taxifunkzentralen wurden über Direktleitungen geführt und ebenfalls aufgezeichnet.

Die *Tonbänder* werden zu Zwecken der Gefahrenabwehr, der Strafverfolgung, des Schutzes der Beamten vor ungerechtfertigten Beschuldigungen und zur Sicherung von Tatsachen, die im Zusammenhang mit dem Verdacht einer Dienst- bzw. Arbeitspflichtverletzung stehen, genutzt.

Zusätzlich zur *Aufzeichnung der Telefongespräche* erfolgt die schriftliche Aufnahme aller Meldungen. Die Formulare mit den Einsatzaufträgen werden 2 Jahre archiviert.

Neben der zentralen Aufzeichnungsanlage befinden sich an jedem Arbeitsplatz platzbezogene Aufzeichnungsgeräte. Diese können vom diensttuenden Beamten nach Bedarf zurückgespult und abgehört werden, um z. B. undeutliche Anrufe zu verstehen. Die platzbezogenen Aufzeichnungsgeräte verwenden Endlos-Bänder, die spätestens nach einem Tag überspielt sind.

Mängel hinsichtlich der Datensicherheit waren nicht feststellbar.

Die Aufzeichnung der auf den Notrufleitungen eingehenden Anrufe ist auch zulässig, da diese Maßnahme zu Zwecken der Gefahrenabwehr gemäß § 18 Abs. 1 Satz 2 ASOG erforderlich ist. Die Tatsache, daß die Anrufe ohne Wissen der Anrufenden aufgezeichnet werden und somit eine verdeckte Ermittlung darstellen, ändert an dieser Bewertung nichts. Die verdeckte Erhebung kann hier ausnahmsweise als zulässig angesehen werden, da sie dem überwiegenden Interesse der betroffenen Personen entspricht (§ 18 Abs. 2 Satz 2 ASOG).

- Bei Anrufen, die im Zusammenhang mit einer unmittelbar drohenden Gefahr eingehen, ist eine schriftliche Dokumentation vielfach nicht möglich. Undeutliche oder unklare Gesprächsbestandteile müssen durch Wiedergabe der Aufzeichnung analysiert werden können. Bei einem unerwarteten Abbruch des Gesprächs muß ein verwertbarer Inhalt gesichert werden können, um die erforderlichen Gefahrenabwehrmaßnahmen einzuleiten.

Auch soweit die Anrufe der Anzeige und Verfolgung einer Straftat dienen, ist ihre Aufzeichnung erforderlich, da in diesem Zusammenhang möglichst unmittelbar Spuren und Beweismittel zu sichern sind (§ 163 StPO).

Datenschutzrechtlich bedenklich ist dagegen, daß jeder Anruf erfaßt wird und daß einzelne Anrufe, die weder mit einem Notfall noch mit einer Straftat in Verbindung stehen, nicht unterdrückt werden können. Wir haben deshalb empfohlen, die Beamten anzuweisen, in diesen Fällen das Gespräch unter Hinweis auf die Tonbandaufzeichnung abzubrechen und den Anrufer auf einen normalen Telefonanschluß der Polizei zu verweisen.

Die lückenlose Aufzeichnung von Gesprächen, die zwar im Zusammenhang mit einem *Notruf* stehen (z. B. mit anderen Dienststellen), aber nicht auf den Notrufleitungen geführt werden, ist für die Gefahrenabwehr oder zur Strafverfolgung nicht erforderlich und daher unzulässig. Die Polizei hat mitgeteilt, daß in Zukunft derartige Aufzeichnungen unterbleiben.

Die weitere Aufbewahrung der Bänder mit den Telefongesprächen zu Zwecken der Gefahrenabwehr und der Strafverfolgung ist gemäß § 42 Abs. 1 Satz 1 ASOG zulässig, wenn die Aufzeichnungen zu diesen Zwecken gemacht worden sind. Die Speicherung im Rahmen der Gefahrenabwehr ist jedoch nur erforderlich, um den Notfalleinsatz abzuwickeln, d. h. bis zum Abschluß des Einsatzes. Dafür sind die Aufzeichnungsmöglichkeiten auf den Einzelplatz-Bändern ausreichend. Gegen eine sechswöchige Aufbewahrung der aufgezeichneten Telefongespräche für Beweiszwecke im Rahmen der Strafverfolgung bestehen dagegen keine Bedenken (§§ 42 Abs. 2 Satz 2, 18 Abs. 2 Satz 2 ASOG).

Gemäß § 42 Abs. 1 Satz 1 ASOG kann die Polizei die aufgezeichneten Daten auch speichern und nutzen, soweit dies zu einer zeitlich befristeten *Dokumentation* erforderlich ist. Die Dokumentationszwecke sind in dieser Bestimmung nicht konkret

[74] BVerwG vom 19. 10. 82 NJW 83, S. 772 und 1338; vom 6. 7. 1988 NJW 89, S. 2640
[75] Jahresbericht 1990, 3.5
[76] BVerfGE 27, 1, 6
[77] Jahresbericht 1990, 3.5, S. 60
[78] siehe unten
[79] siehe 4.2.4

benannt. Als Teil der Vorgangsbearbeitung dient die Dokumentation ausschließlich einem Zweck, der unmittelbar mit dem polizeilichen oder ordnungsbehördlichen Handeln verbunden ist.

Personenbezogene Daten, die nicht mehr für den „Ursprungszweck" der Speicherung – wie Gefahrenabwehr, vorbeugende Straftatenbekämpfung oder Straftatenverfolgung – erforderlich sind, dürfen nur dann zu Dokumentationszwecken (weiter) gespeichert werden, soweit diese Speicherung für einen konkret zu benennenden Zweck, der in einem sachlich engen Zusammenhang zu dem ursprünglichen Speicherungszweck steht, erforderlich ist (z. B. zur Durchsetzung von Amtshaftungsansprüchen oder zur Durchführung von Disziplinarverfahren wegen eines Fehlverhaltens bei der Bearbeitung der Anrufe).

Diese unmittelbare Akzessorietät des Dokumentationszwecks zu dem vorangegangenen Anruf ergibt sich aus dem berechtigten Interesse des Anrufers, das auf Grund der verdeckten Datenerhebung gemäß § 18 Abs. 2 Satz 2 ASOG auf jeden Fall gegeben sein muß.

Eine Speicherung der Telefonanrufe zu weitergehenden Zwecken – z. B. zur allgemeinen Leistungskontrolle oder für Disziplinarverfahren, die nicht unmittelbar im Zusammenhang mit dem konkreten Anruf stehen – ist unzulässig. Derartige Dokumentationszwecke stehen nicht in Zusammenhang zu dem polizeilichen oder ordnungsbehördlichen Handeln und können nicht auf die Speicherungsbefugnis des § 42 Abs. 1 ASOG gestützt werden.

Die für die Speicherung der genannten zulässigen Dokumentationszwecke vorgesehene Aufbewahrungsfrist von sechs Wochen halten wir für angemessen. Innerhalb dieser Frist wird regelmäßig geklärt sein, ob auf Grund von Beschwerden des Anrufers dienstliche Maßnahmen zu ergreifen sind oder Schadensersatzansprüche von Bürgern gestellt werden.

Zugriff der Polizei auf Ausweisdaten

Die nach dem Meldegesetz von 1985 erforderliche Übertragung der Ordnungsaufgaben vom Polizeipräsidenten auf das damals neu geschaffene Landeseinwohneramt machte eine Regelung erforderlich für die Ausweisangelegenheiten (insbesondere die Verlängerungen), die außerhalb der Dienstzeiten des Landeseinwohneramtes zu erledigen waren. Dem Polizeipräsidenten wurde damals eine ausdrückliche Zuständigkeit in Ausweisangelegenheiten zugewiesen, mit der Folge, daß den Polizeibediensteten auch ein Zugriff auf die Meldedaten gewährt werden mußte[80]. Durch einen Dauerdienst im Landeseinwohneramt sollte sichergestellt werden, daß die Daten an die Polizei nur in erforderlichem Umfang herausgegeben werden[81].

In Folge der deutschen Vereinigung ist die Zuständigkeit des Polizeipräsidenten in Ausweisangelegenheiten zwar gegenstandslos geworden. Für besonders gelagerte Fälle hält jedoch die Senatsverwaltung für Inneres einen sofortigen Zugriff auf diese Lichtbilder außerhalb der üblichen Dienstzeiten für unerläßlich, um Straftaten aufzuklären. Es wurde vorgeschlagen, daß bei den Polizeiabschnitten Schlüssel für die Meldestellen in versiegelten Umschlägen hinterlegt werden, mit denen nach telefonischer Absprache mit Meldestellenleitern oder Mitarbeitern des Landeseinwohneramtes Ausweisunterlagen entnommen werden können. Die Meldestellen sollten ein Protokoll über die Entnahme mit einer substantiierten Begründung der Erforderlichkeit erhalten.

Zwar ist anzuerkennen, daß im Einzelfall die Erforderlichkeit bestehen kann, daß die Polizei außerhalb der Dienstzeiten der Meldestellen Unterlagen aus Ausweisanträgen zur Strafverfolgung erhält. Wir haben jedoch Zweifel, ob das vorgeschlagene Verfahren die Sicherung des Rechts auf informationelle Selbstbestimmung bei Datenübermittlungen hinreichend berücksichtigt.

Das vorgeschlagene Verfahren hätte letztlich einen Zugriff auf sämtliche Datenbestände der Meldestellen, vergleichbar einem Online-Zugriff, ermöglicht. Die Polizei würde damit die Möglichkeit erhalten, selbst auf die Ausweisdaten des Landeseinwohneramtes zuzugreifen. Die Prüfungsmöglichkeiten des LEA würden sich auf die telefonische Unterrichtung durch die Polizei beschränken. Eine Protokollierung der Datenübermittlungsersuchen an die Ausweisbehörde ist nach dem Landespersonalausweisgesetz ohnehin erforderlich. Eine zusätzliche Verfahrensabsicherung ist dies somit nicht. Im übrigen widerspricht die vorgeschlagene Überlassung des Protokolls dem Landespersonalausweisgesetz, wonach diese Aufzeichnungen bei der ersuchenden Strafverfolgungsbehörde zu speichern sind. Der Gesetzgeber wollte hierdurch eine Registrierung von Straftatverdächtigen bei den Ausweisbehörden verhindern.

Dem Recht auf informationelle Selbstbestimmung trägt nur die Herausgabe der Ausweisfotos durch die Meldestellen oder den *Dauerdienst des Landeseinwohneramtes* Rechnung. Dem ist die Senatsverwaltung für Inneres gefolgt. Die Polizei erhält nunmehr außerhalb der allgemeinen Dienstzeiten des Landeseinwohneramtes bei Vorliegen der gesetzlichen Übermittlungsvoraussetzungen ausschließlich durch Mitarbeiter des Dauerdienstes des Landeseinwohneramtes Unterlagen aus Paß- oder Ausweisanträgen.

Übermittlung polizeilicher Kfz-Sachfahndungsdaten an Kfz-Hersteller und den HUK-Verband

Ende 1991 bat der Verband der Haftpflichtversicherer, Unfallversicherer, Autoversicherer und Rechtsschutzversicherer e. V. (HUK-Verband) das Bundeskriminalamt um Mithilfe im Zusammenhang mit der Rückführung von als gestohlen gemeldeten Kraftfahrzeugen aus Polen.

Um eine schnelle Identifikation der betreffenden Fahrzeuge vor Ort zu ermöglichen, beantragte der HUK-Verband beim BKA die Überlassung von Fahndungsdaten (Fahrzeugidentifizierungsnummer, letztes amtliches Kennzeichen, Tatort und -zeit) aus der Kfz-Sachfahndungsdatei des INPOL-Systems durch Überspielung der Daten per Diskette.

Weiterhin beschloß das BKA, die Kfz-Fahndungsdaten an verschiedene Kfz-Hersteller zu übermitteln, damit diese in die Fahndung eingebunden werden können.

Bei den personenbezogenen Daten aus der *Fahndungsdatei* handelt es sich um Daten der Länder, da die Daten aus dem Verantwortungsbereich der Landespolizeien stammen und von diesen in das INPOL-System eingegeben werden. Demzufolge waren für die Beurteilung der Zulässigkeit der Übermittlung des Berliner Datenbestandes die Bestimmungen des Berliner Datenschutzgesetzes maßgeblich.

Nach § 13 BlnDSG ist die Übermittlung an private Stellen nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Diese Voraussetzungen liegen nicht vor. Weder haben die Betroffenen eingewilligt noch sieht die Strafprozeßordnung Übermittlungsbefugnisse vor. Die Übergangsregelung des § 34 Abs. 1 BlnDSG konnte nicht über die bisherige Rechtslage hinausgehen und fand deshalb bei der Übermittlung an Private keine Anwendung.

Wir haben die Senatsverwaltung für Inneres aufgefordert, gegenüber dem BKA klarzustellen, daß sie der Datenübermittlung nicht zustimmt. Dem wurde nicht gefolgt. Nur die Daten der Länder Bremen, Nordrhein-Westfalen, Schleswig-Holstein und Saarland werden ab Februar 1992 nicht mehr an den HUK-Verband und die Kfz-Hersteller übermittelt.

Die Senatsverwaltung hat vielmehr mitgeteilt, daß die Führung der *Länder-Verbund-Dateien* innerhalb des INPOL-Systems dem BKA im Rahmen seiner Zentralstellenfunktion nach dem BKA-Gesetz obliege und daher eine Anwendung des Berliner Datenschutzgesetzes nicht in Betracht komme. Im übrigen sei hier ohnehin ausschließlich die Strafprozeßordnung anwendbar. Die Senatsverwaltung verzichtet damit auf die Verantwortung und auch die Möglichkeiten des Landes Berlin, über die Verwendung „seines" Datenbestandes zu bestimmen. Sie ist auch der Sache nach nicht zutreffend. Zweck der Einrichtung einer *Zentralstelle beim BKA* ist es, die Strafverfolgungs- und Polizeibehörden bei ihrer Aufgabenerfüllung zu unterstützen. Die Verfolgung und die vorbeugende Bekämpfung von Straftaten sind grundsätzlich

[80] Jahresbericht 1986, 2.1
[81] Jahresbericht 1987, 6

Sache der Länder. Wenn der Polizeipräsident Daten, die er erhoben hat, zur Erfüllung seiner Aufgaben im *INPOL-System* speichert, muß er auch die Verantwortung für die Zulässigkeit, Richtigkeit und Dauer der Speicherung sowie die weiteren Verarbeitungen – insbesondere Datenübermittlungen – behalten. Da die Strafprozeßordnung (noch) keine Übermittlungsbefugnisse enthält[82], sind die Regelungen des Berliner Datenschutzgesetzes anwendbar.

Ungeachtet dessen bestehen insbesondere hinsichtlich der Datenübermittlung an den HUK-Verband noch Unklarheiten und Widersprüche bei den Datensicherungsmaßnahmen und der Datenverarbeitung des HUK-Verbandes in Polen. Nicht zuletzt wegen dieser ungeklärten Fragen im Verfahren ist das Vorgehen von BKA und HUK-Verband datenschutzrechtlich bedenklich.

Hinzu kommt, daß fraglich ist, ob die Einschaltung privater Stellen für einen Datenaustausch mit Polen noch erforderlich ist, nachdem das Abkommen zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Republik Polen über die Zusammenarbeit der Bekämpfung der organisierten Kriminalität vom 26. August 1992[83] vorliegt.

Polizeiliche Registrierung von Prostituierten

Eine Prostituierte erstattete bei der Polizei Anzeige gegen einen aggressiven Freier, der sie mit Tränengas besprühte, ihr mit einem Hammer auf den Kopf schlug und ihr anschließend das Geld abnahm. Ob der Freier gefaßt wurde, wissen wir nicht – die Frau ist seit diesem Vorfall jedenfalls bei der Polizei als Prostituierte registriert.

Eine andere Frau erstattete bei der Polizei Anzeige gegen einen Freier, der sie unter Würgen am Hals zum Geschlechtsverkehr ohne Kondom zwang und ihr das Geld stahl. Auch ihre Anzeigebereitschaft führte zur Registrierung bei der Polizei als Prostituierte.

Dies sind nur zwei Beispiele zur *Kartei „Zuhälterei, Menschenhandel und ähnliche Delikte"*. Es ist zu bezweifeln, ob eine derartige Praxis zu der von der Polizei gewünschten Aussage- und Anzeigebereitschaft von Prostituierten beiträgt.

In unserem Jahresbericht 1990[84] hatten wir erstmals über diese beim Polizeipräsidenten geführte Kartei berichtet, die überwiegend *Daten von Prostituierten* enthält. In dieser Kartei waren 1990 ca. 5000 Prostituierte registriert, zum Teil mit Fotos in leicht bekleidetem Zustand.

Die von uns geforderte Löschung der Daten sämtlicher Frauen, die lediglich der Prostitution nachgehen, aber keiner Straftat verdächtig sind, wurde von der Senatsverwaltung für Inneres mit dem Hinweis auf die „Eigenart des Kriminalitätsfeldes" abgelehnt.

Ende November 1991 waren in der Kartei 5718 Personen registriert. Davon waren 228 Beschuldigte oder Verdächtige einer Straftat und 5490 Personen, die in Ausübung der Prostitution angetroffen wurden oder als Opfer der genannten Straftaten bekannt wurden. Auch Fotos unbekannter Herkunft, die zum Teil Betroffene auf diskriminierende Weise mit Ganzkörperaufnahmen zeigten, konnten wir erneut feststellen.

Auch nach dem ASOG ist diese Verfahrensweise unzulässig. Danach dürfen Frauen nicht bei der Polizei registriert werden, nur weil sie der Prostitution nachgehen. Es müssen vielmehr 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. Allein die Prostitution bietet noch keine konkreten Anhaltspunkte dafür, daß Straftaten begangen werden, deren Bekämpfung eine jahrelange polizeiliche Registrierung der Frauen rechtfertigt. Keine ausreichende Speicherungsvoraussetzung ist auch der Hinweis, daß allgemein das Umfeld der Prostitution nach polizeilichen Erkenntnissen erheblichen kriminellen Einflüssen ausgesetzt ist. Die Speicherung zur vorbeugenden Straftatenbekämpfung setzt voraus, daß über die Ausübung der Prostitution und allgemeine kriminalistische Erfahrungen hinaus in jedem Einzelfall bei der betroffenen Frau Besonderheiten vorliegen, die geeignet sind, das Grundrecht auf informationelle Selbstbestimmung hinter das öffentliche Interesse gerade im Umkreis der Betroffenen zurücktreten zu lassen. Auch die Aufbewahrung von – zum Teil erheblich in die Intimsphäre eindringenden – Fotos von Prostituierten ist nach dem ASOG unzulässig.

Die Senatsverwaltung für Inneres teilt nunmehr unsere Beurteilung der Rechtslage. Die Kartei wurde inzwischen nochmals bereinigt und enthielt im Juni 1992 noch 4201 Karteikarten.

Wir werden zu gegebener Zeit nachprüfen, ob die strengen Kriterien zur Speicherung unverdächtiger Personen bei der Bereinigung der Kartei beachtet wurden.

4.2.3 Verfassungsschutz

Verfassungsschutzgesetz novelliert

Seit Jahren hatten wir angemahnt, die erforderlichen gesetzlichen Grundlagen für den Umgang des Landesamtes für Verfassungsschutz mit den Daten der Bürger zu schaffen. Wir hatten darauf hingewiesen, daß wegen der schwerwiegenden Informationseingriffe, die mit der Arbeit des Amtes verbunden sind, eine intensive Beratung der zu schaffenden gesetzlichen Grundlagen erforderlich ist[85]. Erst im August 1992 wurde ein Antrag der Koalitionsfraktionen eingebracht[86]. Da die Übergangsfrist im Berliner Datenschutzgesetz abzulaufen drohte, konnte ein abgestimmter Entwurf, der auch die Anregungen des Datenschutzbeauftragten berücksichtigt, durch den Senat offenbar nicht mehr eingebracht werden.

Das novellierte *Gesetz über das Landesamt für Verfassungsschutz*, das am 1. Februar 1993 in Kraft getreten ist[87], orientiert sich weitgehend am Bundesverfassungsschutzgesetz[88]. Der Gesetzgeber hat nicht die Chance genutzt, gegenüber den bundesgesetzlichen Regelungen mögliche Stärkungen der Bürgerrechte vorzusehen. Das Gesetz läßt zwar gewisse Bemühungen in dieser Richtung erkennen. So wird der Einsatz nachrichtendienstlicher Mittel gegen Nichtstörer auf die Gewinnung von Erkenntnissen über gewalttätige Bestrebungen, geheimdienstliche Tätigkeiten und die Anwerbung von Vertrauensleuten beschränkt und eine Speicherung von Informationen über noch nicht Vierzehnjährige grundsätzlich untersagt. Das Berliner Gesetz bleibt dennoch weit hinter den Anforderungen zurück, die die Konferenz der Datenschutzbeauftragten in mehreren Beschlüssen seit Jahren an die Datenschutzregelungen für den Verfassungsschutz gestellt hat[89]. Dies ist um so bedauerlicher, als in anderen Ländern der gesetzgeberische Spielraum zugunsten der Bürgerrechte weitgehender genutzt wurde[90].

Wir haben in den parlamentarischen Beratungen umfangreiche Änderungsvorschläge gemacht, denen jedoch nur in sehr begrenztem Umfang gefolgt wurde.

Zu begrüßen ist, daß doch noch die *Akteneinsicht* für Betroffene aufgenommen wurde. Die Regelung bleibt zwar hinter dem bisher geltenden Akteneinsichtsrecht der Bürger nach dem Berliner Datenschutzgesetz zurück, sieht aber zumindest einen Anspruch auf ermessensfehlerfreie Entscheidung vor. Die Möglichkeit des sogenannten *„Lauschangriffs"*[90a] hingegen wurde in den parlamentarischen Beratungen erweitert. Das heimliche Abhören und Bildaufzeichnen in Wohnungen ist nunmehr zulässig nicht nur für Aufgaben aus den Gebieten der Spionageabwehr, sondern auch des gewaltbereiten politischen Extremismus.

82 siehe 4.3
83 BGBl. II S. 950
84 vgl. 3.5

85 Jahresbericht 1991, 3.4.2
86 Drs. 12/1824
87 GVBl. 1993 S. 33
88 BGBl. I 1990 S. 2953
89 Jahresbericht 1985 Anlage 4; Jahresbericht 1986 Anlage 1; Jahresbericht 1989 Anlage 1.5; Jahresbericht 1990 Anlage 1.6
90 Entwurf des Brandenburgischen Verfassungsschutzgesetzes, Stand Juni 1992; Niedersächsisches Verfassungsschutzgesetz vom 6. Nov. 1992 (GVBl. S. 283)
90a siehe 4.2.1

An der von uns für verfassungswidrig gehaltenen *Auskunftsregelung* wurden Änderungen zugunsten der Bürgerrechte in den Ausschußberatungen abgelehnt. Trotz unserer Bedenken wird künftig das Auskunftsrecht der Betroffenen an die Verpflichtung zur Darlegung eines besonderen Interesses geknüpft. Dieses wesentliche Recht wird damit unter einen sehr einschneidenden Vorbehalt gestellt. Wie das Bundesverfassungsgericht im Volkszählungsurteil festgestellt hat, wäre eine Rechtsordnung, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß, mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar[91]. Als verfahrensrechtliche Schutzvorkehrungen sind daher Auskunftspflichten gegenüber dem Betroffenen wesentlich[92]. Diese sind notwendig, damit der Bürger in Kenntnis des Wissens Staatlicher Kommunikationspartner aus eigener Selbstbestimmung planen, entscheiden und sich entsprechend dieser Entscheidung verhalten kann[93]. Sie sind ferner die Voraussetzung dafür, daß der Betroffene die Erhebung, Speicherung, Verwendung und Weitergabe seiner Daten durch einen effektiven Rechtsschutz (Art. 19 Abs. 4 GG) überprüfen lassen[94] und insbesondere die in den Datenschutzgesetzen vorgesehenen Rechte auf Berichtigung, Sperrung und Löschung geltend machen kann. Das Auskunftsrecht ist daher eine verfassungsrechtlich gebotene Folge des Rechts auf informationelle Selbstbestimmung. Aus diesem Recht als Bestandteil des Allgemeinen Persönlichkeitsrechts ergibt sich bereits das erforderliche Informationsinteresse. Die Darlegung weiterer besonderer Gefährdungen oder Interessen darf vom Betroffenen nicht verlangt werden.

Hervorzuheben sind noch folgende von uns vorgebrachte Kritikpunkte:

Der Gesetzgeber hat es dem Landesamt für Verfassungsschutz ermöglicht, seine Aufgaben eigenständig auszuweiten. Eine derartige Bestimmung befindet sich außer in Baden-Württemberg in keinem weiteren Verfassungsschutzgesetz der Länder oder des Bundes. Künftig dürfen durch Verwaltungsvorschriften *Überprüfungen* vorgesehen werden, bei denen das Landesamt für Verfassungsschutz mitwirkt. Welche Überprüfungen dies sein sollen und welcher Art die Überprüfungen sind, ist dem Gesetz nicht zu entnehmen. Wir halten es für verfassungswidrig, der Exekutive zu überlassen, die im Grundgesetz definierten und vom Bundesgesetzgeber inhaltlich konkretisierten Aufgaben des Verfassungsschutzes (Art. 73 Nr. 10 GG) durch Verwaltungsvorschriften auszuweiten. Es ist ohnehin fraglich, ob der Landesgesetzgeber hierzu befugt ist.

Für verfassungsrechtlich bedenklich halten wir das Fehlen einer generellen *Zweckbindung*[95] für die vom Landesamt für Verfassungsschutz zu verschiedenen Zwecken erhobenen personenbezogenen Daten. Unserem Vorschlag, im Gesetz dieses deutlich zum Ausdruck zu bringen und klarzustellen, daß sie nur in ausdrücklich gesetzlich zugelassenen Fällen durchbrochen werden darf, wurde nicht entsprochen.

Neu ist die in dem Gesetz vorgesehene Möglichkeit des Landesamtes für Verfassungsschutz, sämtliche *Register* von Berliner öffentlichen Stellen einzusehen. Der Verfassungsschutz kann damit von beliebigen Daten ohne jede Einflußmöglichkeit der speichernden Stelle Kenntnis nehmen. Die vom Bundesverfassungsgericht geforderte Unerläßlichkeit[96] für diesen Eingriff in das informationelle Selbstbestimmungsrecht wurde nicht überzeugend dargelegt. Da der Begriff „Register" nicht definiert ist, ist auch unklar, welche Datensammlungen (nur manuelle Dateien? auch alle automatisierten Dateien?) darunter fallen. Nur beispielhaft werden das Melderegister, das Personalausweisregister, das Paßregister, die Führerschein- und Waffenscheinkarteien genannt.

Zweifelhaft ist, ob es mit dem Verfassungsgrundsatz der Verhältnismäßigkeit zu vereinbaren ist, daß auch nicht gewaltbereite Organisationen und Personenzusammenschlüsse mit *nachrichtendienstlichen Mitteln* beobachtet werden sollen. Hier wird vernachlässigt, daß nicht alle als verfassungsfeindlich eingestuften Bestrebungen als gleich gefährlich zu werten sind. Daß bereits das Vorliegen tatsächlicher Anhaltspunkte für den Verdacht solcher Bestrebungen ausreichen soll, um Eingriffe in Grundrechte vorzunehmen, bedeutet eine Verlagerung staatlicher Eingriffe in das Vorfeld, die allenfalls dann hingenommen werden kann, wenn es darum geht, gemeingefährliche, das Staatswesen als solches bedrohende Gewalttaten von erheblicher Intensität zu verhindern. Eine Zulassung solcher Befugnisse auch für den Bereich nicht gewalttätiger Bestrebungen heißt auch, den Geist der Verfassung als lebendige, durchaus änderbare (Art. 79 GG) Grundlage eines demokratischen Gemeinwesens zu verkennen. Sie wie der Staat selbst ist letztlich dazu da, „die äußere Ordnung zu schaffen, derer die Menschen zu einem auf der Freiheit des Einzelnen beruhenden Zusammenlebens bedürfen" [97].

Bedenklich ist auch, daß unklar bleibt, gegen wen nachrichtendienstliche Mittel eingesetzt werden dürfen. Eine generelle Beschränkung auf „Störer" erfolgt nur beim nicht gewaltbereiten Extremismus. *Beobachtungsobjekt* kann damit z. B. bei der Anwerbung von Vertrauensleuten oder bei der Beobachtung gewalttätiger Bestrebungen jede Person werden, unabhängig davon, ob ihr Verhalten den Verdacht einer verfassungsfeindlichen Bestrebung rechtfertigt oder nicht. Es ist nicht einmal eine Beschränkung auf Kontakt- oder Begleitpersonen wie im ASOG vorgesehen.

Datenlöschungen beim Verfassungsschutz in Sicht

Im Zusammenhang mit der Arbeit des Untersuchungsausschusses des Abgeordnetenhauses in der 10. Legislaturperiode ist ein *Löschungs- und Vernichtungsverbot* für die beim Landesamt gesammelten Daten ergangen. Folge davon ist, daß sich seitdem ein riesiger Berg von unzulässig erhobenen oder nicht mehr erforderlichen Daten angesammelt hat. Bei vielen Betroffenen, deren Daten trotz unzulässiger Speicherung weiter aufbewahrt wurden, stieß dieses Verfahren auf verständlichen Unmut. Wir haben eindringlich die Aufhebung des strikten Löschungs- und Vernichtungsverbots empfohlen[98]. Der Ausschuß für Verfassungsschutz des Abgeordnetenhauses hat nunmehr die Senatsverwaltung für Inneres aufgefordert, das Verbot in bestimmtem Umfang aufzuheben:

- Die für die gesetzliche Aufgabenerfüllung des Landesamtes nicht mehr notwendigen personenbezogenen Daten sind in den automatisierten und nicht automatisierten Dateien zu löschen.
- Die für die gesetzliche Aufgabenerfüllung des Landesamtes nicht mehr notwendigen Akten und Unterlagen sind umgehend auszusondern. Die ausgesonderten Akten sind als Altakten in die Altaktenablage zu übernehmen.
- Altakten des Landesamtes sind in besonderen Räumen in der gleichen Ordnung wie der laufende Aktenbestand aufzubewahren. Es ist zu gewährleisten, daß dieser Aktenbestand für die Aufgabenerfüllung des Landesamtes nicht mehr genutzt werden kann.
- Nach Inkrafttreten eines Landesarchivgesetzes sind die Altakten umgehend dem Landesarchiv zur Übernahme anzubieten. Bis zu diesem Zeitpunkt bleibt das Vernichtungsverbot für Akten und Unterlagen bestehen.
- Soweit Betroffenen aus den Unterlagen und Akten bereits Auskunft erteilt wurde und bzw. oder sie Akteneinsicht genommen haben, können diese Akten und Unterlagen vernichtet werden.

Das Landesamt hat die erforderlichen Maßnahmen zur Durchführung des Bereinigungsprozesses eingeleitet.

91 BVerfGE 65, 1, 43
92 BVerfGE a.a.O., S. 46
93 BVerfGE a.a.O., S. 42–43
94 BVerfGE a.a.O., S. 70
95 vgl. BVerfGE 65, 1, 46
96 BVerfGE 65, 1, 44 m.w.N.

97 Carlo Schmid JöR n.F. 1 (1951), S. 47
98 Jahresbericht 1991, 3.4.2

Ungeachtet dessen wurden jetzt auch in den NADIS-Gremien die technischen Voraussetzungen für die *Sperrung* von Daten in dem bundesweiten Informationssystem NADIS vereinbart. Dieses Verfahren ist jedoch nicht datenschutzgerecht.

4.2.4 Meldewesen, Fahrerlaubnisse, Personenstandswesen

ADV-Verfahren Einwohnerwesen

Das ADV-Verfahren Einwohnerwesen (EWW) ist das automatisierte Melderegister Berlins. In dieser Datenbank sind für alle Bürger Berlins einschließlich derer, die in den letzten fünf Jahren verstorben oder verzogen sind, alle nach § 2 Meldegesetz zulässigen Daten gespeichert.

Eine technisch-organisatorische Überprüfung ließ eine Reihe von Mängeln erkennen.

Das ADV-Verfahren EWW wird im Rahmen von Auftragsverarbeitung (§ 3 BlnDSG) im Auftrag des LEA auf Rechnern des LIT durchgeführt.

Nach § 3 BlnDSG hat sich das LIT an Weisungen des LEA zu halten. Solche Weisungen existierten zum Prüfzeitpunkt jedoch nicht in schriftlicher, damit verbindlicher und nachvollziehbarer Form.

Wir haben dem LEA nachdrücklich empfohlen, dem LIT die notwendigen Weisungen zur Auftragsdatenverarbeitung in schriftlicher Form zu erteilen.

Die Anwenderprogramme werden vom LEA erstellt, gewartet und verwaltet. Wegen der engen Verzahnung der programmierenden mit der datenverarbeitenden Stelle wurde auf die *Erstellung von Programmvorgaben und Programmabnahme- bzw. -freigabeprotokolle durch die betreffenden Fachdienststellen* verzichtet.

Dadurch ist die Kontrollierbarkeit der Ordnungsmäßigkeit der Datenverarbeitung stark eingeschränkt. Beim Auftreten von Programmängeln lassen sich weder die Verantwortlichen noch die Ursachen feststellen. Es bleibt unklar, ob schon die Vorgaben oder erst deren Umsetzung in Programme fehlerbehaftet waren.

Im LEA sind Organisationsstrukturen und Verfahrensabläufe zu schaffen, die eine klare und nachvollziehbare Trennung zwischen der Vorgabenentwicklung seitens der Anwender und der Umsetzung solcher Vorgaben seitens der Programmierer bewirken.

Im Auftrag des LEA erstellt, wartet und verwaltet das LIT die *Datenfernübertragungsprogramme* für das EWW. Auch für diese Aufgabe gibt es keine Unterlagen zu den jeweiligen Aufträgen an das LIT und ebensowenig über die Abnahme der Programme durch das LEA. So ist nicht festgelegt, wer im LEA bei auftretenden Fehlern im Netz die Störungsmeldungen an das LIT vornimmt und die Entstörung überwacht, und wer im LIT zur Annahme der Störungsmeldung und Veranlassung der Entstörung berechtigt ist. Das LIT hat jedoch in diesem Zusammenhang ausdrücklich betont, daß dieser Mangel der Organisationskontrolle durch die Einrichtung einer Benutzerleitstelle behoben werden soll.

Die *Datenfernübertragung* zu den Endgeräten erfolgt über angemietete Postleitungen, Postmultiplexer, Synchronknoten vom Typ SK 12 und Multiplexer (MSF).

Während die Verteilung der Datenströme durch die MSF gezielt erfolgt, d. h. nur die für dieses Gerät abgesandten Daten über die Endleitung übertragen werden, ist der Datenverkehr auf der Sekundärseite des SK 12 bedenklich, da alle Datenströme allen angeschalteten MSF angeboten werden. Findet keine Manipulation bei der Datenübertragung statt, übernimmt immer die richtige MSF die Nachricht und alle anderen werten sie nicht aus. Kann jedoch an einer Schnittstelle oder einer Leitung eine Manipulation vorgenommen werden, können die Datenströme aller Endgeräte, die hinter dem SK 12 angeschaltet sind, aufgezeichnet werden. Die Problematik des Synchronknoteneinsatzes ist seit langem bekannt[99]. Wir hatten daher den Einsatz der SK 12 nur als Übergangslösung bis zum Einsatz des neuen Verwaltungsnetzes hingenommen. Das neue Verwaltungsnetz sollte bis 1990 installiert sein. Das Projekt scheiterte jedoch.

Die vom LIT zusätzlich vorgenommenen Sicherheitsmaßnahmen, wie die Unterbringung der MSF in verschlossenen Räumen oder Kästen, wurde von uns als zeitlich zu beschränkende Notlösung angesehen. Mit modernen Mitlesegeräten können, vorausgesetzt, ein physikalischer Zugang zu einer Leitung oder Schnittstelle gelingt, alle Daten, also auch die entsprechenden Ausweisdaten und Geräte-Identifikationen im Klartext gelesen werden.

Mangels sicherer Alternativen in einem modernen Verwaltungsnetz sollen auch alle neuen Meldestellen im Ostteil der Stadt über diese nicht datenschutzgerechte Technik mit den Vorrechnern des LIT verbunden werden.

Da trotz dieser Risiken der gesamte Datenverkehr unverschlüsselt erfolgt, liegen erhebliche Mängel der *Transportkontrolle* gemäß § 5 Abs. 3 Nr. 9 BlnDSG vor.

Wir haben nachdrücklich empfohlen, eine starke kryptographische Leitungsverschlüsselung einzuführen, zumindest für die persönlichen und verbindungstechnischen Identifikationsdaten. Wann das neue Verwaltungsnetz für die Datenverarbeitung in Betrieb gehen wird, ist noch nicht absehbar. Allerdings ist davon auszugehen, daß auch im neuen Netz die Vertraulichkeit und Integrität der Daten bei der Datenübertragung nur durch Verschlüsselungsverfahren sichergestellt werden kann.

Die für die Benutzer-, Speicher- und Zugriffskontrolle nach § 5 Abs. 3 Nr. 3, 4 und 5 BlnDSG notwendige Identifikation und Authentifikation der Benutzer erfolgt mittels einer Magnetkarte. Differenziert wird nach Verfahren (EWW, historische Daten), nach Datenbestand (Echt- oder Testdatenbestand) und nach Programmberechtigung. Wenn eine Magnetkarte dem Besitzer abhanden kommt, hat er dies zwar unverzüglich zu melden, in der Zwischenzeit kann mit der Karte jedoch unberechtigt im Verfahren gearbeitet werden. Dies entspricht nicht mehr dem heutigen Stand der Technik.

Wir haben daher empfohlen, zusätzlich zum Einlesen der Magnetkarte die Eingabe eines persönlichen Codewortes zu verlangen. Dies würde verhindern, daß bei Verlust der Karte Unbefugte damit unberechtigte Abfragen tätigen können.

Während des *Benutzerdialogs* bleibt die Magnetkarte im Leser stecken. Wird sie entfernt, bricht das Programm ab. Dies kann dazu verleiten, den Ausweis steckenzulassen, wenn für einige Zeit nicht mit dem System gearbeitet wird, um danach eine erneute Anmeldungsprozedur zu vermeiden. Es kann ferner dazu verleiten, daß Inhaber von Ausweisen mit vielen Zugriffsrechten diese im Ausweisleser lassen, um sonst notwendige Ausweiswechsel zu vermeiden.

Zur Vermeidung solcher Risiken haben wir empfohlen, dafür zu sorgen, daß der Dialog nach längeren Aktionspausen (10–15 Minuten) und bei Funktionswechseln (z. B. vom Auskunftsdienst zum Änderungsdienst) systemseitig abgebrochen wird, so daß zur Fortsetzung des Dialogs eine erneute Anmeldung notwendig wird.

Für Auskunftsersuchen außerhalb normaler Dienstzeiten bzw. an Orten, von denen aus ein anderer Zugriff auf das System nicht möglich ist, ist beim LEA ein *telefonischer Dauerdienst* eingerichtet worden.

Während bei Abfragen aus dem Netz der Polizei nach dem Meldegesetz Abfrage und Abfragegrund protokolliert werden, kann jeder, der die Telefonnummer des Dauerdienstes kennt, eine unprotokollierte Auskunft aus dem Melderegister erhalten. Gibt sich etwa jemand als Polizeibeamter aus, so werden ihm auch Daten, die über die einfache Melderegisterauskunft hinausgehen, ohne Rückruf übermittelt. Ein Rückruf bei erweiterten Auskünften erfolgt nur bei anderen Dienststellen. Die fernmündliche Angabe des Namens und der Dienststelle wird nur bei weiterführenden Auskünften beim Dauerdienst festgehalten. Mit dieser Auskunftspraxis werden die Zugriffssicherungen unterlaufen.

[99] vgl. Jahresbericht 1986, 4.1

Das Landeseinwohneramt ist nach § 12 Abs. 3 BlnDSG für die Zulässigkeit der Datenübermittlung verantwortlich. Dazu gehört - gerade beim telefonischen Dauerdienst -, daß die Identität des Anfragenden vor der Datenübermittlung, z. B. durch Rückruf, überprüft wird.

Die Praxis, Meldedaten aus dem EWW ungeprüft telefonisch zu übermitteln, ist einerseits ein Mangel der Speicherkontrolle nach § 5 Abs. 3 Nr. 3 BlnDSG, da die unbefugte Kenntnisnahme personenbezogener Daten nicht unterbunden wird, andererseits ein Mangel der Übermittlungskontrolle nach § 5 Abs. 3 Nr. 6 BlnDSG, da in diesen Fällen nicht aufgezeichnet wird, an welche Stellen wann welche Daten übermittelt worden sind. Ausnahmen für die Prüfung der Zulässigkeit von Übermittlungen durch das LEA ergeben sich nach § 25 Abs. 4 Meldegesetz nur für den Sicherheitsbereich, der seinerseits Anfragen zu protokollieren hat. Die Protokollierungspflicht der Polizei wird bei polizeilichen Anfragen über den Dauerdienst jedoch ebenfalls unterlaufen.

Wir haben empfohlen, durch Rückruf die Identität des Anfragenden zu prüfen und solche Anfragen zu dokumentieren. Ungeachtet dessen sollten *telefonische Auskünfte* über Meldedaten nur in dringenden Ausnahmefällen erfolgen, damit der Dauerdienst nicht für die bequeme Auskunftserlangung unter Umgehung datenschutzrechtlicher Schutzmechanismen mißbraucht wird.

Wohnungsanfrage beim Vermieter

Ein Bürger, der bei seiner Lebensgefährtin als Untermieter wohnt und dort auch gemeldet ist, hat sich darüber beschwert, daß die zuständige Meldestelle formularmäßig bei seiner Lebensgefährtin angefragt hat, ob er dort noch wohnt. Da diesem Schreiben weder der Grund noch die Rechtsgrundlagen zu entnehmen waren, suchte er die Meldestelle auf, um den Anlaß der Anfrage zu erkunden. Auch bei diesem Besuch erfolgte weder eine rechtliche Aufklärung noch sind ihm die Zusammenhänge, die zu der Anfrage führten, erläutert worden.

Das Landeseinwohneramt hat uns erklärt, daß Anfragen bei einer Wohnungsgeberin ausschließlich dann gestellt werden, wenn bei der Meldebehörde aus Geschäftsvorgängen (z. B. Wohnungsanfragen) der Verdacht entsteht, daß eine Anmeldung für eine Wohnung nicht den tatsächlichen Wohnverhältnissen entspricht.

Die Meldebehörde hat zwar nach § 9 Meldegesetz unrichtige Daten auch von Amts wegen zu berichtigen. Daraus folgt jedoch nicht die Befugnis, bei Zweifeln an der Richtigkeit der gespeicherten gegenwärtigen Anschrift eines Meldepflichtigen sofort an den *Vermieter* heranzutreten. Bestehen berechtigte Zweifel an der Richtigkeit einer Angabe, muß die Meldebehörde zur Klärung dieser Frage zunächst den Betroffenen selbst befragen. Dieser hat nach §§ 14, 9 Meldegesetz mitzuteilen, ob er noch immer unter der angemeldeten Anschrift wohnt.

Beim Vermieter dürfen Daten über den Meldepflichtigen ohne dessen Kenntnis nur erhoben werden, wenn eine Rechtsvorschrift dies vorsieht. Dies ist hier nicht der Fall. Das Meldegesetz enthält keine derartige Datenerhebungsbefugnis. In § 9 Abs. 1 ist lediglich die Berichtigungspflicht geregelt und in § 13 Abs. 4 die Berechtigung des Wohnungsgebers, den Auszug gegenüber der Meldebehörde anzuzeigen. Eine nach dem Berliner Datenschutzgesetz erforderliche normenklare, die Datenerhebungsvoraussetzungen im einzelnen regelnde Befugnis der Meldebehörde, beim Wohnungsgeber Daten über den Mieter zu erheben, fehlt.

Das ASOG kann nicht herangezogen werden. Nach dem Meldegesetz sollen über Meldeangelegenheiten nur Auskünfte von Betroffenen und im Ausnahmefall vom *Wohnungsgeber* erfolgen. Eine Heranziehung der Auffangbestimmungen des ASOG würde diesen Kreis erweitern und auch die Befragung anderer Personen ermöglichen. Dies widerspricht dem eindeutigen Regelungsgehalt des Meldegesetzes.

„Scheinwohnungen"

Anläßlich einer Kleinen Anfrage haben wir zu der Speicherung von *„Scheinmeldeverhältnissen"* [100] im Melderegister Stellung genommen. Dabei handelt es sich um die Anmeldung bei der Meldebehörde mit einer Wohnung, die der Betroffene in Wirklichkeit gar nicht bezogen hat bzw. bewohnt.

Der Datensatz des Melderegisters ist nach Datengruppen geordnet: Für die Speicherung von Anschriften gibt es die Gruppe G (gegenwärtige Anschrift), Gruppe F (frühere Anschriften), Gruppe H (Hauptwohnung), Gruppe N (Nebenwohnung) und Gruppe O (Scheinmeldung). Wenn das LEA der Auffassung ist, eine Anschrift sei eine Scheinmeldung, so wird sie von der Gruppe G in die Gruppe O übertragen.

Nach dem Meldegesetz darf die Meldebehörde nur gegenwärtige und frühere Anschriften sowie Haupt- und Nebenwohnung speichern. Das Merkmal „Scheinwohnung" ist in dem abschließenden Katalog der Daten, die gespeichert werden dürfen, nicht enthalten und demzufolge unzulässig. Die weitere Qualifizierung einer Wohnung geht über den vom Gesetzgeber vorgegebenen Rahmen hinaus. Dessen ungeachtet ist nicht klar, welchem Zweck die Unterscheidung dienen soll und wie diese Feststellung getroffen wird. Dem Aufgabenkatalog der Meldebehörde nach § 1 Meldegesetz können wir ihn jedenfalls nicht entnehmen.

Das Eröffnen einer neuen Datengruppe „Scheinmeldung" läuft ebenfalls dem klaren Wortlaut des Meldegesetzes zuwider, weil dadurch Rückschlußmöglichkeiten geschaffen werden und damit dieses Merkmal „durch die Hintertür" eingeführt wird. Die von der Senatsverwaltung für Inneres vorgebrachte Rechtfertigung, daß es sich bei den Gruppen um interne Arbeitsmerkmale handele, ist nicht nachvollziehbar. Im Meldegesetz ist abschließend geregelt, welche Ordnungsmerkmale zulässig sind. Dazu gehört nicht das Merkmal „Scheinwohnung". Vielmehr handelt es sich dann, wenn eine Anmeldung zum Schein festgestellt wird - um unrichtige Daten. In diesem Fall müssen die Daten berichtigt werden, was bedeutet, daß die richtigen Daten gespeichert und die unrichtigen gelöscht werden. Eine weitere Speicherung der unrichtigen Daten ist nicht zulässig.

Klärung der Konfessionszugehörigkeit

Eine Bürgerin gab bei ihrer Anmeldung bei einer Gemeinde in Süddeutschland wahrheitsgemäß an, keiner Konfession anzugehören. Wenig später erhielt sie die überraschende Mitteilung der Kirchensteuerstelle Berlin, daß ihre Kirchenmitgliedschaft zu klären sei. Wie die Kirchensteuerstelle zu der Annahme kommt, hier sei die Kirchenmitgliedschaft unklar, war der Bürgerin ein Rätsel.

In der nach der Anmeldung in Süddeutschland von der dortigen Meldebehörde dem Landeseinwohneramt übersandten Rückmeldung war bei der Religionszugehörigkeit „Ungeklärt" angegeben. Eine nach § 2 Abs. 1 Nr. 10 Meldegesetz zu erfassende Religionszugehörigkeit war somit nicht bekannt. Das Landeseinwohneramt hat außer der Erfassung der übrigen Daten der Rückmeldung nichts weiter veranlaßt. Das zuständige Bezirkseinwohneramt hatte allerdings eine weitere - dem Landeseinwohneramt bisher nicht bekannte - Mitteilung der Meldebehörde aus Süddeutschland erhalten und an die *Kirchensteuerstelle zur Klärung der Religionszugehörigkeit* weitergeleitet. In dieser Mitteilung war die Religionsangabe von „Ungeklärt" in „Keine Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft" berichtigt worden. Das Bezirkseinwohneramt hat ferner im Melderegister den Schlüssel in „Keine Religionszugehörigkeit" umgestellt.

Die Übermittlungen der süddeutschen Meldebehörde sind nach § 2 der Ersten Bundes-Meldedatenübermittlungsverordnung zulässig. Der Inhalt der Datenübermittlung - insbesondere, warum zunächst mitgeteilt wurde, die Religionszugehörigkeit sei ungeklärt - konnte von uns mangels Zuständigkeit nicht geprüft werden. Dies war hier auch nicht erforderlich, weil anschließend eine berichtigte Mitteilung erfolgte.

[100] Kleine Anfrage Nr. 2745

Die Unterrichtung der Kirchensteuerstelle war unzulässig. Nach § 27 Meldegesetz darf die Meldebehörde einer öffentlich-rechtlichen Religionsgesellschaft zur Erfüllung ihrer Aufgaben bestimmte Daten ihrer im Land Berlin wohnenden Mitglieder übermitteln. Da die Petentin keiner öffentlich-rechtlichen Religionsgesellschaft angehört und die Übermittlung der Daten auch nicht zur Klärung der Mitgliedschaft erforderlich war, scheidet § 27 Meldegesetz als Rechtsgrundlage für die Datenübermittlung aus. Die süddeutsche Meldebehörde hat in ihrer zweiten Nachricht dem Bezirkseinwohneramt mitgeteilt, daß die Religionszugehörigkeit von „Ungeklärt" in „Keine Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft" berichtigt wurde. Ein Anlaß für eine Unterrichtung der Kirchensteuerstelle bestand damit nicht. Im übrigen war das Bezirkseinwohneramt nicht berechtigt, zu dem Merkmal „Religionszugehörigkeit" Datenspeicherungen oder -veränderungen vorzunehmen. Hierzu ist nach § 1 Abs. 2 Meldegesetz ausschließlich das Landeseinwohneramt befugt[101]. Die Senatsverwaltung für Inneres teilt diese Auffassung nicht. Es ist beabsichtigt, diese Zuständigkeitsfrage bei der anstehenden Novellierung des Meldegesetzes klarzustellen.

Vorsorgliche Übermittlung an die Taxi-Genehmigungsbehörde bei nicht gezahlten Eichgebühren

Eine Taxi-Inhaberin hat vom Landesamt für das Meß- und Eichwesen (LME) eine Mahnung erhalten, weil sie die Eichkosten für ihren Fahrpreisanzeiger nicht gezahlt hat. Ihr wird weiter mitgeteilt, daß die nächste fällige Eichung erst vorgenommen wird, wenn sie den bisher rückständigen Gebührenbetrag einschießlich der bisher angefallenen Mahngebühren sowie einen Vorschuß in Höhe der voraussichtlich entstehenden Kosten entrichtet hat. Darüber hinaus – führt das LME weiter aus – erhalte das Landeseinwohneramt, Referat Fahrerlaubnisse und Personenbeförderung, eine Durchschrift dieses Mahnschreibens. Die Taxi-Inhaberin räumt ein, daß die Bezahlung der Eichgebühren durch ein Versehen in der Buchhaltung unterblieben ist, hält aber eine Information der Erlaubnis- bzw. Konzessionsbehörde, die mit diesem Vorgang (Nichtbezahlen der Eichgebühren) nichts zu tun hat, für unzulässig.

Das LME hat erklärt, daß es bei *rückständigen Eichgebühren* für Fahrpreisanzeiger regelmäßig die Taxifahrer bzw. die Konzessionäre dem Landeseinwohneramt melde. Dieses Verfahren beruhe auf einer Bitte des Landeseinwohneramtes und sei auf dem Wege der Amtshilfe zulässig.

Diese Auffassung ist unzutreffend. Die Übermittlung personenbezogener Daten zwischen Behörden und sonstigen öffentlichen Stellen ist nach § 12 BlnDSG nur zulässig, wenn eine besondere Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Die Einwilligung in die Datenübermittlung durch die Betroffene lag nicht vor. Eine besondere Rechtsvorschrift, die die Datenübermittlung erlaubt, konnte vom LME, das über die Zulässigkeit der Datenübermittlung entscheiden muß und dafür verantwortlich ist, nicht genannt werden. Es gibt auch keine.

Die §§ 4 und 5 Verwaltungsverfahrensgesetz (VwVfG) regeln lediglich die Verpflichtung zur Amtshilfe, verweisen jedoch – was die Zulässigkeit der Hilfeleistung betrifft – auf außerhalb des VwVfG bestehende Rechtsvorschriften und Grundsätze (§ 5 Abs. 2 VwVfG). Die Zulässigkeit der Übermittlung personenbezogener Daten richtet sich daher auch im Falle der Amtshilfe zunächst nach den datenschutzrechtlichen Vorschriften. Wenn danach eine Übermittlung zulässig ist, besteht nach Maßgabe der Vorschriften zur Amtshilfe eine Verpflichtung, diese vorzunehmen. Die Regelungen zum Datenschutz und der zur Amtshilfe schließen einander nicht aus, sondern ergänzen sich gegenseitig.

In § 25 Abs. 3 Personenbeförderungsgesetz (PBefG) ist spezialgesetzlich geregelt, daß der Unternehmer auf Verlangen der Genehmigungsbehörde den Nachweis zur Erfüllung seiner Verpflichtungen zu führen hat; die Finanzbehörden dürfen den Genehmigungsbehörden Mitteilungen über die wiederholte Nichterfüllung der sich aus seinem Unternehmen ergebenden steuerrechtlichen Verpflichtungen oder die Abgabe der eidesstattlichen Versicherung nach § 284 der Abgabenordnung machen. Im übrigen haben die Genehmigungsbehörden nach § 54 a PBefG weitgehende Prüfungsbefugnisse; so dürfen sie die erforderlichen Ermittlungen anstellen und dabei Einsicht in die Bücher und Geschäftspapiere nehmen und vom Unternehmer und seinen Beschäftigten Auskünfte verlangen. Das PBefG enthält also differenzierte Regelungen für die *Überprüfung des Unternehmers* durch die Genehmigungsbehörden sowie eine Datenübermittlungsbefugnis durch eine andere Behörde. Diese spezialgesetzlichen Regelungen sind abschließend. Die Auffangbestimmungen wie etwa § 44 Abs. 1 ASOG, wonach zwischen den Ordnungsbehörden personenbezogene Daten übermittelt werden dürfen, soweit diese zur Erfüllung ordnungsbehördlicher Aufgaben erforderlich sind, sind nicht anwendbar.

Unabhängig davon ist nicht erkennbar, für welche konkrete Aufgabe die Übermittlung der Tatsache, daß Eichgebühren nicht gezahlt wurden, erforderlich sein soll. Maßnahmen können aufgrund dieser Information nicht ergriffen werden. Für den Widerruf der Genehmigung müssen schwerwiegende Verstöße gegen das PBefG und die aufgrund dieses Gesetzes erlassenen Rechtsvorschriften vorliegen. Dies ist beim einmaligen Nichtbezahlen der Eichgebühren sicher nicht der Fall. Eine rein vorsorgliche Übermittlung von Verhaltensdaten der *Taxiunternehmer* an die Konzessionsbehörde ist eine unzulässige Vorratsdatenspeicherung.

Das LME hat erklärt, künftig die Mitteilungen an das Landeseinwohneramt zu unterlassen.

Medizinisch-psychologische Gutachten in Fahrerlaubnisakten

Bei der Neuerteilung von Fahrerlaubnissen nach deren Entzug fordert das Landeseinwohneramt oftmals die Beibringung eines medizinisch-psychologischen Gutachtens (MPG). Diese MPG beschreiben fast vollständig die Persönlichkeit des Betroffenen, beginnend mit der Abstammung, Geburt, Erziehung über Lebensgewohnheiten, körperliche Verfassung, Erörterung der Delinquenz bis hin zu den Untersuchungsbefunden und -ergebnissen. Diese Gutachten werden nach der Auswertung durch das Landeseinwohneramt und Erteilung des Bescheides unverschlossen zu den Akten genommen.

Nach § 5 Abs. 2 BlnDSG sind bei der Verarbeitung in nicht automatisierten Dateien oder Akten Maßnahmen zu treffen, um den Zugriff Unbefugter bei der Bearbeitung und der Aufbewahrung zu verhindern. Auf der Ebene der Verwaltungsvorschriften regelt § 68 Abs. 1 der Gemeinsamen Geschäftsordnung für die Berliner Verwaltung hierzu, daß Schriftstücke, deren Inhalt in besonderem Maß geheimhaltungsbedürftig ist – insbesondere Schriftstücke in Personalangelegenheiten und Schriftstücke, deren Inhalt einem Berufs- oder besonderen Amtsgeheimnis unterliegt, wie z. B. ärztliche Gutachten – nur den an der Bearbeitung unmittelbar Beteiligten zugänglich gemacht werden dürfen und so aufzubewahren sind, daß sie nicht von Unbefugten eingesehen werden können. In den Akten sind sie *in verschlossenen Umschlägen aufzubewahren*, wenn der Schutzzweck dies erfordert.

Bei den Gutachten handelt es sich um Unterlagen, die einem besonderen Berufsgeheimnis (§ 203 StGB) unterliegen. Sie enthalten derart viele Einzelheiten aus der Privatsphäre und über den Gesundheitszustand des Betroffenen, daß besondere Schutzmaßnahmen zu treffen sind. Sie sind verschlossen zur Akte zu nehmen. Anderenfalls ist nicht auszuschließen, daß Unbefugte die Gutachten zur Kenntnis nehmen können. Maßgeblich ist dabei nicht, ob es in der Vergangenheit bereits zu einem Verstoß gegen die besondere Geheimhaltungspflicht gekommen ist, vielmehr sind von vornherein alle Maßnahmen zu treffen, die eine unbefugte Kenntnisnahme verhindern. Es kommt weiterhin nicht darauf an, daß nur die Mitarbeiterinnen und Mitarbeiter des Referates Fahrerlaubnisse und Personenbeförderung und der Aufsichtsbehörde bzw. das Gericht auf die Unterlagen zugreifen können. Entscheidend ist, daß von den Gutachten nur Kenntnis genommen werden darf, wenn es für die ordnungsgemäße Aufgabenerfüllung im Einzelfall erforderlich ist. Das darf ausschließlich durch die mit der unmittelbaren (Sach-) Bearbeitung betrauten Dienstkräfte erfolgen. Bei dem praktizierten Verfahren kann dies nicht sichergestellt werden. Das Landeseinwohneramt hat

101 Jahresbericht 1989, 4.4

selbst eingeräumt, daß beispielsweise Aktenanforderungen von erkennbar unzuständigen Dienstkräften von der Registratur nicht zurückgewiesen werden.

Davon unberührt bleibt die unverschlossene Aufbewahrung von Bescheiden in der Akte, die regelmäßig Bezug auf die Gutachten nehmen. Die Befunde, die dort aufgenommen werden, haben sich auf die entscheidungsrelevanten Daten zu beschränken und sind nicht deckungsgleich mit den Daten im Gutachten. Das Gutachten enthält weit mehr Informationen über die persönlichen Lebensverhältnisse des Antragstellers, als in den Bescheid aufgenommen werden.

Namensänderung mit ungeahnten Folgen

Eine Bürgerin hatte ihren Geburtsnamen wieder angenommen. Vom Standesamt wurde ihr erklärt, daß sie einen Auszug aus dem Familienbuch als Nachweis für die vollzogene Namensänderung vorzulegen hat. Im Fall der Petentin enthielt der Auszug aus dem Familienbuch Angaben über den Todeszeitraum des Ehegatten („verstorben zwischen dem 1. Januar 1991 unbekannter Uhrzeit und dem 1. Februar 1991 gegen 12.00 Uhr in Berlin") sowie den Todeszeitpunkt eines Kindes. Der Petentin ist es unangenehm, daß sie dies offenlegen muß und damit viel mehr Informationen über ihre persönlichen Verhältnisse preisgibt, als zum Nachweis der Namensänderung erforderlich sind.

Nach § 12 Personenstandsgesetz (PStG) wird im Anschluß an die Eheschließung von dem Standesbeamten ein Familienbuch angelegt. Es ist abschließend geregelt, was in das Familienbuch einzutragen ist. So auch der Tod des Ehegatten, die gerichtliche Feststellung der Todeszeit, die Änderung oder allgemein bindende Feststellung des Namens und die gemeinsamen ehelich geborenen Kinder und gegebenenfalls deren Tod.

Der Standesbeamte stellt nach § 61 a PStG auf Grund seiner Personenstandsbücher nur folgende Urkunden aus:

- beglaubigte Abschriften
- Geburtsscheine
- Geburts-, Heirats- und Sterbeurkunden,
- Abstammungsurkunden
- Auszüge aus dem Familienbuch.

Die Personenstandsurkunden haben nach § 66 PStG dieselbe Beweiskraft wie Personenstandsbücher.

Nach § 65 a PStG kann die Petentin sich einen neuen *Auszug aus dem Familienbuch* ausstellen lassen und beantragen, daß die Eintragung über die Eltern und die Kinder nicht aufgenommen werden. Weitere Einschränkungen sind nicht vorgesehen. In jedem Fall werden die Angaben über den Ehegatten und hier insbesondere der Todeszeitraum eingetragen. Um dies zu vermeiden, kann sie sich eine Bescheinigung über die Eintragung der Annahme ihres Geburtsnamens ausstellen lassen. Diese Bescheinigung hat dann allerdings nicht die Beweiskraft eines Auszuges aus dem Familienbuch. Sofern bei der Vorlage dieser Bescheinigung zum Nachweis der Annahme des Geburtsnamens eine öffentliche Stelle auf der Vorlage eines Auszuges aus dem Familienbuch, das dann weitergehende, aber dafür nicht erforderliche Informationen enthält, bestehen sollte, haben wir der Petentin empfohlen, sich detailliert die Erforderlichkeit erläutern zu lassen. Wenn diese nicht dargelegt werden kann, braucht der Auszug aus dem Familienbuch nicht vorgelegt zu werden. Im privaten Bereich ist zunächst ohnehin nicht erkennbar, aus welchen Gründen sie verpflichtet sein könnte, eine derartige Urkunde vorzulegen.

Weil der Petentin hiermit nur teilweise geholfen und die Rechtslage unbefriedigend ist, haben wir den Bundesbeauftragten für den Datenschutz gebeten zu prüfen, ob nicht gesetzlich klargestellt werden kann, daß künftig der *Nachweis über die Namensänderung* mit einer Urkunde geführt werden kann, die sich auf diese Aussage beschränkt.

Wir empfehlen, daß sich auch der Senat im Bundesrat für eine entsprechende Gesetzesänderung einsetzt.

4.2.5 Ausländer, Einbürgerungen

Ausländergesetz

Die bereits mehrfach angekündigten *bundeseinheitlichen Verwaltungsvorschriften zur Durchführung des Ausländergesetzes* liegen, obwohl das Gesetz bereits seit zwei Jahren in Kraft ist, immer noch nicht vor. Sie sind insbesondere zur Konkretisierung und verfassungsmäßigen Begrenzung der Datenübermittlungsbestimmungen dringend erforderlich.

Um dieses Regelungsdefizit abzubauen, wird Hessen in Kürze Verwaltungsvorschriften, die in enger Zusammenarbeit mit dem Amt für multikulturelle Angelegenheiten der Stadt Frankfurt am Main und dem Hessischen Datenschutzbeauftragten erarbeitet wurden, in Kraft setzen.

Da die Regelungen auf Bundesebene nicht absehbar sind, sollten auch in Berlin für die Übergangszeit entsprechende Verwaltungsvorschriften in Kraft gesetzt werden. Dies könnte sofort durch Übernahme des Entwurfs erfolgen, der von einer verwaltungsübergreifenden Arbeitsgruppe unter unserer Mitwirkung erarbeitet wurde[102].

Pauschale ed-Behandlung von Asylbewerbern

Die Konferenz der Innenminister und -senatoren der Länder hat am 3. Mai 1991 im Zusammenhang mit der Einführung eines *automatisierten Fingerabdruckverfahrens* (AFIS) beschlossen, „das erkennungsdienstliche Material aller Asylantragsteller zu erfassen"[103]. Dieses Vorhaben wurde mit der Verabschiedung des Gesetzes zur Neuregelung des Asylverfahrens (AsylVerfG) vom 26. Juni 1992[104] auf eine gesetzliche Grundlage gestellt. § 16 Abs. 1 AsylVerfG bestimmt, daß „die Identität eines Ausländers, der um Asyl nachsucht, durch *erkennungsdienstliche Maßnahmen* zu sichern ist" und Lichtbilder und Abdrucke aller zehn Finger aufgenommen werden müssen. Nach § 16 Abs. 3 AsylVerfG leistet das Bundeskriminalamt Amtshilfe bei der Auswertung der gewonnenen Fingerabdrücke. Zum Einsatz kommt dabei AFIS, das Anfang Dezember 1992 vom Bundeskriminalamt in Betrieb genommen wurde. Es soll die schnelle Erfassung und Auswertung von Fingerabdrücken ermöglichen. Nachdem zunächst die Fingerabdrücke aller Asylbewerber in AFIS gespeichert werden, soll das System ab Herbst 1993 auch in der allgemeinen Verbrechensbekämpfung eingesetzt werden. Die Entwicklung des ausbaufähigen Systems, das derzeit für die Erfassung von 400 000 Asylbewerbern angelegt ist, wurde vom Bund und den Ländern mit einem Kostenaufwand von rund 100 Millionen Mark betrieben[105].

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich – gegen Bayern und Sachsen – in einer Entschließung gegen diese ausnahmslose Erfassung gewandt[106].

Die erkennungsdienstliche Behandlung fast aller Ausländer, die um Asyl nachsuchen, auch wenn deren Identität bereits feststeht, sowie die nach § 16 Abs. 5 AsylVerfG nahezu unbeschränkte Nutzung der Unterlagen für Zwecke der Strafverfolgung ist mit dem Menschenbild des Grundgesetzes und der Europäischen Menschenrechtskonvention kaum vereinbar.

Durch die pauschale ed-Behandlung, wie sie in § 16 Abs. 1 AsylVerfG bestimmt ist, werden alle betroffenen Asylbewerber wie potentielle Rechtsbrecher behandelt. Angesichts der objektiv geringen Anzahl von Mißbrauchsfällen – das Bundeskriminalamt rechnet mit fünf bis sieben Prozent[107] – ist eine derartige Maßnahme unangemessen. Nicht zuletzt wegen des massiven Eingriffs in die Persönlichkeitsrechte der Betroffenen sollten erkennungsdienstliche Maßnahmen nur nach einer Einzelfallprüfung erfolgen, wenn Zweifel an der Identität des Betroffenen bestehen.

---

102 Jahresbericht 1991, 3.4.3
103 Jahresbericht 1991, 3.4.3
104 BGBl. I, S. 1733
105 Frankfurter Rundschau vom 4. 12. 1992
106 Anlage 2.3
107 Frankfurter Rundschau a.a.O.

Das beim Bundeskriminalamt zur Verfügung stehende Fingerabdrucksystem AFIS ermöglicht zudem, daß die Fingerabdrücke aller Asylbewerber wie bei Straftätern im sogenannten *Langsatz verformelt* und damit voll recherchierfähig gemacht werden. Dadurch erhält die erkennungsdienstliche Behandlung und Erfassung aller Asylbewerber eine neue Qualität. Obwohl gegen die betroffenen Asylbewerber kein Strafverdacht vorliegt, werden sie von vornherein wie Straftäter behandelt, da die ihnen abgenommenen Fingerabdrücke in gleicher Weise wie die von Straftätern aufbereitet und zur Strafverfolgung auf Vorrat vorgehalten werden.

Dies stellt einen unverhältnismäßigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar.

Anfragen bei Arbeitgebern bei Einbürgerungen

Die Rechtsämter der Bezirke sind im Zusammenhang mit Einbürgerungen an die Arbeitgeber der Antragsteller herangetreten und haben auf einem Formular um Auskunft über die Art und Dauer des Arbeitsverhältnisses sowie über Führung, Ruf und Verhalten des Beschäftigten gebeten. Gestützt wurden diese Anfragen auf die Einwilligung des Betroffenen.

Nach § 6 Abs. 1 BlnDSG ist die Erhebung von personenbezogenen Daten nur zulässig, wenn eine besondere Rechtsvorschrift sie erlaubt oder die Einwilligung des Betroffenen vorliegt.

§§ 8 Abs. 2, 8 Abs. 1 Nr. 4 des Reichs- und Staatsangehörigkeitsgesetzes sowie Nr. 3.4 der bundeseinheitlichen *Einbürgerungsrichtlinien* bilden zwar die Rechtsgrundlage für die *Überprüfung der wirtschaftlichen Voraussetzungen,* die Überprüfungsmethode selbst ist darin jedoch nicht festgelegt. Weil es somit keine spezialgesetzliche Regelung für die Arbeitgeberanfragen gibt, wird von den Bewerbern die Einwilligung abgefordert.

Die geforderte Einwilligung ist aber ebenfalls am Erforderlichkeitsprinzip (§ 9 BlnDSG) zu messen. Das bedeutet, daß die erfragten Informationen für das weitere Verwaltungsverfahren und im Hinblick auf die Entscheidung benötigt werden. Aus den genannten Vorschriften läßt sich nicht entnehmen, daß ein Abfragen von Daten über Führung, Ruf und Verhalten des Antragstellers am Arbeitsplatz im Rahmen der Antragsbearbeitung erforderlich sein soll.

Unabhängig davon wird die beabsichtigte Datenerhebung beim Arbeitgeber auch durch den Vordruck „Erklärung zum Einbürgerungsantrag" nicht gerechtfertigt, weil darin lediglich die Zustimmung zur Überprüfung der *wirtschaftlichen* Voraussetzungen und der Erfüllung der steuerlichen Verpflichtung erteilt wird. Gemäß § 6 Abs. 2 Satz 3 BlnDSG ist der Betroffene zudem unter Darlegung der Rechtsfolgen auf sein Recht zur Verweigerung der Einwilligung hinzuweisen. Dies geschieht auf dem Vordruck nicht.

Auch der Rechtsprechung konnten wir nicht entnehmen, daß eine Arbeitgeberanfrage vorgenommen werden darf. Die Tatsache, daß ein Antragsteller nachhaltig im Stande sein muß, sich und seine Familie auf Dauer zu ernähren (so OVG Lüneburg), sagt nichts darüber aus, *wie* eine solche Feststellung zu treffen ist.

Die Nachforschungen beim Einbürgerungsverfahren betreffen den existentiellen Bereich des einzelnen und greifen tief in dessen Grundrechte ein. Zur Vermeidung von Nachteilen für den Betroffenen ist eine normenklare gesetzliche Regelung zwingend erforderlich. Die fehlende gesetzliche Befugnis kann nicht durch die Einwilligung des Betroffenen umgangen werden, wenn derartig einschneidende Entscheidungen wie die Ablehnung eines Einbürgerungsantrages zu befürchten sind.

Sowohl die Erhebung und Speicherung der *Arbeitgeberangaben* durch die Einbürgerungsbehörde als auch die Auskunftserteilung durch die Arbeitgeber ist unzulässig. Dieser Bewertung wollte sich die Senatsverwaltung für Inneres nicht anschließen, hat uns aber mitgeteilt, daß die bisher vorgenommenen Arbeitgeberanfragen im Zusammenhang mit der Neuorganisation der Staatsangehörigkeitsangelegenheiten mit Wirkung vom 1. Juli 1992 abgeschafft worden sind.

Fremdenpaß für Asylberechtigte, Staatenlose oder Kontingentflüchtlinge mit Angabe der Nasen- und Gesichtsform

Asylberechtigte, Staatenlose und Kontingentflüchtlinge, die einen Fremdenpaß oder einen Kinderausweis beantragen, müssen zusätzlich zu den üblichen Daten laut Formblatt Fragen nach ihrer Hautfarbe, Haarfarbe, Nasen- und Gesichtsform beantworten. Bei deutschen Staatsbürgern, die einen Antrag auf einen Reisepaß stellen, genügt dagegen die Angabe von Körpergröße und Augenfarbe.

Diesem Verfahren liegen alte, auslaufende *Fremdenpaßvordrucke* zugrunde, die in der Tat Fragen nach körperlichen Merkmalen enthalten, die über die von Deutschen nach § 4 Paßgesetz geforderten Angaben hinausgehen. Neue Formulare, die der zum 1. Januar 1991 in Kraft getretenen Durchführungsverordnung zum Ausländergesetz (§ 22 Abs. 1 DVO AuslG) entsprechen, wonach die als Paßersatz eingeführten Ausweise nur noch diese Angaben enthalten dürfen, sind bisher noch nicht eingeführt worden. Im vergangenen Jahr wurde zwischen Bund und Ländern Übereinstimmung dahingehend erzielt, daß zunächst entsprechend dem Gebot des sparsamen Verwaltungshandelns die vorhandenen alten Paßvordrucke Verwendung finden sollten.

Anfang Januar 1992 hat der Bundesminister des Innern einen Entwurf des Musters für das Reisedokument den Bundesländern zur Stellungnahme übersandt, das noch Angaben über Gesichtsform und besondere Kennzeichen des Dokumenteninhabers vorsah. Erst nach Intervention einzelner Länder hat der Bundesminister des Innern die Angaben über besondere Kennzeichen, Gesichtsform und Beruf gestrichen. Nach der Übergangsvorschrift des § 28 DVO AuslG durfte der alte Paßvordruck nur noch bis zum Jahresende 1992 verwendet werden.

Anders sieht es mit den *Reiseausweisen für Flüchtlinge und Staatenlose* aus. Nach der Genfer Flüchtlingskonvention von 1951 und dem Übereinkommen vom 28. September 1954 über die Rechtsstellung der Staatenlosen sind in den Ausweisen neben der Eintragung von Größe und Farbe der Augen auch die Eintragung von Haarfarbe, Nasen- und Gesichtsform, Hautfarbe, besondere Kennzeichen und Beruf enthalten.

Wir haben die Problematik an den Bundesbeauftragten für den Datenschutz herangetragen. Dieser hat mitgeteilt, daß der Erhebungsumfang beim Reiseausweis für Flüchtlinge bzw. Staatenlose, der aus internationalen Abkommen der 50er Jahre stammt, heute wohl nicht mehr so festgelegt werden würde. Angesichts vordringlicher Probleme im Ausländer- und Asylbereich sieht er gegenwärtig kaum eine Chance, zu diesem Thema weitere Initiativen zu ergreifen.

Es wäre wünschenswert, wenn der Senat zumindest hinsichtlich der Reiseausweise für Staatenlose eine Bundesratsinitiative ergreifen würde. Denn hier handelt es sich nicht um die Änderung eines internationalen Abkommens wie bei der Genfer Flüchtlingskonvention, sondern hier hat die Bundesrepublik Deutschland eigenen Spielraum. Nach dem Übereinkommen über die Rechtsstellung der Staatenlosen obliegt es den Vertragsstaaten zu prüfen, ob sie das Muster eines Reiseausweises verwenden.

4.2.6 Statistik

Landesstatistikgesetz – endlich verabschiedet

Auch mit der Verabschiedung des Landesstatistikgesetzes durch das Abgeordnetenhaus am 26. November 1992 wurde einer jahrelangen Forderung des Berliner Datenschutzbeauftragten entsprochen. Zum ersten Mal wird damit die amtliche Statistik im Land Berlin auf eine gesetzliche Grundlage gestellt.

Das Gesetz verpflichtet dazu, die Landesstatistik nach den Grundsätzen der Neutralität, der Objektivität und der wissenschaftlichen Unabhängigkeit zu organisieren. Gesetzlich fixiert ist damit auch der aus dem Urteil des Bundesverfassungsgerichts zur Volkszählung resultierende Grundsatz der *Zweckbindung* der für statistische Zwecke erhobenen Einzelangaben sowie die Verpflichtung, die Daten unter Verwendung wissenschaftlicher Erkenntnisse und unter Einsatz der jeweils sachgerechten Metho-

den und Informationstechniken zu gewinnen. Normenklarheit wurde auch hinsichtlich Rechtsstellung und Zuständigkeit des Statistischen Landesamtes erreicht. So ist das *Weisungsrecht der Fachaufsichtsbehörde* im Vergleich zum alten Rechtszustand eingeschränkt und erstreckt sich nicht mehr auf die Weitergabe von Einzelangaben, die der statistischen Geheimhaltung unterliegen. Damit wird die Eigenverantwortlichkeit des Statistischen Landesamtes bei der Wahrung des Statistikgeheimnisses und damit des Datenschutzes unterstrichen. Jedem Mitarbeiter des Statistischen Landesamtes drohen bei Verstößen gegen das *Statistikgeheimnis* strafrechtliche und dienstrechtliche Sanktionen. Das im Volkszählungsurteil des Bundesverfassungsgerichtes fixierte Gebot der strikten Abschottung von amtlicher Statistik und Verwaltungsvollzug wurde damit landesgesetzlich festgeschrieben.

Ferner regelt das Landesstatistikgesetz die Verfahren zur *Anordnung von Landesstatistiken* sowie die Maßnahmen zu deren Durchführung. Hier werden im wesentlichen die inhaltlichen Regelungen des Bundesstatistikgesetzes übernommen. Grundsätzlich bedürfen Landesstatistiken auch eines Landesgesetzes. Nur in Ausnahmefällen dürfen durch Rechtsverordnung des Senats Statistiken mit einer Geltungsdauer von bis zu drei Jahren angeordnet werden. Die Belange des Datenschutzes werden auch dadurch gesichert, daß der Berliner Datenschutzbeauftragte bei der Vorbereitung von Rechtsvorschriften, durch die Statistiken angeordnet werden, zu beteiligen ist. Darüber hinaus wurde klargestellt, daß Rechtsvorschriften über Landesstatistiken präzise die Erhebungs- und Hilfsmerkmale, die Art der Erhebung, den Berichtszeitraum, die Periodizität und den Kreis der zu Befragenden zu bestimmen haben.

In einem gesonderten Komplex werden die für den Datenschutz der Statistik entscheidenden Regelungen der *Geheimhaltung von statistischen Einzelangaben* festgeschrieben. Die Regelungen sind so gefaßt, daß in der praktischen Arbeit des Statistischen Landesamtes keine Unterschiede im Umgang mit Einzelangaben bei Statistiken für Bundeszwecke einerseits und bei Statistiken für Landeszwecke andererseits bestehen. Darüber hinaus wurde auch ein *Verbot der Reidentifizierung* von Einzelangaben aus Landesstatistiken mit anderen Angaben für die Herstellung eines Personen-, Unternehmens-, Betriebs- oder Arbeitsstättenbezugs erlassen und durch eine Strafvorschrift bewehrt. Wir haben kritisiert[108], daß der Entwurf des Landesstatistikgesetzes die Anonymisierung von statistischen Einzelangaben, die aus dem Verwaltungsvollzug für statistische Zwecke genutzt werden, noch zuließ. Die diesbezügliche Regelung wurde zwar in das Gesetz übernommen, jedoch vor der Verabschiedung durch den Unterausschuß „Datenschutz" so interpretiert, daß bei kleineren Einheiten, bei denen die Gefahr einer Deanonymisierung besteht, die Erhebungsmerkmale nicht einzelnen Gebäuden zugeordnet werden dürfen. Damit ist unserem Anliegen entsprochen worden.

Moderne statistische Informationssysteme können ihre Aufgabe nur erfüllen, wenn es möglich ist, Ergebnisse unterschiedlicher amtlicher Statistiken in sachlicher und regionaler Gliederung kombiniert auszuwerten. Diese Aufgabe stellt sich auch bei den in dem Statistischen Landesamt in der Entwicklung befindlichen *Statistischen Informationssystem (STATIS)*[109]. Vergleichbare Systeme sind auch in anderen Bundesländern und beim Statistischen Bundesamt im Aufbau und teilweise schon in Betrieb. Berlin ist das erste Bundesland, das für ein derartiges Informationssystem eine datenschutzgerechte Rechtsgrundlage geschaffen hat, die wesentlich auf unseren Empfehlungen beruht. Danach dürfen personenbezogene Daten, die im Verwaltungsvollzug auf Grund eines Gesetzes erhoben worden sind, nur dann dem statistischen Landesamt für *Sekundärstatistiken* übermittelt werden, wenn das zugrundeliegende Gesetz dies ausdrücklich zuläßt. Hat die Verwaltung dagegen Daten beim Bürger auf freiwilliger Basis erhoben, darf sie diese nur mit Einwilligung des Bürgers an die amtliche Statistik weitergeben. Dies gilt auch für Daten, die vor dem Inkrafttreten des Landesstatistikgesetzes übermittelt worden sind. Den genauen Umfang der Datenübermittlung aus dem Verwaltungsvollzug an das Statistische Landesamt hat der Senat bis zum 31. Dezember 1993 durch Rechtsverordnung zu bestimmen. Ab dem 1. Januar 1994 ist auch eine Verknüpfung und Auswertung von Statistischen Einzelangaben nur noch auf spezialgesetzlicher Grundlage zulässig. Einzelangaben aus Bundesstatistiken z. B. aus der Volkszählung 1987 dürfen mit Hilfe von STATIS dagegen weder miteinander noch mit Daten aus Berliner Landesstatistiken oder aus dem Verwaltungsvollzug verknüpft werden, weil das Bundesrecht dies nicht zuläßt.

Die konkrete Umsetzung der datenschutzrechtlichen Normen des neuen Landesstatistikgesetzes sollte zügig erfolgen. Wir werden diesem Prozeß besonderes Augenmerk widmen insbesondere hinsichtlich

- der normenklaren Fixierung von Landesstatistiken in Rechtsvorschriften,
- der Schaffung normenklarer Regelungen für den Umgang mit den im Statistischen Landesamt befindlichen Altdateien aus dem Verwaltungsvollzug und den zu regelnden Befugnissen künftiger Übermittlungen an das Statistische Landesamt,
- der Abschottung bei der Verarbeitung statistischer Daten, so bei den in Vorbereitung befindlichen Möglichkeiten des Online-Zugriffs auf die Statistische Datenbank, bei der personellen organisatorischen und räumlichen Abschottung gegenüber dem Verwaltungsvollzug, des PC-Einsatzes und der Nutzung von PC-Netzen sowie anderen Formen der kombinierten verteilten Datenverarbeitung.

Einzelprobleme

Zu den interessantesten Statistiken gehören ohne Zweifel diejenigen, die das *Wahlverhalten der Wahlberechtigten* zeigen und analysieren. Dazu kann nach dem Landeswahlgesetz der Landeswahlleiter anordnen, daß in einzelnen Stimmbezirken die Stimmzettel nach Geschlechts- und Altersgliederung gekennzeichnet werden. In der bis Januar 1992 geltenden Landeswahlordnung war jedoch nicht ausgeschlossen, daß die Stimmabgabe einzelner Personen eindeutig erkennbar ist. Wir haben deshalb eine klare Regelung empfohlen, daß in die *repräsentative Wahlstatistik* nur solche Stimmbezirke einbezogen werden dürfen, in denen in jeder Geschlechts- und Altersgruppe mindestens 20 Wahlberechtigte im Wahlverzeichnis eingetragen sind[110]. Dieser Forderung wurde mit der Zweiten Verordnung zur Änderung der Landeswahlordnung Rechnung getragen. Sie wurde erstmals bei den Wahlen zu den Bezirksverordnetenversammlungen am 24. Mai 1992 angewandt.

Auch im Jahr 1992 waren auf der Grundlage des *Mikrozensusgesetzes* rund 35 000 Berliner zur umfassenden statistischen Auskunft über ihre Lebensverhältnisse und -umstände verpflichtet. Für eine gewisse Verwirrung sorgte bei einigen auskunftspflichtigen Bürgern in den östlichen Stadtbezirken, daß ihnen zwar bei der erstmaligen Befragung im Mai 1991 mitgeteilt wurde, daß sie im jährlichen Abstand viermal hintereinander in den Mikrozensus einbezogen seien, sie jedoch bereits im Oktober 1991 und im Januar 1992 schon wieder befragt wurden. Dies betraf immerhin ein Viertel der im Mai 1991 Befragten. Die gesetzliche Grundlage für diese Zusatzbefragungen fand sich in der Mikrozensusanpassungs-Verordnung des Bundesministers für Arbeit und Sozialordnung vom 18. Oktober 1991. Diese erst im Oktober verabschiedete Verordnung wurde schon unmittelbar nach ihrer Verabschiedung durch eine Befragung umgesetzt. Eine wirksame Öffentlichkeitsarbeit, die eine wesentliche Bedingung für die bei statistischen Datenerhebungen geforderte Transparenz für den Betroffenen ist, wurde damit unmöglich. „Ad-hoc"-Statistiken mit mangelhafter Vorabinformation der Befragten sind daher aus Sicht des Datenschutzes grundsätzlich abzulehnen. Dies gilt auch für künftig durch Rechtsverordnung anzuordnende Statistiken.

Zu klären war die Frage, ob im Statistischen Landesamt eine *Abschottung zwischen* den vertraulich zu haltenden *Mikrodaten und* den der Industrie- und Handelskammer (und später der Öffentlichkeit) zugänglich zu machenden *Makrodaten* durch getrennte Rechner oder durch Softwaremaßnahmen denkbar ist. Es sind beide Varianten möglich.

[108] Jahresbericht 1991, 3.4.4
[109] vgl. Jahresbericht 1988, 4.5
[110] Jahresbericht 1989, 4.4

Während die Abschottung durch physisch getrennte Rechner, bei denen der Durchgriff vom Makrodaten-Rechner auf den Mikrodaten-Rechner auszuschließen ist, eindeutig als sicherer und vermutlich auch als wirtschaftlicherer Weg anzusehen ist, muß bei der Software-Abschottung dafür Sorge getragen werden, daß sie den gleichen Sicherheitsstandard wie die Hardware-Abschottung erreicht. Dies ist möglich, wie z. B. die gleichzeitige Nutzung von Großrechnern von Versandhäusern als Produktionsrechner und als externer Rechner am Bildschirmtextsystem zeigt.

Benutzer der Makrodatenbank dürfen keine noch so theoretische Möglichkeit haben, über ihre Schnittstellen auf Mikrodaten zuzugreifen. Die Software muß also dafür Sorge tragen, daß Benutzer der Makrodatenbank nach Identifizierung und Authentifizierung von ihren Schnittstellen aus direkt auf die Makrodatenbank geführt werden. Jeder Legitimierungsversuch für die Mikrodatenbank von diesen Schnittstellen aus muß vom Rechner abgewiesen und protokolliert werden. Letztlich läuft es darauf hinaus, den Zugriff auf die Makrodatenbank im Teilhaberverfahren zu realisieren.

Nach unserer Einschätzung dürfte der Gesamtaufwand für eine solche Software-Abschottung kaum preisgünstiger werden als die Beschaffung eines der Makrodatenbank gewidmeten Rechners. Wir haben daher für den öffentlichen Zugang an die Makrodaten die Abschottung durch getrennte Rechner empfohlen, zumal dies auch die Akzeptanz der amtlichen Statistik unterstützen würde.

Daß zunächst nur die Industrie- und Handelkammer mittels Standleitungen zugreifen soll, ändert an dieser Empfehlung nichts, denn ihr gegenüber ist das Statistikgeheimnis genauso zu wahren wie gegenüber der sonstigen Öffentlichkeit. Da die baldige Ausweitung des öffentlichen Zugriffs auf die Makrodatenbank vorgesehen ist, sollte von Anfang an die optimale Abschottung realisiert werden.

Für viele Nutzer ist die amtliche Statistik zwar eine wichtige, jedoch bei weitem nicht die einzige Datenquelle, um sachlich und regional tiefgegliederte Informationen zu erhalten. Die Grundsätze der statistischen Geheimhaltung lassen den Datenhunger von Wirtschaft und Verwaltung teilweise ungesättigt. In diese Lücken stoßen *private Datenanbieter,* die – unter Nutzung der mittlerweile fast unbegrenzten Möglichkeiten von PCs – verschiedenste Angaben aus öffentlichen Quellen mit Eigenerhebungen kombinieren und auf dem Markt anbieten. Hier entstehen Systeme, die es erlauben, Personenbezüge herzustellen sowie auch vorhandene, zunächst nicht mehr personenbezogene statistische Angaben – wenn sie eine bestimmte regionale oder sachliche Tiefe aufweisen – zu deanonymisieren. Diese Entwicklung muß sowohl vom Berliner Datenschutzbeauftragten als auch von der Aufsichtsbehörde für nichtöffentliche Stellen sehr aufmerksam verfolgt werden.

4.2.7 Personalwesen

Neues Personalaktenrecht

Das am 1. Januar 1993 in Kraft getretene *9. Dienstrechtsänderungsgesetz*[111] des Bundes regelt zum ersten Mal die Führung der Personalakten von Beamten und Richtern. Diese Regelung bleibt in zentralen Punkten hinter den Forderungen der Datenschutzbeauftragten des Bundes und der Länder zum Schutz von Arbeitnehmerdaten im Öffentlichen Dienst zurück. So bleibt die Frage ungeklärt, ob und unter welchen Voraussetzungen sich Bewerber oder Bedienstete Tests, ärztlichen Untersuchungen und anderen Überprüfungen zu unterziehen haben. Auch die dringend erforderliche gesetzliche Regelung der im Öffentlichen Dienst steht nach wie vor aus.

Das neue *Beamtenrechtsrahmengesetz* greift einige Forderungen der Datenschutzbeauftragten zur Führung von Personalakten auf und schreibt vor, daß bestimmte Vorgänge (z. B. Beihilfeanträge, Disziplinarvorgänge, Kindergeldakten) getrennt von den Hauptpersonalakten zu führen sind. Positiv zu vermerken ist die Klarstellung, daß der betroffene Beamte *Einsicht auch in Sachakten* verlangen kann, wenn und soweit sie Informationen über ihn enthalten. Dies gilt allerdings nicht für Akten der Sicherheitsüberprüfung.

Das Beamtenrechtsrahmengesetz zwingt die Länder, ihr *Landesbeamtenrecht* entsprechend zu modifizieren. Dabei legt es allerdings nur einen Mindeststandard zu Gunsten der betroffenen Beamten fest, den der Landesgesetzgeber nicht unterschreiten darf. Zulässig ist es dagegen, in das Landesbeamtenrecht Vorschriften aufzunehmen, die einen weitergehenden Datenschutz gewährleisten als es das Bundesrecht vorschreibt. Dafür werden wir uns im Zuge der Beratungen des Entwurfs für ein 23. Landesbeamtenrechtsänderungsgesetz einsetzen.

Kurz vor der Verabschiedung steht der Entwurf für das *22. Landesbeamtenrechtsänderungsgesetz,* das unter anderem eine ausnahmsweise Befugnis der Dienstbehörde enthalten wird, Befunde der amtsärztlichen Untersuchung eines Beamten anzufordern. Der ursprüngliche Entwurf der Senatsverwaltung für Inneres ließ eine Durchbrechung der ärztlichen Schweigepflicht immer schon dann zu, wenn die Dienstbehörde Zweifel am Untersuchungsergebnis des Amtsarztes („geeignet/nicht geeignet für einen bestimmten Dienstposten") hatte. Wir haben uns im Gesetzgebungsverfahren gemeinsam mit dem Hauptpersonalrat dafür eingesetzt, daß diese pauschale Regelung dahingehend präzisiert wird, daß eine Anforderung von ärztlichen Untersuchungsbefunden nur ausnahmsweise dann zulässig ist, wenn dies im Einzelfall erforderlich ist, um eine Entscheidung über die Dienstfähigkeit des Beamten treffen zu können.

Im *Personalvertretungsgesetz* sind zwar im vergangenen Jahr die *Mitbestimmungsrechte der Personalräte* bei der Einführung und Änderung von Verfahren der *IuK-Technik* gestärkt worden. Allerdings müssen auch in das Personalvertretungsgesetz noch bereichsspezifische Befugnisse der Personalvertretung zur Erhebung und Verarbeitung von Personaldaten aufgenommen werden. Ferner sollte die Mitbestimmung des Personalrats auch bei der Bestellung des behördlichen Datenschutzbeauftragten vorgesehen werden. Bisher hat der Personalrat nur dann ein Mitbestimmungsrecht, wenn ein behördlicher Datenschutzbeauftragter neu eingestellt wird, was angesichts des gegenwärtigen Stellenmangels praktisch nicht vorkommt. Das fehlende Mitbestimmungsrecht des Personalrats bei der Übertragung der Aufgaben des behördlichen Datenschutzbeauftragten auf einen vorhandenen Bediensteten der Behörde hat in der Vergangenheit häufig zu Konflikten und gegenseitigem Mißtrauen geführt, weil der behördliche Datenschutzbeauftragte als Kontrollinstanz des Dienststellenleiters verstanden wurde.

Erklärung zum Ortszuschlag

Bereits im letzten Jahresbericht[112] hatten wir kritisiert, daß vor allem *ledige Mütter im öffentlichen Dienst* in diskriminierender Weise jährlich auf einem Formular befragt werden, ob sie mit einer anderen Person zusammenleben und deshalb der Ortszuschlag gekürzt werden muß. Andere Beamtinnen und Beamte wurden bisher in dreijährigem Abstand dazu aufgefordert, das entsprechende Formular jeweils vollständig erneut auszufüllen.

Auf Grund unserer Kritik an diesem unverhältnismäßigen Eingriff in die Persönlichkeitsrechte vor allem lediger Mütter hat die Senatsverwaltung für Inneres mittlerweile zugesagt, das bisherige Überprüfungsverfahren aufzugeben und stattdessen künftig einheitlich jeweils nach drei Jahren allen Beamtinnen und Beamten einen Vordruck zuzuleiten, auf dem sie erklären können, daß eine Änderung in den für den Ortszuschlag maßgeblichen Verhältnissen nicht eingetreten ist. Damit sind unsere Empfehlungen akzeptiert worden.

Datenerhebung auf Vorrat im Disziplinarverfahren

Gegen einen Beamten wurden Vorermittlungen eingeleitet, um zu prüfen, ob eine Disziplinarmaßnahme verhängt oder ein förmliches Disziplinarverfahren eingeleitet werden sollte. Im Rahmen dieser Vorermittlungen wurde der Beamte aufgefordert, ein

111 BGBl. I, S. 1030 ff.

112 Jahresbericht 1991, 2.4

Formular „Übersicht über die wirtschaftlichen Verhältnisse" auszufüllen, in dem unter anderem auch Daten über den Beruf, den Arbeitgeber, die Marke, den Typ und das Baujahr des Kraftfahrzeugs und weitere detaillierte Angaben über den Beruf, den Arbeitgeber und die Höhe des Einkommens auch der Ehefrau erfragt wurden. Der Zweck dieser Datenerhebung wurde dem Beamten nicht erläutert. Als dieser es ablehnte, die Fragen zu beantworten, ließ der Ermittlungsführer das Formular anhand der Personalakte des Beamten ausfüllen. Bei dieser Gelegenheit teilte die personalaktenführende Stelle dem Ermittlungsführer auch mit, daß die Ehefrau des Beamten sich vor kurzem aus einem Beamtenverhältnis habe entlassen lassen.

Diese Datenerhebung war aus mehreren Gründen rechtswidrig. Zum einen erfolgte sie auf Vorrat bereits zu einem Zeitpunkt, zu dem erst der Sachverhalt dahingehend aufgeklärt werden sollte, ob der *Verdacht eines Dienstvergehens* zu Recht bestand oder nicht. Zu diesem Zeitpunkt ist es unter keinem denkbaren Gesichtspunkt für die Dienstbehörde von Interesse, welchen Autotyp der betroffene Beamte bevorzugt oder was seine Frau verdient. Eine Rechtsgrundlage für eine derartige *Datenerhebung auf Vorrat* gibt es nicht. Der Beamte hätte deshalb darauf hingewiesen werden müssen, daß es ihm freistand, die Fragen zu beantworten, und er keinerlei Nachteile zu befürchten hatte, falls er sie nicht beantwortete. Er hätte außerdem darüber aufgeklärt werden müssen, zu welchem Zweck die Daten in einem späteren Stadium des *Disziplinarverfahrens* (falls es nicht ohnehin eingestellt wird) verwendet werden sollten. Auch die Datenerhebung hinter dem Rücken des Betroffenen anhand seiner Personalakte war unzulässig.

Abgesehen davon, daß die Datenerhebung zu früh und auf Vorrat erfolgte, wäre sie auch zu einem späteren Zeitpunkt in diesem Umfang nicht erforderlich gewesen. Der Verdienst der Ehefrau kann zwar zur Beurteilung der wirtschaftlichen Verhältnisse auch des Beamten erforderlich sein, insbesondere wenn die Verhängung einer Geldbuße gegen ihn erwogen wird. Welchen Beruf die Ehegattin ausübt und wer ihr Arbeitgeber ist, hat dagegen keinerlei Bedeutung für diese Entscheidung. Diese Fragen greifen deshalb in unverhältnismäßiger Weise in das Grundrecht der Ehefrau auf informationelle Selbstbestimmung ein. Auch die Auskunft der personalaktenführenden Stelle, die Ehefrau habe sich bereits vor der konkreten Anfrage aus einem Beamtenverhältnis entlassen lassen, hätte nicht erteilt werden dürfen.

Auf Grund unserer Beanstandung hat die Senatsverwaltung für Inneres mitgeteilt, daß sie unsere Rechtsauffassung teile und dies den Dienstbehörden bereits im Jahre 1981 in einem Rundschreiben mitgeteilt habe.

Der Gleitzeitbogen – zur Einsichtnahme für alle?

In einem Bezirksamt war eine Dienstvereinbarung über die gleitende Arbeitszeit abgeschlossen worden, nach der alle Beschäftigten mit Zustimmung des Personalrats verpflichtet waren, ihren ausgefüllten Zeiterfassungsbogen, in dem sie Anfang und Ende der täglichen Arbeitszeit handschriftlich einzutragen haben, stets sichtbar am Arbeitsplatz aufzubewahren.

Darin liegt ein unverhältnismäßiger Eingriff in das informationelle Selbstbestimmungsrecht des öffentlichen Bediensteten. Zwar sind die Dienstkräfte verpflichtet, über ihre tatsächliche Anwesenheitszeit Aufzeichnungen zu führen und diese nach zwei Monaten über den unmittelbaren Vorgesetzten dem Büroleiter zuzuleiten. Der Vorgesetzte kann außerdem jederzeit von dem Bediensteten die Vorlage des laufenden Gleitzeitbogens verlangen. Dagegen kann die Dienstkraft nicht verpflichtet werden, diesen Bogen für alle Arbeitskollegen, Bürger und für den Vorgesetzten, *sichtbar an seinem Arbeitsplatz* aufzubewahren.

Das Bezirksamt hat auf Grund unseres Hinweises die entsprechende Dienstvereinbarung mit dem Personalrat geändert und die rechtswidrige Passage gestrichen.

Es handelt sich bei dieser Dienstvereinbarung nicht um einen Einzelfall. Es gibt auch eine Rahmendienstvereinbarung über die Einführung der gleitenden Arbeitszeit zwischen der Senatsverwaltung für Justiz und dem Gesamtpersonalrat der Berliner Justiz aus dem Jahre 1991, die in den einzelnen Gerichten und Dienststellen der Justizverwaltung umgesetzt wurde. Diese Dienstvereinbarungen enthalten ebenfalls die Verpflichtung zur offenen Aufbewahrung der Zeiterfassungsbögen am Arbeitsplatz.

Die Senatsverwaltung für Justiz vertritt die Auffassung, „offen" im Sinne der Dienstvereinbarung könne nur bedeuten: „offen für die jederzeitige, auch unangemeldete Kontrolle durch die Dienstaufsicht". Die Zeiterfassungsbögen dürften allerdings nicht so am Arbeitsplatz aufbewahrt werden, daß auch andere Personen (Kollegen, Bürger), die keine Befugnisse der Dienstaufsicht haben, darin Einsicht nehmen könnten. Es sei Sache der jeweiligen Dienststelle, wie die Zugangs- und Kontrollmöglichkeit jederzeit durch die Dienstaufsicht auch in Abwesenheit des Betroffenen sichergestellt werde. Die Dienstvereinbarungen müßten deshalb nicht geändert werden. Das Amtsgericht, dessen Datenschutzbeauftragter uns auf das Problem hingewiesen hatte, hat dieses jetzt einvernehmlich mit dem Personalrat dahingehend gelöst, daß die Zeiterfassungsbögen in *blickdichten Hüllen* am Arbeitsplatz ausgelegt werden sollen, so daß der Vorgesetzte auch in sie Einsicht nehmen kann, wenn die betroffene Dienstkraft nicht am Arbeitsplatz ist.

Diese Lösung trägt den datenschutzrechtlichen Erfordernissen nur zum Teil Rechnung. Auch der Vorgesetzte sollte Informationen über die Arbeitszeit seiner Mitarbeiter grundsätzlich offen bei diesem und nicht hinter deren Rücken erheben (§ 34 Abs. 2 BlnDSG in Verbindung mit § 13 Abs. 2 Satz 1 BDSG). Im Gegensatz zum Berliner Datenschutzgesetz verlangt das Bundesdatenschutzgesetz zwar nicht ausdrücklich eine Erhebung der Daten beim Betroffenen „mit seiner Kenntnis". Das Bundesdatenschutzgesetz enthält aber andererseits auch keine Befugnis zur verdeckten Beobachtung des Betroffenen. Eine Datenerhebung ist auch nur dann mit dem Grundrecht auf informationelle Selbstbestimmung vereinbar, wenn sie grundsätzlich „mit offenem Visier" bei Betroffenen stattfindet.

Ohne Mitwirkung des Betroffenen dürfen Personaldaten nach dem BDSG nur erhoben werden, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt, die zu erfüllende Verwaltungsaufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Wenn der Vorgesetzte in Abwesenheit der betroffenen Dienstkraft deren Anwesenheitszeiten überprüfen will, so ist in der Regel keine dieser Ausnahmevoraussetzungen erfüllt. Vielmehr hat es der Vorgesetzte im Regelfall hinzunehmen, daß er dem Betroffenen erst bei seiner Rückkehr in den Dienst oder an den Arbeitsplatz befragen und um Vorlage des Zeiterfassungsbogens bitten kann.

Darf der behördliche Datenschutzbeauftragte Einsicht in Personalakten nehmen?

Dem Datenschutzbeauftragten des Amtsgerichts, der uns auf die oben genannte Dienstvereinbarung hingewiesen hatte, wurde die Einsichtnahme in Personalvorgänge verweigert, die im Zusammenhang mit Verstößen gegen diese Dienstvereinbarung entstanden waren. Dabei berief sich der Direktor dieses Amtsgerichts darauf, daß der Personaldatenschutz der Einsichtnahme durch den behördlichen Datenschutzbeauftragten in diese Vorgänge entgegenstehe.

Dies widerspricht dem Berliner Datenschutzgesetz. Die datenverarbeitenden Stellen sind verpflichtet, zur Sicherstellung des Datenschutzes in ihrem Verantwortungsbereich behördliche Datenschutzbeauftragte zu bestellen (§ 19 Abs. 5). Zu diesem Bereich gehört auch die Personalaktenführung. Der behördliche Datenschutzbeauftragte ist im Verhältnis zwischen datenverarbeitender Stelle (Dienstbehörde) und Dienstkraft nicht Dritter, sondern Teil der datenverarbeitenden Stelle. Deshalb können die öffentlichen Bediensteten der Einsichtnahme in ihre Personalakte durch den behördlichen Datenschutzbeauftragten auch nicht in der Weise widersprechen, wie sie der Kontrolle ihrer Personalakten durch den Berliner Datenschutzbeauftragten widersprechen können (§ 24 Abs. 2 Satz 4 BDSG). Die Dienstbehörde ist selbst zur Einhaltung des Datenschutzgesetzes verpflichtet und

muß daher ihre eigene Personalaktenführung laufend kontrollieren und deren Rechtmäßigkeit sicherstellen. Auch dazu hat sie einen behördlichen Datenschutzbeauftragten einzusetzen, der sie allerdings nicht von ihrer eigenen Verpflichtung freistellt.

4.3 Justiz

Gesetz zur Ausführung des Gerichtsverfassungsgesetzes

Am 27. März 1992 ist das *Ausführungsgesetz zum Gerichtsverfassungsgesetz (AGGVG)* in Kraft getreten[113]. Damit wurde eine gesetzliche Grundlage für die Datenverarbeitung der Berliner Justiz geschaffen, nachdem auf Bundesebene die notwendigen Gesetzgebungsvorhaben noch immer ausstehen. Das AGGVG regelt die Voraussetzungen der Datenverarbeitung für alle Gerichtszweige und für die Staatsanwaltschaften, enthält Auskunfts- und Einsichtsrechte für andere öffentliche Stellen bzw. private Dritte in Justizakten oder -dateien sowie ein Auskunftsrecht für Betroffene.

Wir hatten im Jahresbericht 1991 unsere Kritik zu dem damals noch als Entwurf vorliegenden Gesetz dargestellt[114]. Das Gesetz ist schließlich noch mit einigen Änderungen verabschiedet worden.

Ein wesentlicher Kritikpunkt, der keine Beachtung gefunden hat, war der *Ausschluß der Dateibeschreibungspflicht* für nicht automatisiert geführte Dateien. Die in § 19 Abs. 2 BlnDSG vorgesehene, sehr differenzierte Verpflichtung zur Beschreibung des Inhalts und der Nutzung von Dateien soll bei *Karteien* der Justiz, die auf der Grundlage einer Rechts- oder Verwaltungsvorschrift geführt werden, entfallen. Diese Einschränkung ist bedenklich, da die Dateibeschreibung sowohl für automatisierte als auch für manuelle Dateien die notwendige Voraussetzung für das beim Berliner Datenschutzbeauftragten zu führende *Dateienregister* ist. Nur ein lückenloses Dateienregister gewährleistet eine wirksame Datenschutzkontrolle und stellt die Informationsrechte der Bürger sicher.

Das ursprünglich im Gesetzentwurf vorgesehene *Auskunfts- und Akteneinsichtsrecht* der Betroffenen, wurde in den parlamentarischen Beratungen eingeschränkt.

Nach § 24 Abs. 1 AGGVG erhalten die Betroffenen bei *abgeschlossenen* Verfahren Auskunft aus *Dateien* der Justizbehörden. Regelungen über ein Auskunfts- oder Akteneinsichtsrecht bei gerichtlichen oder staatsanwaltschaftlichen *Akten* fehlen. Auch fehlen Bestimmungen zum Auskunfts- und Akteneinsichtsrecht der Betroffenen während *laufender* Verfahren. Hier verweist das AGGVG auf das Verfahrensrecht. Das Verfahrensrecht enthält jedoch nur unzureichende Auskunfts- und Akteneinsichtsrechtsbestimmungen.

Nach § 147 Abs. 1 StPO besteht nur ein *Akteneinsichtsrecht während laufender Strafverfahren.* Es soll einem früheren Beschuldigten nicht Akteneinsicht für Zwecke gewährt werden, die mit seiner Verteidigung in der Strafsache nicht mehr zusammenhängen. Zwar ist in der Rechtsprechung teilweise anerkannt worden, daß die Betroffenen auch bei abgeschlossenen Verfahren ein Recht haben können, die Strafverfahrensakten einzusehen, wenn sie ein berechtigtes Interesse haben[115]. Hierfür fehlt jedoch eine eindeutige gesetzliche Regelung. Diese ist erst in dem Entwurf des Strafverfahrensänderungsgesetz vorgesehen, wonach bei abgeschlossenen Verfahren auch Auskunft aus Akten nach Maßgabe des BDSG zu erteilen ist.

Ein Rückgriff auf das Auskunfts- und Akteneinsichtsrecht der Betroffenen nach dem Berliner Datenschutzgesetz ist nicht möglich, da diese vom AGGVG ausgeschlossen wurden.

Diese Regelungslücke ist verfassungsrechtlich bedenklich. Den Betroffenen ist das Recht einzuräumen, bei abgeschlossenen Straf- oder Ermittlungsverfahren Akteneinsicht, zumindest aber Auskunft, über die zu ihrer Person in Akten gespeicherten Daten zu erhalten. Das AGGVG muß insoweit verfassungskonform ergänzt werden. Hier gelten die gleichen Überlegungen wie beim Verfassungsschutzgesetz[115 a].

Hierzu kommt, daß der Betroffene nach § 147 StPO selbst kein Recht auf Akteneinsicht hat, sondern hierfür einen Rechtsanwalt beauftragen muß. Damit verursacht die Verwirklichung des informationellen Selbstbestimmungsrechts für die Betroffenen durch die unvermeidbare Beauftragung eines Rechtsanwalts Kosten. Dieser bedenkliche Zustand wird mit dem Inkrafttreten des Strafverfahrenssänderungsgesetzes verbessert werden, das in seinem Entwurf vom 9. Januar 1990 vorsieht, daß dem verteidigerlosen Beschuldigten Auskünfte und Abschriften aus Akten erteilt werden können, soweit nicht der Untersuchungszweck gefährdet wird. Dessen Verabschiedung ist aber noch nicht absehbar[116].

Auch die in § 24 Abs. 1 AGGVG vorgesehene Beschränkung der Auskunft auf Dateien *bei abgeschlossenen Verfahren* führt zu bedenklichen Ergebnissen.

Damit soll den Belangen der Strafjustiz Rechnung getragen werden, während eines laufenden Straf- bzw. Ermittlungsverfahrens den Untersuchungszweck durch die Erteilung von Auskünften an die Betroffenen nicht zu gefährden.

Das AGGVG gilt jedoch nicht nur für den Strafprozeß, sondern für alle Justizverfahren, für die dann ebenfalls ohne ersichtlichen Grund in laufenden Verfahren das Auskunftsrecht der Betroffenen über ihre in Dateien gespeicherten Daten ausgeschlossen wird. Hinzu kommt, daß im datenintensiven Registerbereich der „Abschluß" des Verfahrens keine Rolle spielt.

Eine weitere wesentliche Änderung ist der *Ausschluß* §§ 7, 10–12, 16 und 17 *des Berliner Datenschutzgesetzes* für den gesamten Bereich der Berliner Justiz. Hiermit sind wesentliche datenschutzrechtliche Grundsätze, die das Bundesverfassungsgericht im Volkszählungsurteil festgelegt hat und die in diesen Regelungen ihren Niederschlag gefunden haben, ausgeschlossen worden (z. B. Zweckbindungsgebot – § 11 BlnDSG – und der zunächst vorgesehene, aber später wieder eingeschränkte Ausschluß des in § 9 BlnDSG enthaltenen Erforderlichkeitsgrundsatzes). Dies führt bei der Anwendung dieses Gesetzes durch die Verwaltungen teilweise zu erheblichen Schwierigkeiten, wie Einzelfälle uns bereits gezeigt haben:

> *Wer bei rechtskräftigen Bußgeldbescheiden Zahlungserleichterungen beantragt, weil es seine wirtschaftlichen Verhältnisse nicht erlauben, eine Geldbuße gleich vollständig zu bezahlen, muß der Staatsanwaltschaft viele Fragen über seine wirtschaftlichen Verhältnisse beantworten. Unter anderem sollte ein Antragsteller – unter Beifügung seiner Netto-Lohn- oder Gehaltsbescheinigung – sein monatliches Netto-Einkommen angeben, Name und Anschrift seines Arbeitgebers und seiner Krankenversicherung mitteilen sowie Auskünfte über Vermögen, Grundbesitz und Zahlungsverpflichtungen geben. Darüber hinaus sollte er sich damit einverstanden erklären, daß die Staatsanwaltschaft Auskünfte über seinen jeweiligen Arbeitgeber bei der Krankenversicherung einholt bzw. beim Finanzamt um Auskunft über seine Einkommensverhältnisse ersucht.*

Grundsätzlich ist nicht zu beanstanden, daß ein Betroffener, der Zahlungserleichterungen begehrt, schriftlich darlegt und nachweist, warum ihm die fristgemäße und vollständige Zahlung nach seinen wirtschaftlichen Verhältnissen nicht möglich ist. Dies umfaßt jedoch nicht Daten, die erst erforderlich sind, im Falle der Nichtzahlung eine wirkungsvolle Zwangsvollstreckung zu ermöglichen.

Der Einwand, die Erhebung dieser Daten sei für eine nachhaltige und zügige Vollstreckung notwendig, damit in den Fällen der Nichteinhaltung der Ratenzahlungsbewilligung beim Arbeitgeber des Vollstreckungsschuldners Lohnpfändungen vorgenommen werden können, ist nicht gerechtfertigt. Zur Durchführung der Zwangsvollstreckung genügt der Nachweis der Gehaltszahlung. Die notwendigen Angaben über den Arbeitgeber stehen damit der Vollstreckungsbehörde zur Verfügung. Das Verlangen, schon

113 GVBl. S. 73
114 vgl. 3.6
115 OLG Hamm, NJW 1984, S. 880
115 a vgl. 4.2.3
116 vgl. unten

zur Ratenzahlungsgewährung eine pauschale Einwilligungserklärung zur Einholung von *Auskünften bei Krankenversicherungen* bzw. bei Finanzämtern abzugeben, ist nicht vereinbar mit dem *Grundsatz der Erforderlichkeit.*

Die Justizverwaltung hat zwar eingeräumt, daß diese Auskunftseinholungen auch aus ihrer Sicht nicht erforderlich seien, im Hinblick auf den zum damaligen Zeitpunkt noch vorgesehen Ausschluß des § 9 Abs. 1 BlnDSG im AGGVG, der den Erforderlichkeitsgrundsatz enthält, aber keine Veranlassung gesehen werde, hier eine Verfahrensänderung vorzunehmen.

Erst nach dem auch im Rechtsausschuß des Abgeordnetenhauses energisch vorgetragenen Hinweis auf den Verfassungscharakter des Erforderlichkeitsprinzips wurde eine Änderung der Fragebögen angeordnet. Zukünftig müssen Bürger, die Ratenzahlungen bei Geldbußen beantragen, nicht mehr pauschal ihre Einwilligung zur Einholung von Auskünften bei Krankenversicherungen und Finanzämtern erklären.

Eine ähnliche Reaktion erhielten wir aber auch noch nach Inkrafttreten des AGGVG von der Präsidentin des Kammergerichts. Die Korrespondenz betraf die *Mitteilungen in Zivilsachen (Mizi)* – bundeseinheitliche Verwaltungsvorschriften, die durch das Justizmitteilungsgesetz abgelöst werden sollen. Die Mizi regeln die Mitteilungen durch die Zivilgerichte an andere öffentliche Stellen. Sie listen im einzelnen auf, welche Informationen aus gerichtlichen Verfahren anderen öffentlichen Stellen mitzuteilen sind. Durch die Regelung des § 29 Abs. 2 AGGVG ist den Verwaltungsvorschriften „Mitteilungen in Zivilsachen" (Mizi) und den „Mitteilungen in Strafsachen" (MiStra) nun Gesetzeskraft bis zum Inkrafttreten des Justizmitteilungsgesetzes verliehen worden.

Anläßlich eines Einzelfalls äußerte sich die Kammergerichtspräsidentin zu unseren Bedenken zur Erforderlichkeit bestimmter regelmäßig erfolgender Mitteilungen auf der Grundlage der Mizi folgendermaßen: Durch § 29 Abs. 2 AGGVG sei jetzt die notwendige Rechtsvorschrift geschaffen worden, die die nach der Mizi vorgeschriebenen Mitteilungen erlaubt. Ob eine Erforderlichkeit der Übermittlung gegeben war, könne indes dahingestellt bleiben; für einzelfallbezogene, wertende Betrachtungen über die Erforderlichkeit sei nunmehr kein Raum mehr.

Diese Auffassung ist mit dem in § 9 Abs. 1 BlnDSG enthaltenen, auch nach dem AGGVG zu berücksichtigenden Erforderlichkeitsgrundsatz nicht zu vereinbaren.

Bundesrecht und Datenschutz

Im gesamten Zuständigkeitsbereich des Bundes fehlen noch immer bereichsspezifische Regelungen zum Datenschutz in der Justiz. Es ist schon bemerkenswert, daß ausgerechnet in diesem Ressort die nach dem Volkszählungsurteil des Bundesverfassungsgerichts[117] erforderlichen Gesetzesnovellierungen am weitesten zurück sind.

Noch immer ist der Entwurf für ein *Strafverfahrensänderungsgesetz (StVÄG)*[118] nicht in den Bundestag eingebracht worden.

Vorab verabschiedet wurden allerdings Änderungen des Strafverfahrensrechts durch das *„Gesetz zu der Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität" (OrgKG)*[119]. Es ist am 15. September 1992 in Kraft getreten. Dieses Gesetz sieht eine erhebliche Ausweitung des Ermittlungsinstrumentariums für die Polizei und die Staatsanwaltschaft vor.

Losgelöst von der ursprünglichen Zielsetzung wurden schwerwiegende Ermittlungsmethoden wie *Rasterfahndung, verdeckte Ermittler, Wanzen, Richtmikrofone* und andere nicht konkret benannte *technische Mittel* in der StPO verankert. Diese Maßnahmen können nicht nur gegen Tatverdächtige eingesetzt werden, sondern auch gegen unverdächtige Personen. Das Ermittlungsverfahren, das bis dahin Eingriffe in Rechte Unverdächtiger nur in sehr begrenztem Umfang vorsah, hat damit eine grundsätzliche Änderung erfahren.

117 BVerfGE 65, S. 1, 44
118 Jahresbericht 1991, 3.6
119 Jahresbericht 1991, a.a.O.; BGBl. I 1992, S. 1302

Die von den Datenschutzbeauftragten gemachten Vorschläge[120] wurden im Gesetzgebungsverfahren nicht berücksichtigt. Die einzige gegenüber den vorangegangenen Vorschlägen des Bundesrats vorgenommene datenschutzrechtliche Verbesserung in der Gesetzesvorlage vom April 1991 wurde in den Beratungen im Bundestag wieder gestrichen. Es handelte sich um die Klarstellung, bei welchen Straftaten bestimmte schwerwiegende Ermittlungsmethoden eingesetzt werden dürfen. Der für die Rasterfahndung und den Einsatz verdeckter Ermittler vorgesehene *Straftatenkatalog* wurde in den Gesetzesberatungen wieder fallen gelassen. Statt dessen wurde erneut der schwammige Begriff „Straftat von erheblicher Bedeutung" verwandt.

Einzige Verbesserung des verabschiedeten Gesetzes ist, daß auf Initiative der F.D.P.-Fraktion im Bundestag die Regelungen über den Einsatz technischer Mittel zum Abhören in Wohnungen und zu heimlichen Bildaufzeichnungen in Wohnungen entfallen sind. Allerdings wurde diese Frage unmittelbar nach Verabschiedung des OrgKG wieder aufgegriffen[121].

Keine Regelung enthält die StPO nach wie vor für den *genetischen Fingerabdruck.*

Die Strafgerichte greifen in immer stärkerem Maße auf diese Methode zurück[122], um so Verdächtige identifizieren und am Tatort gefundene Spuren ihnen zuordnen zu können. Dabei wird teilweise die Aussagekraft des genetischen Fingerabdrucks überschätzt und unsorgfältig verfahren.

> *Ein Landgericht hatte die Verurteilung eines Angeklagten wegen Vergewaltigung ausschließlich mit dem „genetischen Fingerabdruck" begründet, ohne weitere Beweise zu würdigen. Der Sachverständige, auf dessen Gutachten das Gericht sich berief, hatte festgestellt, daß das am Tatort gefundene Spurenmaterial mit einer Wahrscheinlichkeit von 99,986 % von dem Angeklagten stammte. Die genetische Struktur dieses Spurenmaterials sei nur bei einer von 6937 Personen vorhanden. Der angerufene Bundesgerichtshof[123] bekräftigte seine bereits 1990 getroffene Feststellung, daß molekulargenetische Methoden zur Identifikation eines Täters niemals als einziges Beweismittel herangezogen werden dürfen. Immerhin wären bei der angegebenen Wahrscheinlichkeit insgesamt 35 männliche Einwohner der Großstadt, in der die Tat verübt wurde, als Täter in Frage gekommen.*

Der Fall verdeutlicht erneut, wie vordringlich eine klare gesetzliche Regelung des Einsatzes molekulargenetischer Methoden im Strafprozeß ist. Diese steht allerdings noch immer aus. Das Bundesministerium der Justiz hat lediglich seinem Diskussionsentwurf von 1990 im vergangenen Jahr einen Referentenentwurf zum „genetischen Fingerabdruck" folgen lassen, dessen weiteres Schicksal ungeklärt ist. Der Rechtsausschuß des Deutschen Bundestages hat die Bundesregierung wegen der zögerlichen Behandlung dieses wichtigen Gesetzgebungsvorhabens kritisiert. Inzwischen haben eine Reihe von Abgeordneten und die Fraktion der SPD im Bundestag einen Gesetzentwurf eingebracht[124].

Der Referentenentwurf enthält zwar eine Reihe von Verbesserungen gegenüber dem Diskussionsentwurf vom Dezember 1989. Insbesondere sieht er ausdrücklich vor, daß Feststellungen über genetische Anlagen nicht erfolgen dürfen. Die im Diskussionsentwurf vorgesehene Möglichkeit einer *Genomanalyse* derjenigen „sprechenden" Teile der Erbinformation, die auf äußerliche sichtbare Körpermerkmale schließen lassen, hat das Bundesjustizministerium offenbar auf Grund der Kritik der Datenschutzbeauftragten fallen gelassen. Dennoch wirft auch die jetzt vorgesehene Regelung Probleme auf. Es bleibt unklar, was mit „Feststellungen über genetische Anlagen" gemeint ist. In der Begründung des Entwurfs wird ausgeführt, etwaige „Überschußinformationen", die eventuell unvermeidbar anfallen, dürften nicht weitergegeben oder in das Verfahren eingebracht werden. Zu fordern ist demgegenüber, daß derartige Informationen nicht verwertet werden dürfen und unverzüglich gelöscht werden müssen.

120 Jahresbericht 1991, Anlage 2.4
121 siebe 4.2.1
122 vgl. dazu Jahresbericht 1989, 2.3; Jahresbericht 1990, 3.6
123 Urteil vom 12. August 1992, NJW 1992, S. 2976 f.
124 Bundestag-Drs. 12/3981

Auch greift der Referentenentwurf unsere Empfehlungen nicht auf, eine molekulargenetische Untersuchung im Strafverfahren nur zuzulassen, wenn sie im Einzelfall der geringstmögliche Eingriff in die Persönlichkeitsrechte des Angeklagten ist. Auch werden die zulässigen Untersuchungsmethoden für die Herstellung des „genetischen Fingerabdrucks" weder hinreichend präzise beschrieben noch dem notwendigen Zulassungsverfahren unterworfen.

Wie wichtig derartige Regelungen sind, zeigt der schnelle Erkenntnisfortschritt und die Entwicklung grundlegend neuer Methoden in der Molekulargenetik. So ist es inzwischen möglich, mit Hilfe der sogenannten *„Polymerase-Kettenreaktion" (PCR)* jeden Abschnitt des menschlichen Genoms schon mit Hilfe winziger Zellspuren millionenfach zu vervielfältigen und damit eine Analyse zu ermöglichen, die bisher erst ab einer bestimmten Mindestgröße des Spurenmaterials möglich war. War die herkömmliche Methode des genetischen Fingerabdrucks nur anwendbar, wenn eine bestimmte Menge Blut für die Untersuchung zur Verfügung stand, so reichen für die neue Methode schon ein Tropfen Blut, eine Haarwurzel oder Schleimhautzellen aus einer Mundspülung. Diese Verfeinerung der molekulargenetischen Methode ist von erheblicher praktischer Bedeutung und muß im Zusammenhang damit gesehen werden, daß inzwischen von privaten Herstellern *„Baukästen" (Kits) zur Erstellung von genetischen Fingerabdrücken* vermarktet werden. Damit gewinnt die Forderung der Datenschutzbeauftragten zusätzliches Gewicht, daß der Gesetzgeber Aussagen darüber treffen muß, wen das Gericht mit der Erstellung eines molekulargenenetischen Gutachtens beauftragen darf und auf welche Weise bestimmte Qualitätsstandards bei der Anwendung dieser Methoden sichergestellt werden können.

Der Polizeipräsident beabsichtigt, dem Beispiel der gerichtsmedizinischen Institute an der Freien Universität und der Humboldt Universität zu folgen und ein Verfahren der künstlichen Vervielfältigung menschlicher Erbinformationen für Zwecke der Identifikation zu nutzen, das erstmals auch den codierenden (sprechenden) Bereich der Erbinformationen mit einbezieht. Damit soll die Informationsbasis und die Aussagekraft der bisherigen Untersuchungen im nicht-codierenden Bereich erhöht werden. Zwar bestehe die technische Möglichkeit, im codierenden Bereich Überschußinformationen zu erheben, von dieser Möglichkeit werde allerdings kein Gebrauch gemacht.

Mit diesem Verfahren wird eine Grenze überschritten, die für die Datenschutzbeauftragten bisher stets von entscheidender Bedeutung war. Die Identifizierung oder Entlastung von Verdächtigen mit molekulargenetischen Methoden ist nur dann verfassungskonform, wenn diese Methoden zur vollständigen Registrierung der menschlichen Erbinformationen untauglich sind. Der Bundesminister der Justiz hat auf Grund unseres Hinweises dem Bundesbeauftragten für den Datenschutz zugesagt, diesen Gesichtspunkt in die weiteren Überlegungen zur Schaffung einer gesetzlichen Regelung zum genetischen Fingerabdruck einzubeziehen. Je länger diese Überlegungen andauern, desto größer ist die Gefahr, daß in der Praxis Methoden angewandt werden, die die kritische Grenze zwischen dem „stummen" und dem „sprechenden" Teil der menschlichen Erbinformation überschreiten.

Auch das Gesetzgebungsverfahren im Bereich des Strafvollzugs machte keine Fortschritte. Das Gesetz zur *Änderung des Strafvollzugsgesetzes,* das die Datenverarbeitung auf die notwendige gesetzliche Grundlage stellen soll, liegt noch immer nur als Referentenentwurf vor[125]. Somit bleibt der Strafvollzug ein datenschutzrechtlich weitgehend ungeregelter Bereich. Dringend notwendig ist jedoch gerade dort die Schaffung von klaren gesetzlichen Grundlagen, da im Strafvollzug in umfangreicher und vielfältiger Weise Datenverarbeitung erfolgt.

Einen besonderen Eingriff in das informationelle Selbstbestimmungsrecht des Gefangenen stellt die *Gefangenenpersonalakte* dar, die ein Sammelsurium hochsensibler Daten des einzelnen Gefangenen hält. Bislang besteht anstaltsintern hierzu ein nahezu uneingeschränkter Zugang aller Vollzugsbediensteten.

Auch Strafgefangene haben ein Recht auf Datenschutz

Ein Gefangener aus der Justizvollzugsanstalt (JVA) Moabit beschwerte sich darüber, daß er auf Anträgen zu einem Arztbesuch Angaben zu seinen Beschwerden machen muß. Diese „Vormelder" würden dann offen an den Stationsbeamten weitergegeben. Es komme häufig vor, daß Gefangene dann von einem Beamten auf ihre Krankheiten angesprochen werden. Der Gefangene machte uns außerdem darauf aufmerksam, daß Kontoauszüge, auf denen alle Angaben über Einzahler und Kontobewegungen jeder Art vermerkt sind, offen von der Zahlstelle über die Stationsbeamten an die Gefangenen weitergereicht werden.

Durch den offenen Transport von *Arztvormeldern* (Anträge für einen Arztbesuch) und *Kontoauszügen* wird ermöglicht, daß auch unbefugte Dritte von so sensiblen Daten wie Krankheitsangaben und Kontobewegungen Kenntnis erlangen können. Die Justizvollzugsanstalten sind nach § 5 Abs. 2 BlnDSG verpflichtet, technisch-organisatorische Maßnahmen zu treffen, die sicherstellen, daß persönliche Daten des Gefangenen nicht unbefugten Personen zugänglich sind. Wir haben daher den verschlossenen Transport von Kontoauszügen und Anträgen für Arztbesuche innerhalb der Anstalt gefordert. Die JVA Moabit hat mitgeteilt, daß die Gefangenen die sog. Arztvormelder auch in verschlossenen Umschlägen abgeben dürfen. Hierüber seien die Gefangenen belehrt worden. Wie die uns vorliegende Beschwerde eines Gefangenen zeigt, scheint diese Möglichkeit jedoch nicht hinreichend bekannt zu sein.

Eine verschlossene Versendung der Kontoauszüge der Gefangenen wurde von der JVA Moabit abgelehnt mit Hinweis auf den Transport durch die zuständigen Mitarbeiter und auf den finanziellen und personellen Aufwand. Ein höherer Verwaltungsaufwand kann jedoch kein Grund sein, auf datenschutzrechtlich notwendige Maßnahmen zu verzichten. Auch die Bediensteten der JVA, die die Kontoauszüge transportieren, sind nicht befugt, deren Inhalt zur Kenntnis zu nehmen.

Sonderakten für Sozialarbeiter im Justizvollzug

Ein in einer Justizvollzugsanstalt tätiger Sozialarbeiter wies uns darauf hin, daß von betreuenden Sozialarbeitern keine Sonderakten über ihrer Tätigkeit geführt werden dürfen. Die Wahrnehmungen des Sozialarbeiters werden zur Gefangenenpersonalakte genommen. Diese ist eine Sammlung personenbezogener, zum Teil hoch sensibler Daten des Gefangenen und verschafft dem Einsichtnehmenden ein umfassendes Persönlichkeitsbild des Betroffenen. Bei Besuchen verschiedener Vollzugsanstalten haben wir festgestellt, daß allen Bediensteten ein nahezu uneingeschränkter Zugriff zur Gefangenenpersonalakte möglich ist.

Wir haben empfohlen, auch für Sozialarbeiter und Anstaltspsychologen - ebenso wie es für Gesundheitsakten schon der Fall ist - die Führung von *Sonderakten* zuzulassen, um zu gewährleisten, daß die Informationen, die der Gefangene dem Sozialarbeiter im Verlaufe seiner Gespräche anvertraut, nicht in den Zugriff anderer Bediensteter gelangen, die diese Informationen für ihre Aufgabenerfüllung nicht benötigen.

Die dadurch ermöglichte umfassende Kenntnisnahme von Geheimnissen und vertraulichen Angelegenheiten der Inhaftierten durch Anstaltsleitung und andere Vollzugsbedienstete stellt eine Verletzung des informationellen Selbstbestimmungsrechts des Gefangenen dar. Darüber hinaus bringt sie Sozialarbeiter oder Anstaltspsychologen in Bedrängnis, weil diese Berufsgruppen ebenso wie Ärzte eine strafrechtlich sanktionierte Schweigepflicht haben. Wenn ein staatlich anerkannter Sozialarbeiter Informationen offenbart, die er in einem vertraulichen Gespräch mit einem Gefangenen erfährt und die seiner Geheimhaltungspflicht unterliegen, macht er sich nach § 203 StGB strafbar.

Um hier einen ausreichenden Schutz für alle Betroffenen zu gewährleisten, sollte Sozialarbeitern und Anstaltspsychologen die Möglichkeit eröffnet werden, Sonderakten über ihre Tätigkeiten zu führen, die getrennt von der Gefangenenpersonalakte aufzubewahren sind und so geführt werden müssen, daß grundsätzlich keine Zugriffsbefugnisse der Anstaltsleitung oder anderer Vollzugsbediensteter bestehen.

125 Jahresbericht 1991, 3.6

Auskünfte über Inhaftierte

Eine Justizvollzugsanstalt wandte sich wegen der täglich eingehenden Anfragen öffentlicher und privater Gläubiger, die zur Beitreibung ihrer Forderungen Informationen über Inhaftierte begehrten, an uns. So erfragte die Postbank mit Formbrief, ob ein Schuldner einsitzt und wann mit seiner Entlassung zu rechnen ist. Die AOK und ein Jugendamt wollten noch zusätzlich die neue Anschrift wissen, falls der Betroffene entlassen wurde. Das Jugendamt wollte außerdem bei einer noch nicht absehbaren Entlassung diese Tatsache schriftlich bestätigt haben. Auch über die Höhe des verwahrten Eigengeldes wird Auskunft begehrt.

Auskünfte der Justizvollzugsanstalten an andere öffentliche Stellen sind ohne Einwilligung des betroffenen Gefangenen nur zulässig, wenn eine besondere Rechtsvorschrift dies erlaubt. Dies gilt auch für Auskünfte an private Stellen.

Für die Übermittlung personenbezogener Daten von Strafgefangenen durch die Justizvollzugsanstalten an andere Stellen des öffentlichen oder privaten Bereichs existiert bisher keine Befugnisnorm im Strafvollzugsgesetz. In Berlin ist die Zuständigkeit für die *Auskunft über den Aufenthalt von Strafgefangenen* spezialgesetzlich in § 20 Abs. 2 Meldegesetz geregelt, wonach das Landeseinwohneramt über die Auskunft zu entscheiden hat. Dabei hat die Meldebehörde den Betroffenen vorher zu hören und seine schutzwürdigen Belange zu berücksichtigen. Auf Grund der spezialgesetzlichen Zuweisung an das Landeseinwohneramt war auch kein Raum mehr für Auskünfte über den Aufenthaltsort eines Gefangenen durch die Justizvollzugsanstalten auf der Grundlage der Übergangsregelung des § 34 Abs. 1 BlnDSG. Diese Auskünfte dürfen nur vom Landeseinwohneramt erteilt werden. Dies gilt ebenfalls für den Wohnsitz Haftentlassener.

Weitere Informationen über den Gefangenen, den Entlassungstermin, die Haftdauer und die Höhe des verwahrten Eigengeldes dürfen ebenfalls grundsätzlich nicht durch die Justizvollzugsanstalten herausgegeben werden.

Bei Anfragen zu freiem *Eigengeld* und zu Wertsachen sind die Gläubiger auf die abschließenden Zwangsvollstreckungsvorschriften der Zivilprozeßordnung zu verweisen.

Eine Mitteilung der *Haftdauer* bzw. des *Entlassungstermins* würde in unvertretbarer Weise in die schutzwürdigen Belange des Gefangenen eingreifen, da sich aus diesen Informationen Rückschlüsse auf die Höhe der Strafe und damit der Intensität des kriminellen Verhaltens des Betroffenen ziehen ließen.

Ausnahmsweise haben wir auf der Grundlage der Übergangsvorschrift des § 34 Abs. 1 BlnDSG eine Mitteilung über den Entlassungszeitpunkt für zulässig erachtet, wenn dieser in naher Zukunft, d. h. innerhalb eines Monats, liegt. In diesem Fall muß der Gefangene im Hinblick auf berechtigte Gläubigerinteressen hinnehmen, daß sein in Kürze bevorstehender Entlassungstermin mitgeteilt wird. Die anfragende Stelle hat dabei aber die Auskunft des Landeseinwohneramtes über den Aufenthalt in der Justizvollzugsanstalt einzureichen, damit die Anfrage bei der zuständigen Meldebehörde nicht durch ein Ersuchen auf Mitteilung des Entlassungszeitpunktes umgangen wird. Da nach dem 31. Januar 1993 keine Spezialnorm vorliegt, müssen auch diese Übermittlungen nunmehr unterbleiben. Die Senatsverwaltung für Justiz hat mitgeteilt, daß die Berliner Justizvollzugsanstalten ohne Einwilligung der Inhaftierten keine Auskünfte erteilen, wenn hierfür die Rechtsgrundlage fehlt.

Zwangsvollstreckungsankündigungen – offen im Briefkasten

Eine Bürgerin fand in ihrem Hausbriefkasten eine Mitteilung von einem Gerichtsvollzieher über eine angekündigte Zwangsvollstreckung, die einen Mitmieter gleichen Nachnamens betraf. Die Mitteilung war unverschlossen in den Briefkasten eingeworfen worden.

Der Einwurf unverschlossener Vollstreckungsaufträgen in den Briefkästen entspricht nicht den Geboten der Datensicherheit. Nach § 5 Abs. 2 BlnDSG sind bei dem Transport von Unterlagen mit personenbezogenem Inhalt Maßnahmen zu ergreifen, die den Zugriff Unbefugter verhindern. Hier ist die *Verwendung verschlossener Briefumschläge* unerläßlich.

Die Justizverwaltung vertritt demgegenüber den Standpunkt, hier liege kein Fall des Transports personenbezogener Daten vor, da der Gerichtsvollzieher die schriftliche Nachricht eigenhändig in den Bereich des Empfängers gibt, indem er ihn in den verschlossenen Briefkasten einwirft.

Dem ist nicht zuzustimmen. Der Begriff des „Transports" umfaßt auch die Phase, die zwischen dem Zeitpunkt liegt, in dem der Datenträger in den Herrschaftsbereich des Adressaten gelangt (hier Einwurf in den Briefkasten) und dem, in dem der Adressat den Datenträger tatsächlich in Gewahrsam nimmt und damit die Möglichkeit hat, selbst für die Sicherung der Daten zu sorgen.

Auch wenn Irrtümer über die Person des Empfängers nie ganz ausgeschlossen werden können, wird jedenfalls das Risiko der Kenntnisnahme derartiger Mitteilungen durch unbefugte Dritte erheblich verringert, wenn Zwangsvollstreckungsankündigungen grundsätzlich in geschlossenen Umschlag versandt oder eingeworfen werden.

In einem vergleichbaren Fall aus dem Bereich der Finanzverwaltung, wo der Vollziehungsbeamte den Vollstreckungsauftrag unverschlossen zwischen Wohnungstür und Türrahmen klemmte, wurde auf die Dienstaufsichtsbeschwerde des betroffenen Schuldners der Vollziehungsbeamte wegen eines Verstoßes gegen eine Vorschrift der Vollzieheranweisung, wonach Zwangsvollstreckungsankündigungen *verschlossen* zu hinterlassen sind, gerügt. Warum in der Justizverwaltung hier andere Maßstäbe herrschen sollen, ist nicht einsichtig.

4.4 Schule und Sport

Endlich auch Datenschutzregelungen im Berliner Schulgesetz

Mit dem Artikelgesetz[126] wurde eine Bestimmung in das Schulgesetz eingeführt, die die *Befugnis der Schulen, personenbezogene Daten von Schülern und deren Erziehungsberechtigten zu erheben und zu verarbeiten,* regelt (§ 5 a). Sie verpflichtet die zuständige Senatsverwaltung, bis zum 31. Dezember 1993 durch Rechtsverordnung Art und Inhalt der Angaben sowie Zwecke, für die diese verarbeitet werden dürfen, festzulegen. In diese Rechtsverordnung sollten die datenschutzrechtlichen Grundsätze der gegenwärtig noch bestehenden Ausführungsvorschriften wie die über *Schülerunterlagen* oder *Noten und Zeugnisse* aufgenommen werden. Datenübermittlungen sind nur noch zulässig, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat. Personenbezogene Daten des Schulpsychologischen oder Schulärztlichen Dienstes dürfen ohne Einwilligung der Betroffenen übermittelt werden, wenn sie bei verbindlichen Veranstaltungen der Schule erhoben worden sind, allerdings nur in dem Umfang, in dem sie für Entscheidungen zwingend erforderlich sind. Für Schüler vom vollendeten 14. Lebensjahr an besteht das Recht auf Auskunft und Akteneinsicht nach dem Berliner Datenschutzgesetz auch ohne Zustimmung der Erziehungsberechtigten. Eingeschränkt wird dieses Recht lediglich durch die Einspruchsmöglichkeit des Schulleiters.

Bereits Mitte des Jahres 1980 trat eine Richtlinie für die Genehmigung von *wissenschaftlichen Untersuchungen* an der Berliner Schule außer Kraft. Seitdem gab es keine diesbezüglich gültige Regelung mehr. Dieser Mangel wurde ebenfalls durch Änderung des Berliner Schulgesetzes beseitigt. Danach müssen wissenschaftliche Forschungsvorhaben in Schulen schulaufsichtlich genehmigt werden. Grundsätzlich dürfen personenbezogene Daten für Forschungsvorhaben nur mit dem schriftlichen Einverständnis der Erziehungsberechtigten oder der volljährigen Schüler verarbeitet werden, soweit nicht das im Berliner Datenschutzgesetz enthaltene Wissenschaftsprivileg greift. Auch besteht ein Übermittlungsverbot an Dritte. Veröffentlichungen personenbezogener Daten sind nur mit Einwilligung der Betroffenen zulässig.

Im Jahr 1992 wurde eine Reihe von *Forschungsvorhaben* an Berliner Schulen datenschutzrechtlich betreut. Alle diese Vorhaben gründeten sich auf die Einwilligung der betroffenen Eltern bzw.

126 GVBl. 1993, S. 40 ff., 46

Schüler. Es zeigte sich, daß die Eltern eher bereit sind, ihre Einwilligung zu geben, wenn sie umfassend über Ziel und Inhalt des Forschungsvorhabens aufgeklärt wurden und sie auch auf Wunsch über Ergebnisse informiert werden können. Forschungsprojekte, die sich über einen längeren Zeitraum mit der Entwicklung der Kinder beschäftigen und auf einer anonymisierten Verarbeitung der Daten basieren, fanden so hohe Akzeptanz. Den Eltern wurde ermöglicht, bei auftretenden Lernproblemen die Anonymität aufzulösen und sich – ohne daß der Lehrer von den Forschungsergebnissen erfuhr – von den Wissenschaftlern beraten zu lassen.

Schüler plaudern aus dem Nähkästchen

Die Rahmenpläne für die Grundschulklassen sind stark umfeld- und familienbezogen. Kinder erstellen Familienstammbäume, zeichnen Mutter und Vater bei der Arbeit, erzählen am Montagmorgen oder nach den Ferien über ihre letzten Erlebnisse.

Daraus entsteht ein Spannungsfeld zwischen pädagogischen Zielen und dem Recht auf informationelle Selbstbestimmung. Es zeigt sich, daß die pädagogische Arbeit nicht nur eine Einbahnstraße der Wissensvermittlung ist, sondern daß das vermittelte Wissen gekoppelt mit Eindrücken, Erfahrungen und Erlebnissen der Kinder und Jugendlichen durch diese auch im Rahmen der Schule reproduziert wird. Unvermeidlich werden Informationen und Angaben über die *Privatsphäre der Kinder und ihrer Familien* durch Erzählungen, schriftliche Darlegungen oder Bilder im Rahmen der Klasse öffentlich. Dies kann jedoch nicht bedeuten, daß der Unterricht ohne Beachtung der Privatsphäre durchgeführt wird. Insbesondere bei familienbezogenen Themen sollten die Pädagogen ein Gespür für die Datenschutzbelange entwickeln. Der Lehrer hat also zu prüfen, ob die angewandte Methode bzw. Fragestellung unter Beachtung des jeweiligen *Rahmenplanes* erforderlich ist und damit das mildeste Mittel darstellt. So sollte es Schülern, die ihre häusliche Sphäre nicht weiter offenbaren wollen bzw. von den Eltern dazu aufgefordert wurden, möglich sein, ein anderes Aufsatz- oder Erzählthema zu wählen. Elternabende sollten dazu genutzt werden, den Eltern die mit der Unterrichtsführung verbundene Datenschutzproblematik klarzumachen. Arbeitsbögen, die persönliche Angaben über die Eltern, wie deren Namen, Geburtsdaten und Berufe, enthalten, sollten nicht über Wochen und Monate in den entsprechenden Arbeitsunterlagen der Kinder abgeheftet und täglich zur Schule gebracht werden.

Mit viel Witz und Humor entwarfen Gymnasiasten einen Fragebogen. Jeder Abiturient hatte die Möglichkeit, sich darin in humoristischer oder ernster Form selbst darzustellen. Auch Lehrer wurden befragt. Es bestand die Absicht, diese Fragebögen zu kopieren und zu einer lustig-witzigen Abiturzeitung zusammenzufügen. Als diese Zeitung nun auf der schuleigenen Kopieranlage vervielfältigt werden sollte, hatte der Schulleiter erhebliche Bedenken.

Die Einwände gegen die Abiturzeitung waren nicht unberechtigt. Wenn man sich die Bögen genau anschaute, ergaben sie bei allen humorvollen Verdrehungen der Antworten doch recht tiefgehende Aussagen über die einzelne Persönlichkeit. Auf Grund unserer Empfehlung wurde jedem Teilnehmer die Möglichkeit gegeben, innerhalb einer bestimmten Frist seinen Fragebogen zurückzuziehen oder neu auszufüllen. Die veröffentlichten Fragebögen enthielten deshalb den Zusatz: „Die Teilnehmer wurden darauf hingewiesen, daß der beste Datenschutz natürlich im Nichtausfüllen des Fragebogens besteht. . . . Weiterhin unverbesserliche Teilnehmer an der Befragung erklärten schriftlich ihr Einverständnis zur Veröffentlichung ihrer personenbezogenen Aussagen und Falschaussagen sowie auch der unkontrollierten Weiterverwendung noch in 50 Jahren." Die Abiturzeitung wurde dem Berliner Datenschutzbeauftragten gewidmet. Dieses Beispiel unterstreicht, daß Datenschutz in der Schule nicht nur ein Thema des Informatikunterrichts sein kann und wie auch bei durchaus erfreulichen Anlässen eine Sensibilisierung für Datenschutzprobleme erforderlich sein und erreicht werden kann.

Computer in der Schule und zu Hause

Da es im Jahre 1992 noch keine bereichsspezifische Grundlage für die Verarbeitung von Schülerdaten gab, fiel es uns schwer, verbindliche Stellungnahmen zu Konzepten von *Schüler-Informationssystemen* abzugeben, die uns im Berichtsjahr vorgelegt worden waren.

Dies galt u. a. für die Programmsysteme für das *Schulsekretariat* und für die *gymnasiale Oberstufe,* die uns von einem Bezirksamt zur Begutachtung vorgelegt worden waren.

Grundsätzlich gehen wir davon aus, daß Schülerinformationssysteme nach dem Vorbild der nicht mehr als Rechtsgrundlage ausreichenden AV Schülerunterlagen die unterschiedlichen Datensammlungen über Schüler auch weiterhin zu differenzieren haben, wenn sie unterschiedlichen Zwecken dienen und von unterschiedlichen Funktionsträgern geführt werden. Schülerinformationssysteme, die diese Abgrenzungen ignorieren und insbesondere die aus diesen Abgrenzungen folgenden diffenzierten Zugriffsberechtigungen nicht realisieren, greifen in das informationelle Selbstbestimmungsrecht der Schüler unverhältnismäßig ein und sind daher unzulässig. Wenn sich im System jedoch die Zugriffsbeschränkungen so definieren lassen, daß jeder Zugriffsberechtigte nur jene Daten erhalten bzw. ändern kann, die nach den AV Schülerunterlagen von ihnen auch zu führen bzw. abzurufen sind, sich also außer der Tatsache, daß die Daten automatisiert geführt werden, an der Verfügbarkeit der Daten im Vergleich zur nicht-automatisierten Führung der Dateien nichts ändert, so bestehen keine Bedenken gegen ein solches System.

Das Sekretariatsprogramm für die Schülerdatei sah eine Erweiterung gegenüber den Ausführungsvorschriften über die Führung schriftlicher Unterlagen über Schüler (AV Schülerunterlagen) vor und führt weitere Dateien mit personenbezogenen Daten auf, die dort nicht vorgesehen sind und daher nach derzeitiger Rechtslage nicht geführt werden dürften.

Das Programm für die Oberstufe sieht im großen Umfang die längerfristige Speicherung und flexible Auswertung von Leistungsdaten vor. Gerade bei Leistungsdaten ist besonders darauf zu achten, daß normenklare Befugnisse vorhanden sind, denn es handelt sich um subjektive Urteile über Menschen, die sich in einem Abhängigkeitsverhältnis zur datenverarbeitenden und gleichzeitig beurteilenden Stelle befinden. Schon deshalb, weil Schüler keine institutionalisierten Möglichkeiten haben, die Verarbeitung ihrer Daten in der Schule zu beeinflussen, obliegt es der besonderen Fürsorgepflicht der Schule, Zurückhaltung bei der Speicherung solcher dispositiver Daten zu üben. Die Schulen müssen konkrete Anhaltspunkte dafür erhalten, was sie dürfen oder nicht. Dies bedeutet, daß die kommende Rechtsverordnung zur Verarbeitung von Leistungsdaten in der Schule etwas sagen muß.

Auch nach Inkrafttreten des § 5a SchulG wird die Verarbeitung von Schülerdaten in den AV Schülerunterlagen konkretisiert. Danach ist unter dort genau bestimmten Voraussetzungen auch die *Verwendung privater DV-Geräte* durch Lehrer möglich. Wir haben diese Ausnahmeregelung mitgetragen, da wir es für nicht hinnehmbar halten, daß Lehrer, die ihre Arbeit außerhalb des Unterrichts zu Hause zu erledigen haben, sich nicht moderner Schreibtischausstattungen bedienen dürfen, zu denen auch PCs mit Textverarbeitung gehören. Die in Nr. 14 Abs. 6 AV Schülerunterlagen genannten Voraussetzungen sollen der Schulleitung ermöglichen, ihrer Verantwortung für die dienstliche Verarbeitung personenbezogener Daten von Schülern gerecht zu werden, und die Voraussetzungen für eine externe Kontrolle durch den Berliner Datenschutzbeauftragten liefern. Diese Bestimmung bietet einen praktikablen Weg, private PCs für dienstliche Zwecke einzusetzen.

Es zeigt sich allerdings in der Praxis, daß viele Lehrer *eigene PCs* verwenden, ohne diesen Voraussetzungen gerecht zu werden. Insbesondere kommen sie ihrer Pflicht nicht nach, personenbezogene Dateien, die sie zu Hause verarbeiten, zum Dateienregister zu melden. Zu dem nach altem Recht gegenüber der heutigen Situation noch einfacher strukturierten Dateienregister hat genau ein Lehrer eine Datei gemeldet. Dies steht im krassen Gegensatz zu den allenthalben in Lehrerkreisen wohlfeilen Hinweisen, daß eine Vielzahl, wenn nicht die Mehrzahl der Lehrer Schülerdaten auf eigenen Rechnern zu Hause verarbeiten.

Auf Anfragen aus dem Kreis der Schuldatenschutzbeauftragten haben wir uns auch zu dem Rahmen geäußert, in dem sich die häusliche Verarbeitung von Schülerdaten zu bewegen hat:

- Für *Leistungsdaten* (Zeugnisse, Zensurenlisten) gilt wegen ihrer besonderen Schutzbedürftigkeit der Grundsatz, daß sie zwar im Rahmen der Textverarbeitung erstellt werden dürfen, nach Fertigstellung des Textes aber zu löschen sind. Eine Speicherung auf längere Dauer halten wir in jedem Fall für unzulässig, bevor der Schulgesetzgeber eine entsprechende Befugnis dieser sensiblen Daten dort schafft, wo dies erforderlich erscheint (etwa in der gymnasialen Oberstufe).
- *Aufgaben der Schulverwaltung* dürfen nicht auf eigene Personalcomputer abgewickelt werden. Wenn dies automatisiert erfolgen soll, hat dies in den Räumen der Schule zu geschehen. Anders als bei normalen Lehrern ist bei Funktionsträgern, die Daten zu Zwecken der Schulverwaltung (Schülerdatei, Lehrerdatei, Stundenplanerstellung, Raumverteilung, Organisation von Betriebspraktika etc.) verarbeiten, davon auszugehen, daß ihnen in der Schule die dafür erforderlichen Arbeitsräume zur Verfügung stehen.

Der Datenschutz als „Olympische Disziplin"

Im Juni 1992 berichtete ein Fernsehmagazin über die angebliche Speicherung sensibler personenbezogener Daten der Mitglieder des Internationalen Olympischen Komitees (IOC) im Zusammenhang mit der Bewerbung Berlins für die Austragung der Olympischen Spiele im Jahr 2000.

Zur Vorbereitung der Olympia-Bewerbung hat das Land Berlin die *Berlin 2000 Olympia GmbH* gegründet, bei der es die Mehrheit des Stammkapitals hält. Außerdem ist die Berlin 2000 Marketing GmbH gegründet worden, deren Stammkapital ganz überwiegend von privaten Sponsoren gehalten wird. Der Anteil des Landes Berlin am Kapital dieser Gesellschaft ist sehr gering. Schließlich hatte die Berlin 2000 Olympia GmbH bereits im August 1991 ein privates Beratungsunternehmen damit beauftragt, eine *„Bewerbungsstrategie Olympische Spiele in Berlin 2000"* zu erarbeiten.

Die Berlin 2000 Olympia GmbH unterliegt der Kontrolle durch den Berliner Datenschutzbeauftragten. Man wird die Bewerbung um die Austragung der Olympischen Spiele als Aufgabe der öffentlichen Verwaltung anzusehen haben, die das Land Berlin durch eine Gesellschaft des privaten Rechts wahrnehmen läßt. Diese ist deshalb ebenso wie öffentliche Stellen des Landes Berlin zum Schutz personenbezogener Daten nach dem Berliner Datenschutzgesetz verpflichtet (§ 2 Abs. 1 Satz 2 BlnDSG). Da Berlin jedoch mit anderen Städten um die Austragung der Olympischen Spiele im Jahr 2000 konkurriert, ist es sachgerecht, die datenschutzrechtlichen Vorschriften über Wettbewerbsanstalten entsprechend anzuwenden (§ 2 Abs. 2 BlnDSG), so daß statt der strengeren Vorschriften des Berliner Datenschutzgesetzes der 3. Abschnitt des Bundesdatenschutzgesetzes gilt. Demgegenüber sind die *Berlin 2000 Marketing GmbH* mit einer Minderheitsbeteiligung des Landes Berlin und das private Beratungsbüro nichtöffentliche Stellen, die der Kontrolle durch die Aufsichtsbehörde - in Berlin die Senatsverwaltung für Inneres - unterliegen.

Sofort nach Bekanntwerden der in den Medien erhobenen Vorwürfe haben wir die Berlin 2000 Olympia GmbH und - in Amtshilfe für die Senatsverwaltung für Inneres - auch die Berlin 2000 Marketing GmbH überprüft. Bei der Berlin 2000 Olympia GmbH stellten wir fest, daß auf einem PC u. a. sechs Dateien mit personenbezogenen Daten über *IOC-Mitglieder* eingerichtet waren. Dabei handelte es sich um eine Adreßdatei, eine Datei mit Angaben über Art und Anlaß von Kontakten, Inhalt von Kontakten, Kontaktpersonen und Datum des Kontaktes, eine weitere Datei mit Angaben über Art, Anlaß und Datum von Geschenkübergaben, eine Datei mit Angaben über Muttersprache, Sprachraum sowie praktizierte Sprachen, eine Datei mit Angaben über aktive Sportarten sowie Sportfunktionen und schließlich eine Datei mit Hobbybeschreibungen. Die gespeicherten Informationen über die IOC-Mitglieder waren durchweg sachbezogener Art und ließen keine Beeinträchtigung schutzwürdiger Belange erkennen.

Den Dateieintragungen liegen papierene Unterlagen zugrunde, die in der für die Betreuung der IOC-Mitglieder zuständigen Abteilung gesammelt werden. Diese Unterlagen enthalten zu allen aktiven und Ehrenmitgliedern des IOC zunächst Kopien aus einem einschlägigen Handbuch, in dem eine Reihe personenbezogener Daten über die einzelnen Mitglieder veröffentlicht sind. Zusätzlich sind dort Presseausschnitte und Durchschriften des geführten Briefwechsels abgelegt. In einem Fall wurde ein Protokoll über einen Berlin-Besuch gefunden. Die Begleitperson hatte hier den Verlauf des Besuches notiert; in diesem Zusammenhang wurden Angaben über besondere Vorlieben des Gastes gemacht („trinkt gern Bier", „Vorliebe für deftiges Essen", „wegen der Körpergröße Wunsch nach besonders langem Bett", „Vorliebe für Jazz-Musik"). Im Hinblick darauf, daß die *Betreuung der Besucher* zu den Aufgaben der Berlin 2000 Olympia GmbH gehört, sind auch diese Daten als sachgerecht anzusehen. Hinweise auf die Speicherung beeinträchtigender Daten oder treuwidrige Datenerhebungen (§ 28 BDSG) wurden nicht festgestellt. Bei der anschließenden Überprüfung der *Berlin 2000 Marketing GmbH* wurden keine personenbezogenen Datensammlungen vorgefunden. Die Aktivitäten dieser Gesellschaft beschränken sich darauf, von den Sponsoren bestimmte Leistungen für die eingeladenen IOC-Mitglieder (z. B. Reservierung eines Zugabteils durch die Bundesbahn) zu erwirken.

Die Überprüfung der privaten Consulting-Firma durch die Senatsverwaltung für Inneres als Aufsichtsbehörde ergab, daß dort Überlegungen zur Führung einer Sammlung personenbezogener Daten der IOC-Mitglieder in einer PC-gestützten Datei angestellt worden waren. Im Rahmen dieser Überlegungen wurde probeweise eine Datei mit Phantasie-Daten aufgebaut. Das Consulting-Unternehmen selbst gelangte jedoch noch während der Probephase zu der Überzeugung, daß die Führung dieser Datei rechtlich und moralisch nicht zu rechtfertigen sei. Diese Auffassung wurde auch von der Berlin Olympia 2000 GmbH geteilt, woraufhin Anfang September 1991 alle entsprechenden Dateien sowohl bei der *privaten Consulting-Firma* als auch bei der Berlin Olympia 2000 GmbH gelöscht und alle papierenen Datenträger vernichtet worden wären. Es ist nicht auszuschließen, daß Teile dieser *hypothetischen Spiel-Datei* vor der Vernichtung entwendet und später dem Fernsehmagazin zugespielt worden sind.[127] Abschließend läßt sich feststellen, daß die in den Medien erhobenen Vorwürfe, bei der Berliner Olympia-Bewerbung sei gegen Datenschutzrecht verstoßen oder die Persönlichkeitsrechte der Mitglieder des IOC verletzt worden, sich nicht bestätigt haben.

4.5 Soziales

Unterstützungsbetrug - kein Fall für den Datenschutz

Ein Amt betreut in einem Heim obdachlose Mitbürger. Ein Großteil dieser Klientel empfängt von einem anderen Amt laufende Hilfe zum Lebensunterhalt. Einer der im Heim tätigen Betreuer erfährt, daß ein Heimbewohner, welcher Sozialhilfe bezieht, gleichzeitig über erhebliche Geldmittel verfügt, sei es, daß bei diesem Bargeld gefunden wird, sei es, daß dieser schwarz arbeitet. Es liegt deshalb der Verdacht eines Unterstützungsbetruges nahe. Fraglich ist, ob der Betreuer berechtigt ist, seine Erkenntnisse dem Sozialamt zu übermitteln.

Wir haben die Zulässigkeit der Datenoffenbarung aus § 69 Abs. 1 Nr. 1 SGB X abgeleitet. Dies gilt in jedem Falle dann, wenn das Heim ohnehin in bezirklicher Trägerschaft geführt wird. Allerdings sollten die Leistungsempfänger spätestens beim Antritt des Heimaufenthaltes darüber informiert werden, daß die Betreuer verpflichtet sind, Erkenntnisse über die wirklichen Vermögensverhältnisse des Leistungsempfängers an die zuständige Leistungsbehörde weiterzuleiten. Grundsätzlich sollte jedoch dem Betroffenen zunächst selbst die Möglichkeit gegeben werden, entsprechende Angaben nachzuholen. Dies ergibt sich aus der Mitwirkungspflicht nach § 60 SGB I i. V. m. § 20 SGB X. Ohnehin wird im Antrag auf wirtschaftliche Hilfen die Einwilli-

[127] Vgl. die Schreiben des Regierenden Bürgermeisters als Vorsitzenden des Aufsichtsrats der Berlin 2000 Olympia GmbH sowie des Geschäftsführers dieser Gesellschaft und der privaten Consulting-Firma, veröffentlicht im LPD vom 8. Juli 1992, S. 2 ff.

gung in die Datenoffenbarung und in die Überprüfung der Vermögensverhältnisse erklärt. Wenn zusätzlich zu Beginn des sozialen Betreuungsverhältnisses darauf aufmerksam gemacht wird, daß sich der besondere Vertrauensschutz nicht auf wahrheitswidrige Angaben bezieht, ist ein Schutzbedürfnis für eine etwaige unredliche Antragstellung und Leistungsgewährung nicht mehr gegeben. Die Verhinderung des Unterstützungsbetruges stellt ein wesentliches Element der Aufgabenerfüllung nach § 69 Abs. 1 Nr. 1 SGB X dar.

Dem soll auch die Schlußerklärung im *Sozialhilfeantrag* dienen. Die derzeit gebräuchliche Formularfassung wurde im Einvernehmen mit uns vor mehreren Jahren entwickelt. Gleichwohl haben sich in jüngster Zeit Beschwerden gegen diese Formulierung ergeben. Auf Grund der veränderten Rechtslage, die durch die Neufassung von Teilen des Sozialgesetzbuches und durch die Weiterentwicklung des Datenschutzrechtes im sozialen Bereich eingetreten ist, haben wir empfohlen, die Formulierung zu überarbeiten und dabei die folgenden Grundsätze zu berücksichtigen:

- Grundsätzlich sind Daten beim Betroffenen und mit seiner Kenntnis zu erheben.
- Die Verpflichtung zur Preisgabe personenbezogener Daten bedarf einer bereichsspezifischen präzisen gesetzlichen Regelung.
- Die Vorschriften sind – unter Beachtung des verfassungsmäßigen Prinzips der Verhältnismäßigkeit – auszulegen und anzuwenden. Es ist insbesondere auf die Geeignetheit, geringstmögliche Beeinträchtigung und angemessene Zweck-Mittel-Relation zu achten.

Diese Grundgedanken sind auf die Auslegung der Vorschriften in §§ 60 bis 67 SGB I anzuwenden. Die Einverständniserklärung unter dem Antragsbogen auf Sozialhilfe mußte dem angepaßt werden. Wir hatten Bedenken dagegen geäußert, daß die Geldinstitute nicht genannt waren, der Zeitraum der Erklärung nicht spezifiziert war und die Ermächtigung zeitlich oder räumlich unbegrenzt war.

Bei der bisher gebräuchlichen Formulierung wäre es möglich, alle Kreditinstitute über vorhandene Konten zu befragen. Die Erklärung mußte auf ein angemessenes Verhältnis zurückgeführt werden. Wir haben empfohlen, die Kreditinstitute, bei denen Konten des Antragstellers bestanden, konkret aufzuführen und den Antragsteller über die gesetzlich gegebenen Möglichkeiten der Sachverhaltsaufklärung von Amts wegen zu informieren, insbesondere auf §§ 20, 21 Abs. 4 SGB X (Auskunft von Finanzbehörden) hinzuweisen, sowie darauf, daß beim Betrugsverdacht die Ermittlung des Sachverhaltes auch ohne seine Beteiligung erfolgen kann. Hierzu ist mit der Senatsverwaltung für Soziales eine schnelle Einigung erfolgt.

Amtsärztliche Gutachten zum Abheften

Wer nach abgeschlossenem Sozialarbeitsstudium einen Antrag auf staatliche Anerkennung als Sozialarbeiter stellt, war durch eine „Gemeinsame vorläufige Ordnung" aus dem Jahre 1968 gezwungen, neben Lebenslauf, Lichtbildern, polizeilichem Führungszeugnis und Nachweis über Hauptprüfungen und Berufspraktikum auch ein amtsärztliches Zeugnis zu den Akten zu geben. Jeder Bewerber wurde vor seinem Gang zum Amtsarzt gezwungen, darüber nachzudenken, ob er unter das Bundesseuchengesetz fällt, unter nervösen Störungen leidet, regelmäßig Arzneimittel einnimmt oder gar raucht und Alkohol trinkt. Gefragt wurde auch, unter welchen Krankenheiten Geschwister, Eltern oder Großeltern litten und ob – bei weiblichen Antragstellern – gerade eine Regelblutung besteht.

Dieser Auszug aus dem Fragenkatalog macht deutlich, daß amtsärztliche Untersuchungen, die ja bekanntlich nicht auf Freiwilligkeit und freier Arztwahl beruhen, mit erheblichen Zwängen zur Preisgabe sensibler Daten verbunden sind. Zwar wird das Ergebnis nicht detailliert übermittelt, es bleibt jedoch beim Amtsarzt gespeichert. Hier handelte es sich keineswegs um eine Einstellungsuntersuchung, sondern lediglich um ein Anerkennungsverfahren, das keinen Anspruch auf einen künftigen Arbeitsplatz sichert. Es ist auch kein Fall bekannt, daß auf Grundlage des amtsärztlichen Zeugnisses ein Bewerber abgelehnt wurde. Dieses Verfahren wurde von uns daher als unverhältnismäßig bemängelt. Seit dem 31. Oktober 1992 wird für die staatliche Anerkennung als Sozialarbeiter kein amtsärztliches Gutachten mehr verlangt.

Darüber hinaus genügt die „Gemeinsame vorläufige Ordnung" nicht den Anforderungen an Rechtsgrundlagen für Datenerhebungen. Eine normenklare Rechtsvorschrift über die Ausbildung und Berufszulassung der Sozialarbeiter ist notwendig.

Berliner Automatisiertes Sozialhilfe-Interaktions-System BASIS

Bereits im Vorjahr[128] haben wir ausführlich über das Automationsprojekt BASIS in der Berliner Sozialverwaltung berichtet. Im Rahmen dieses Projektes sollen alle Arbeitsplätze der Sachbearbeiter, die in den Sozial- und Jugendämtern der Bezirke und in der Zentralen Sozialhilfestelle für Asylbewerber beim Landesamt für Zentrale Soziale Aufgaben (LASoz) mit Aufgaben aus dem Bundessozialhilfegesetz betraut sind, Computerunterstützung erhalten.

Im Rahmen der Voruntersuchung wurden die Varianten PROSOZ-Bremen (mit *zentraler Datenhaltung* im Landesamt für Informationstechnik [LIT]) und PROSOZ-Herten (mit *dezentraler Datenhaltung* bei den datenverarbeitenden Stellen) in verschiedenen Bezirksämtern erprobt. Mit Abschluß der Voruntersuchung wurde entschieden, daß der dezentralen Variante PROSOZ-Herten der Vorzug gegeben werden soll und daß die Ausgestaltung dieses Verfahrens und seine Anpassung an Berliner Verhältnisse Gegenstand der jetzt beginnenden Hauptuntersuchung sein soll. In den Bezirksämtern sollen lokale Netze in Client-Server-Architektur installiert werden. Die Server, auf denen die Datenhaltung erfolgt, sollen mit einer Variante des Betriebssystems UNIX ausgestattet werden, während die Arbeitsplätze mit Personalcomputern mit dem Betriebssystem MS-DOS (Clients) ausgerüstet werden sollen. Das LIT soll über Datenfernverbindungen Leistungen zur Systemverwaltung erbringen, soweit sie nicht vor Ort präsent sein müssen.

Die bereits im Vorjahr ausführlich behandelte Frage, ob es zulässig ist, einen *allgemeinen Datenaustausch zwischen den Bezirken* mit dem Ziel zu ermöglichen, Sozialhilfebetrug durch Mehrfachbeantragung der Sozialhilfe sofort erkennbar zu machen, ist nicht weiter geklärt worden. Wir hatten im Lenkungsausschuß immer wieder deutlich gemacht, daß ohne gravierende Rechtsänderungen die Rechtsgrundlagen für einen solchen Datenverbund nicht vorliegen und überdies der befürchtete Sozialhilfebetrug mit diesem Verfahren in vielen Fällen, insbesondere bei Zuzug aus anderen Kommunen, nicht entdeckt werden könne. Das Problem wurde im Rahmen der Voruntersuchung ausgeklammert. Dies bedeutet allerdings auch, daß eine Auseinandersetzung mit unseren Argumenten und den von uns vorgebrachten und im letzten Jahresbericht bereits beschriebenen Alternativempfehlungen nicht erfolgte. Dies wird daher der jetzt beginnenden Hauptuntersuchung überlassen bleiben.

Im Laufe der Hauptuntersuchung werden die Bezirke mit der notwendigen Informationstechnik ausgestattet. Die zentrale Systemadministration wird mit dem Anschluß des Systems im Bezirksamt Schöneberg an einen UNIX-Rechner im LIT erprobt.

Da im Rahmen der Hauptuntersuchung mit personenbezogenen Echtdaten operiert werden soll, wurden *„Empfehlungen zum Datenschutz und zur Datensicherheit* für die Phasen der Hauptuntersuchung incl. Erprobung von PROSOZ-Herten und Erstellung von Pflichtenheft und Ausschreibung" erarbeitet.

Nachdem eine erste Fassung grundsätzliche Aussagen enthielt, die darauf hindeuteten, daß elementare Datenschutzanforderungen im Rahmen der Hauptuntersuchung unbeachtet bleiben sollten und insbesondere im Gesamtprojekt dem Datenschutz und der Sicherheit der Informationstechnik nur eine untergeordnete und möglichst kostenneutrale Bedeutung zugemessen werden sollte, konnten wir darauf hinwirken, daß in einer zweiten Fassung für die Hauptuntersuchung noch einige Unterlassungen ver-

128 Jahresbericht 1991, S. 9

mieden werden konnten und für das Gesamtprojekt nicht die Chance verbaut wurde, ein der Bedeutung, der Größe und der Sensibilität der Daten angemessenes *Datenschutzkonzept* zu entwickeln.

Die Senatsverwaltung für Soziales geht nunmehr davon aus, daß für Maßnahmen zum Datenschutz und zur Datensicherung mindestens 5 % der Gesamtinvestitionsausgaben anzusetzen sind. Ferner wird explizit festgehalten, daß für die Maßnahmen zum Datenschutz und zur Datensicherung in der Hauptuntersuchung für das Gesamtprojekt ein Konzept erstellt werden soll.

Wir begrüßen diese Aussagen ausdrücklich und halten beides für ein Projekt dieser Größenordnung und Bedeutung für angemessen.

Nichtsdestoweniger enthält das Datenschutzkonzept für die Hauptuntersuchung noch *Mängel.* Ob sie zu realen Risiken für die Sicherheit der Datenverarbeitung und die Vertraulichkeit der dem Sozialgeheimnis unterliegenden Daten führen werden, wird zu prüfen sein. Spätestens für die Umsetzung des Gesamtprojektes sind diese Mängel aber keineswegs mehr akzeptabel, da sie nach dem heutigen Stand der Technik vermeidbar sind:

- Die *Aufstellungsräume der Server,* in denen auch die Datenträger gelagert werden sollen, erhalten keine besondere Zugangssicherung außer den auch sonst üblichen Schlüsselsystemen und dem Verzicht auf Hinweisschilder.
- Die *Verwaltung der Paßwörter* soll zunächst von den Systemverwaltern und erst zu einem späteren Zeitpunkt von den Benutzern selbst übernommen werden. Die vorläufige Regelung bleibt weit unter dem Stand der Technik und bedeutet, daß individuelle Paßwörter weiteren Personen bekannt sind und somit Vorgänge, die unter einer bestimmten Kennung ablaufen, nicht der Person eindeutig zugeordnet werden können, zu der die Kennung gehört. Alle programmierten Kontrollen (Führung einer Logdatei, Protokollierung von Paßwortänderungen und Fehlversuchen beim Einloggen etc.), die am System für Revisionszwecke durchgeführt werden, verlieren dadurch ihren Sinn.
- Zwar soll einerseits eine menugesteuerte Bedienerführung Bedienungsfehler und fahrlässige und vorsätzliche Fehlhandlungen verhindern, andererseits aber soll zumindest für lesende Zugriffe, also Auswertungen, eine *Datenbankabfragesprache* wie SQL nutzbar sein. Damit steht den Benutzern jedoch ein Instrument zur Verfügung, mit dem sich leicht und flexibel beliebige Auswertungen auf den Datenbeständen durchführen lassen, auch solche, die vom Erforderlichkeitsprinzip nicht rechtlich gedeckt sind. Normale Benutzer sind vom Zugang zur Datenbankabfragesprache auszuschließen und durch Menuführung auf die ihnen zukommenden Auswertungen zu beschränken. Ansonsten sind Auswertungen unter Verwendung der Datenbankabfragesprache ausführlich automatisch zu protokollieren.
- Die Übertragung von schutzwürdigen Daten über ein *öffentliches Datennetz* soll zwar protokolliert werden, Maßnahmen zur Transportkontrolle, etwa also die Verschlüsselung der Daten auf dem Übertragungsweg, sind ausdrücklich nicht vorgesehen.

4.6 Stadtentwicklung und Umweltschutz

Fragwürdige Rechtsgrundlagen für Umweltschutz und Stadtplanung

Die EG-Richtlinie über den freien Zugang zu Informationen über die Umwelt hätte bis zum 31. Dezember 1992 in deutsches Recht umgesetzt werden müssen. Der Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit hat dazu sehr spät einen Referentenentwurf eines *Umweltinformationsgesetzes* (UIG) vorgelegt. Nach der EG-Richtlinie muß es Zweck des geplanten Gesetzes sein, für jeden „den freien Zugang" zu Umweltinformationen zu gewährleisten. Dabei ist zu sichern, daß jedem auf Antrag „ohne Nachweis eines Interesses" Informationen über die Umwelt zur Verfügung gestellt werden. Mit diesem Referentenentwurf wird nur ein erster Schritt in Richtung auf eine allgemeine Informationsfreiheitsgesetzgebung getan, die leider in Berlin am Ende der vergangenen Legislaturperiode zunächst gescheitert ist.

Bislang enthält der Entwurf keine ausreichend konkreten Regelungen, die den tatsächlichen Zugang zu Umweltinformationen für jedermann ermöglichen, und unter welchen Ausnahmebedingungen dieser einzuschränken ist. Wir fordern vor allem eine Beratungspflicht der Behörden gegenüber den Antragstellern. Werden durch das Informationsbegehren dem Datenschutz unterliegende Daten berührt, so sollten dem Antragsteller Alternativen – z. B. Auskunftsrecht statt Einsichtsrecht – aufgezeigt werden. Die Beratung durch die Behörden sollte kostenfrei erfolgen. Werden durch ein Auskunftsbegehren schutzwürdige Interessen (beispielsweise Betriebs- und Geschäftsgeheimnisse) berührt, so sollten diese vom Verursacher innerhalb einer Frist gegenüber der Behörde dargelegt werden. In Anlehnung an § 22 Chemikaliengesetz ist eine Regelung erforderlich, die zu einer Offenbarung verpflichtet, wenn durch sie kein oder nur ein unwesentlicher wirtschaftlicher Schaden entstehen kann. Hingegen sollten personenbezogene Daten von Geschädigten und Informanten nur mit deren Einwilligung zugänglich gemacht werden dürfen. Da bis zum 31. Dezember 1992 der Gesetzgeber die EG-Richtlinie nicht umgesetzt hat, kommt ihr nunmehr unmittelbare Geltung zu. Für diese Übergangszeit hat die Senatsverwaltung für Stadtentwicklung und Umweltschutz in einem Rundschreiben Bearbeitungshinweise gegeben. Diese folgen nicht nur den halbherzigen Vorgaben des Bundesentwurfes, sondern schränken den Informationszugang noch darüber hinaus ein.

Auch wenn das Umweltinformationsgesetz des Bundes demnächst verabschiedet werden sollte, kann der Berliner Gesetzgeber nicht untätig bleiben. Da der Bund nur für bestimmte Bereiche, in denen Umweltinformationen anfallen (z. B. Immissionsschutzrecht, Atomrecht), die Gesetzgebungskompetenz hat, müssen die Länder umgehend den Informationszugang in allen übrigen Bereichen des Umweltrechts regeln, um die EG-Richtlinie umzusetzen. In Berlin liegen Vorentwürfe für ein Umweltaktenein sichtsgesetz sowie der in den Ausschüssen des Parlaments seinerzeit abschließend beratene Entwurf eines Informationsfreiheitsgesetzes[129] vor.

Auch zum Entwurf eines Berliner *Bodenschutzgesetzes* haben wir Stellung genommen. Durch das Festlegen einer Informationspflicht für Eigentümer und Nutzer sollen flächendeckende, grundstücksbezogene Aussagen über Bodenverunreinigungen und die Bodenqualität ermöglicht werden. Dabei sollen Grundlagen für automatisierte Dateien (ein *Bodenbelastungskataster,* eine *Bodenschadstoffdatenbank* und eine *flächendeckende Bodenzustandsdatenbank)* geschaffen werden. Insbesondere bei der flächendeckenden Zustandsdatenbank ist der Bezug zur Aufgabenerfüllung jedoch noch nicht eindeutig festgelegt. Dies wäre Datenspeicherung auf Vorrat ohne entsprechende Zweckbindung.

Unvereinbar mit dem informationellen Selbstbestimmungsrecht ist eine nicht näher definierte Übermittlungsverpflichtung anderer Behörden für Daten, die in deren Zuständigkeitsbereich erhoben, gespeichert und verarbeitet werden, sowie ein Abweichen vom Grundsatz, daß Daten in erster Linie beim Betroffenen mit seiner Kenntnis zu erheben sind. Die Erhebung von Daten beim Betroffenen ohne dessen Kenntnis durch verdeckte Beobachtung oder bei anderen öffentlichen Stellen ohne sein Wissen muß die präzise zu bestimmmende Ausnahme bleiben und sich auf die Gefahrenabwehr beschränken. Eine flächendeckende Erfassung von Bodenzustandsdaten für die Bodendatenbanken sollten grundsätzlich nur beim Betroffenen selbst mit seiner Kenntnis erfolgen. Der ursprüngliche Entwurf enthielt auch eine Vorschrift zur Durchsetzung der Auskunftspflicht des Betroffenen, die mit dem Grundrecht auf Unverletzlichkeit der Wohnung unvereinbar war. Zur Abwehr einer dringenden Gefahr durch eine Bodenverunreinigung die Geschäftsräume des Betroffenen gegen seinen Willen betreten zu dürfen, mag noch angehen. Bei der Erstellung von flächendeckenden Bodendatenbanken kann dagegen nicht von einer dringenden Gefahr gesprochen werden. Wenn Daten auf Grund bereits erfolgter Erhebungen in Boden-

[129] Drs. 11/958; vgl. dazu Jahresbericht 1990, 1.2

datenbanken gespeichert werden, so ist der Betroffene nachträglich zu benachrichtigen. Unzureichend ist auch die vorgesehene Regelung, inwieweit und für welche Zwecke Daten dieser drei Datenbanken miteinander verknüpft werden dürfen. Auch sollte präzise festgelegt werden, aus welchen Gründen der freie Zugang zu den Daten des künftigen Umweltinformationssystems eingeschränkt wird.

Mit der 7. Änderung des *Berliner Wassergesetzes*[130] wurde die Übermittlung von personenbezogenen Daten zwischen Wasserbehörde und Berliner Wasserbetrieben datenschutzrechtlich normenklar geregelt. Dabei geht es um die Übermittlung von Daten über *Direkteinleiter*. Die Datenübermittlung zum Aufbau des Altlastenkatasters ist im Rahmen des Artikelgesetzes durch eine weitere Ergänzung des Wassergesetzes[131] geregelt worden.

Fortgesetzt wurden im Jahr 1992 die Arbeiten an einem *Gesetz über die Datenverarbeitung für Zwecke der räumlichen Stadtentwicklung*. Auch hier soll der Aufbau einer flächendeckenden Stadtplanungsdatei mit Hilfe einer gesetzlichen Auskunftspflicht geregelt werden. Dies halten wir für unverhältnismäßig. Obwohl eine derartige Auskunftspflicht bislang nicht bestand, konnten offenbar die Stadtplanungsbehörden ihre Aufgaben erfüllen. Als bedenklich wird angesehen, daß - zur Durchsetzung der angestrebten Auskunftspflicht - auch hier das Grundrecht der Unverletzlichkeit der Wohnung z. B. bei Einfamilienhäusern eingeschränkt werden soll. Wenn es um die Erstellung von *Stadtplanungsdateien* geht, kann von einer dringenden Gefahr für die öffentliche Sicherheit und Ordnung nicht gesprochen werden. Jedoch nur unter dieser Voraussetzung kann Art. 13 Grundgesetz durch einfaches Gesetz eingeschränkt werden. Wohnungen sollten aus unserer Sicht auch künftig nur mit Zustimmung der Wohnungsinhaber betreten werden dürfen. Offen ist im Entwurf, ob mit der Stadtplanungsdatei ein automatisiertes Abruf- und Informationssystem geschaffen werden soll, an dem sich auch die Senatsverwaltung für Bau- und Wohnungswesen beteiligt. Die Arbeiten an diesem Gesetzentwurf sollten schnellstens abgeschlossen werden, zumal die im Artikelgesetz enthaltene Übergangsregelung im Ausführungsgesetz zum Baugesetzbuch[132] Ende 1993 außer Kraft tritt.

Die intelligente Mülltonne

Das Problem der ständig wachsenden Müllberge und der *Abfallentsorgung* zwingt dazu, daß die Abfälle möglichst frühzeitig - am besten schon durch den Verbraucher selbst, der den Abfall produziert, - sortiert und getrennt gesammelt werden. Systeme der getrennten Abfallsammlung können allerdings nur effektiv sein, wenn die Verbraucher den Abfall tatsächlich entsprechend getrennt sammeln. Ob sie dies tun, müßte - zumindest stichprobenartig - überwacht werden.

Wir haben bereits Eingaben erhalten, in denen sich Bürger darüber beschweren, daß Vermieter oder deren Beauftragte derartige Kontrollen durchführen. Die Mieter fühlen sich dadurch in ihrer Privatsphäre verletzt. Es läßt sich nicht bestreiten, daß durch entsprechende Überwachungsmaßnahmen die Privatsphäre eines Bürgers beeinträchtigt werden kann, dem ein bestimmter Müllbehälter zugewiesen ist.

Die *Berliner Stadtreinigung* hat im Berichtszeitraum einen *Modellversuch zur Müllgefäßidentifikation* begonnen, bei dem sie *„intelligente Mülltonnen"* einsetzt. In den Deckel dieser Mülltonnen sind Mikrochips integriert, die das Gewicht des Tonneninhalts registrieren und beim Entladen dieses Gewicht direkt auf einen Bordcomputer im Müllentsorgungsfahrzeug übertragen. Zugleich werden die Müllgefäße mit Hilfe der Mikrochips den einzelnen Kunden zugeordnet. Damit auch für den Bürger erkennbar ist, welches „seine" Mülltonne oder die seiner Hausgemeinschaft zugewiesene Mülltonne ist, sind die Tonnen jeweils mit Straße, Hausnummer und gegebenfalls dem Namen beschriftet. Auf diese Weise können die Abfallmengen gewichts- und grundstücksbezogen ermittelt werden und die Gebühren verursachergerecht errechnet werden. Dies dient mittelbar auch dem Ziel der Müllvermeidung. Allerdings kann mit Hilfe der intelligenten Mülltonne nicht überprüft werden, ob die Bewohner des Versuchsgebiets jeweils den richtigen Müll (Wertstoffe oder Restmüll) auch in die richtige Tonne gefüllt haben. Wird bei der Entleerung festgestellt, daß die Behälter falsch gefüllt sind, werden sie lediglich von einem herkömmlichen Müllfahrzeug abgeholt und entleert. Die intelligente Mülltonne kann also kein Verhaltensprofil des Bürgers bezüglich seiner „Abfallgewohnheiten" erstellen. Die Teilnehmer an dem einjährigen Modellversuch wurden von der BSR vorab über das Vorhaben informiert. Wir werden die Durchführung des Modellversuchs weiterhin begleiten und technisch überprüfen.

4.7 Wissenschaft und Forschung

Transparenz im Umgang mit Studentendaten

Im Rahmen des Artikelgesetzes wurde das *Berliner Hochschulgesetz* (BerlHG) um eine Rechtsgrundlage für die Erhebung und Verarbeitung von personenbezogenen Daten ergänzt (§ 6)[133]. Bislang war für keinen Studienbewerber, Studenten oder Prüfungskandidaten nachvollziehbar, auf welcher Grundlage und für welche Zwecke sie oder er seine Daten an den Hochschulen anzugeben hatte. Durch die Neufassung wird der Student zwar nicht aus dieser Pflicht entlassen, jedoch wird die Senatsverwaltung verpflichtet, durch Rechtsverordnung bis zum 31. Dezember 1993 die anzugebenden Daten und die Zwecke, für die sie verarbeitet werden dürfen, festzulegen. Im Rahmen dieser *Hochschuldaten-Verordnung* ist ein präziser und überschaubarer Katalog der zu erhebenden Daten, der datenverarbeitenden Stellen (z. B. Immatrikulationsbüro, Prüfungsämter) sowie der Übermittlungen und der Verwendungszwecke zu erstellen.

In diesem Zusammenhang ist auch zu regeln, welche Hochschuldaten für Zwecke der Hochschulstatistik nach dem *Hochschulstatistikgesetz* genutzt und an das Statistische Landesamt übermittelt werden. Ein erster Entwurf der Hochschuldaten-Verordnung wurde diesen Ansprüchen noch nicht gerecht. Ein Sonderproblem besteht darin, daß Daten nach dem Hochschulstatistikgesetz zu übermitteln sind, die für eigene Verwaltungszwecke der Hochschule nicht benötigt werden. Auch dies ist durch die Hochschuldaten-Verordnung abzudecken, da der Student bislang gegenüber der Hochschule nicht zur Auskunft verpflichtet werden kann. Die erforderliche Trennung von Statistik und Verwaltung gebietet, daß Stellen, in denen außerhalb der statistischen Ämter Bundesstatistiken ganz oder teilweise vorbereitet, erhoben oder aufbereitet werden, diesem Gebot nachzukommen haben. Die Wahrung des Statistikgeheimnisses ist gleichermaßen sicherzustellen wie bei statistischen Ämtern. Angaben, die nur für statistische Zwecke aufgeliefert wurden sowie Erkenntnisse, die aus statistischen Auswertungen gewonnen werden, dürfen nicht für andere Verfahren oder Zwecke verwandt werden. Für die Hochschulstatistik als Sekundärstatistik bedeutet dies, daß die Abschottung der Datenverarbeitung nur gesichert ist, wenn eine strikte Trennung von Dateien der Studenten- und Prüfungsverwaltung einerseits und der aus diesen Quellen gespeisten Dateien der Hochschulstatistik andererseits vorgenommen wird.

Durch die Neufassung des § 6 BerlHG wurden auch die Befugnisse zur Übermittlung von Daten an das Studentenwerk, die Rechte der Frauenbeauftragten bei der Einsicht in Personalunterlagen, die Datenübermittlungen von Prüfungsämtern an die Studienabteilungen bzw. Immatrikulationsbüros sowie die Verarbeitung personenbezogener Daten durch Hochschuleinrichtungen wie Bibliotheken geregelt. Ein Vergleich der gegenwärtig vorhandenen Strukturen bei der Verarbeitung personenbezogener *Studentendaten* zeigt, daß es zwischen den einzelnen Hochschulen historisch gewachsene Unterschiede gibt. Dem wird dadurch Rechnung getragen, daß der neue § 6 BerlHG die Hochschulen ermächtigt, durch *Satzung* die Befugnisse zur Verarbeitung weiterer personenbezogener Daten zu schaffen, soweit dies für Forschung und Lehre sowie für die Datenübermittlung nach dem Hochschulstatistikgesetz erforderlich ist.

130 GVBl. 1992, S. 472
131 GVBl. 1993, S. 47
132 GVBl. 1993, S. 52
133 GVBl. 1993, S. 45

Unterschiede bestehen jedoch nicht nur zwischen den Hochschulen, sondern auch zwischen den *Fachbereichen* der einzelnen Hochschulen selbst. In einigen Fachbereichen sind bestimmte Studienverwaltungsfunktionen unmittelbar auf der Fachbereichsebene angesiedelt, in anderen wiederum werden diese Aufgaben auf Institutsebene erledigt. Mit der Hochschuldaten-Verordnung sollte die Möglichkeit gegeben werden, durch die Hochschulen im Einzelfall festzulegen, welche Ebene (Fachbereich *oder* Institut) die Befugnis zur Verarbeitung von Studentendaten zur Sicherung des Hochschulbetriebes übertragen bekommt. Der Datenumfang ist jedoch eindeutig festzuschreiben.

Studenten beurteilen Lehrkräfte

Im Jahr 1992 wurden an allen drei Berliner Universitäten Befragungen von Studenten durchgeführt, bei denen die Lehrveranstaltungen sowie die Dozenten zu beurteilen waren. Mit dem neu gefaßten § 6 BerlHG wird jetzt den Hochschulen die Möglichkeit eröffnet, diese Befragung zur *Evaluation der Lehre*[134] in allen Fachbereichen durchzuführen sowie die Ergebnisse öffentlich zu erörtern. Bislang war dies nur auf freiwilliger Grundlage möglich. Der bewertete Dozent konnte einer Veröffentlichung dieser Ergebnisse widersprechen. Das Ergebnis war zunächst den Lehrenden zuzuleiten, bevor es die Dekane oder geschäftsführenden Direktoren zu einer möglichen Veröffentlichung erhielten.

An der Technischen Universität hatten eine Reihe evaluierter studentischer Beschäftigter (Tutoren) parallel zum von der Universitätsleitung vorgesehenen Zustimmungsverfahren (durch Ablauf einer Widerspruchsfrist) eine gesonderte Erklärung übergeben, in der eine Veröffentlichung von Ergebnissen erst nach ausdrücklicher Zustimmung der Betroffenen verlangt wurde. Diese Erklärung wurde vom Präsidialamt der Technischen Universität ignoriert. Eine Überprüfung ergab, daß diese Erklärungen in teilweise ungeöffneten Umschlägen in einem Karton gesammelt und abgelegt wurden.

Diese rechtswidrige Vorgehensweise wurde von uns bemängelt. Prinzipiell gilt, daß bei freiwilligen Erhebungen die Betroffenen jederzeit - unabhängig vom technischen Verfahren - der weiteren Verarbeitung ihrer Daten widersprechen bzw. diese von ihrer erneuten Zustimmung abhängig machen können.

Studentenakten mit Vergangenheit

Der Umgang mit Studentenakten von heute noch studierenden Studenten, die schon zu DDR-Zeiten immatrikuliert wurden, macht ein besonderes Verfahren erforderlich. Solche Akten sind leicht an ihrem Umfang zu erkennen. Sie sind gefüllt mit Fragebögen, Lebensläufen, Beurteilungen aus DDR-Zeiten, die durch ihre heute kaum noch zu deutenden Aussagen keinem Studenten zum Vorteil gereichen.

Für das Vorhalten dieser Angaben in den Studentenakten bestehen gegenwärtig weder eine gesetzliche Grundlage noch ein Erfordernis zur Erfüllung der gesetzlich zugewiesenen Aufgaben. Ein datenschutzgerechter Umgang mit diesen Akten ist nur gewährleistet, wenn die Akten dieser Studenten geteilt werden. Es wäre eine Akte zu erstellen, die für das heutige Studium relevant ist und den normalen Zulassungs- bzw. Prüfungsbedingungen entspricht. Eine zweite Akte beinhaltet den Teil der Unterlagen, der aus DDR-Zeiten stammt und heute nicht mehr erforderlich ist. Dieser zweite Teil ist als „gesperrt" gesondert zu kennzeichnen und dem jeweiligen *Hochschularchiv* bis zur endgültigen Regelung - beispielsweise durch ein Landesarchivgesetz oder eine universitäre Satzung - zu übergeben. Natürlich haben die betroffenen Studenten selbst auch bei Sperrung das Recht, in diesen zweiten Teil der Akte einzusehen - einschließlich der Möglichkeit, Kopien zu erstellen. Jede darüber hinausgehende Nutzung ist unzulässig. Auch eine wissenschaftliche Aufbereitung von Altakten unter Hinweis auf das Forschungsprivileg nach § 30 BlnDSG wäre ohne Einwilligung des Betroffenen nicht zu rechtfertigen. Wir haben daher empfohlen, nach und nach diese Trennung vorzunehmen und den nicht mehr benötigten Teil der Altakte mit einem Sperrvermerk an das Archiv weiterzuleiten.

[134] vgl. Jahresbericht 1991, 3.11

Das Wissenschaftsprivileg - kein Freibrief

Ein Wissenschaftler möchte im Rahmen eines Forschungsvorhabens die Absolventen vergangener Jahre eines Fachbereiches befragen. Dazu werden die Adressen der Absolventen benötigt, also - nichts leichter als die letzten der Hochschule vorliegenden Adressen abfordern. Der betreffende Fachbereich befürwortet dieses Vorhaben, bittet die oberste Landesbehörde um Zustimmung zur Übermittlung dieser Daten ohne Einwilligung der Betroffenen. Die Senatsverwaltung stimmt zu und informiert den Berliner Datenschutzbeauftragten.

Wir halten hier die Anwendung des Wissenschaftsprivilegs, das einen erheblichen Eingriff in die Rechte der Betroffenen darstellt, für unangemessen. Mit der Wissenschaftsklausel (§ 30 BlnDSG) wurde eine *ausnahmsweise* Möglichkeit zur Datenoffenbarung ohne Einwilligung des Betroffenen geschaffen. Diese Ausnahme ist nur gerechtfertigt, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen *erheblich überwiegt* und der Zweck der Forschung nicht auf andere Weise erreicht werden kann. Ein einfaches wissenschaftliches Interesse an der Durchführung eines Forschungsvorhabens kann damit gegenüber dem Geheimhaltungsinteresse eines jeden Betroffenen keinen Vorrang haben. Bei sensibleren Daten muß dem Geheimhaltungsinteresse ein überragendes Gemeinschaftsinteresse gegenüberstehen, um eine Verarbeitung ohne Einwilligung des Betroffenen zu rechtfertigen. Bei Prüfungsarbeiten (auch Dissertationen) liegt in der Regel kein überwiegendes, geschweige denn ein erheblich überwiegendes wissenschaftliches Interesse, das als öffentliches Interesse aufgefaßt werden kann, vor.

Im vorliegenden Fall ging es zwar „nur" um Adressen. Aber dafür gibt es das *Adreßmittlungsverfahren.* Beim Adreßmittlungsverfahren, das datenschutzrechtlich unbedenklich ist, wird vermieden, daß die Adressen der Betroffenen Dritten zur Kenntnis gelangen. Dabei werden den Bildungseinrichtungen von den Wissenschaftlern frankierte, aber nicht adressierte Umschläge sowie das zu versendende Material übergeben. Die Bildungseinrichtung adressiert die Umschläge auf Grund der ihr vorliegenden Adressen und übergibt sie dem Postweg. Der einzelne Angeschriebene muß in dem Begleitschreiben über dieses Verfahren aufgeklärt werden, damit er sichergehen kann, daß seine persönlichen Angaben nicht an Dritte weitergegeben wurde. Der Angeschriebene kann damit frei entscheiden, ob er antwortet oder nicht. Nach anfänglicher Weigerung unter (falschem) Hinweis auf die Portokosten wurde nach unserem Vorschlag verfahren.

5. Medien und Telekommunikation

Der Berliner Datenschutzbeauftragte hat die Sicherung des Rechts auf informationelle Selbstbestimmung im Bereich der Medien und der Telekommunikation stets als einen Schwerpunkt seiner Tätigkeit verstanden. In diesen Bereichen wird das Grundrecht auf Datenschutz durch die schnelle technische Entwicklung ständig neuen Gefährdungen ausgesetzt, denen mit den vorhandenen rechtlichen Regelungen nur unvollkommen zu begegnen ist. Diesen Problemen haben wir auch im Berichtszeitraum sowohl in Berlin (5.1) als auch in Deutschland und Europa (5.2) sowie schließlich weltweit (5.3) besondere Aufmerksamkeit gewidmet. Der Berliner Datenschutzbeauftragte hat dabei als Vorsitzender des Arbeitskreises Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Telekommunikation und Medien der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre zugleich auf mehreren Ebenen die Funktion, das Expertenwissen zu bündeln.

5.1 Berlin

Der neue *Staatsvertrag über die Zusammenarbeit zwischen Berlin und Brandenburg im Bereich des Rundfunks*[135] ersetzt seit seinem Inkrafttreten am 7. Mai 1992 das *Kabel-Pilotprojekt-Gesetz* (KPPG). Der hohe datenschutzrechtliche Standard des KPPG

[135] GVBl. 1992, S. 150 ff.

wurde auch in § 58 des Staatsvertrages festgeschrieben. Lediglich die Berichtspflicht des Berliner Datenschutzbeauftragten nach § 55 Abs. 1 KPPG ist nicht in den Staatsvertrag übernommen worden. Auch ohne eine entsprechende Verpflichtung wird der Datenschutzbeauftragte weiterhin dem Abgeordnetenhaus von Berlin über Mängel, die er in diesem Bereich festgestellt hat, und über seine Vorschläge zu ihrer Behebung und zur Verbesserung des Datenschutzes berichten. Im vergangenen Jahr haben wir in diesem Bereich keine Mängel festgestellt.

Polizeifunk kann abgehört werden – auch ein Datenschutzproblem

Das *Fernmeldegeheimnis* wird durch neue Entwicklungen zusätzlich gefährdet. Bisher benutzten Polizei, Feuerwehr und Rettungsdienste (z. B. das Rote Kreuz) für ihre Funkkommunikation Frequenzbereiche, die mit privaten Rundfunkempfängern nicht empfangen werden durften. Der Bundesminister für Post- und Telekommunikation hat mit Wirkung vom 30. Juni 1992 die Beschränkung der zulässigen Empfangsfrequenzbereiche für Rundfunkempfänger aufgehoben, so daß künftig auch solche Rundfunkempfänger betrieben werden dürfen, die technisch das Abhören des Funkverkehrs der Polizei, der Feuerwehr, des Zolls, der Rettungsdienste, des Taxifunks, aber auch die mit schnurlosen Telefonen und mit Autotelefonen (B- und C-Netz) geführten Telefongespräche ermöglicht. Das Betreiben solcher Rundfunkempfänger, die bereits im Handel erhältlich sind, ist seitdem nicht mehr strafbar.

Dies bedeutet für die öffentlichen Stellen Berlins, die sich der Funkkommunikation bedienen, also vor allem für die Polizei und die Feuerwehr, daß sie technische und organisatorische Maßnahmen zu treffen haben, um dem erhöhten Risiko des unbefugten Mithörens zu begegnen. Jede datenverarbeitende Stelle, die Funkgeräte zur Datenübermittlung nutzt, ist für die Transportkontrolle bei der Übermittlung personenbezogener Daten im Sinne des § 5 Abs. 3 Nr. 9 BlnDSG verantwortlich. Ergänzende technische und organisatorische Maßnahmen zur Sicherung dieser Transportkontrolle durch Verschlüsselung der personenbezogenen Daten vor ihrer Übermittlung sind geboten. Die Antwort von Polizei und Feuerwehr auf unsere Aufforderung, solche Maßnahmen unverzüglich zu treffen, steht noch aus. Die Konferenz der Innenminister und -Senatoren der Länder hat am 20. November 1992 mit Besorgnis festgestellt, daß die Aufhebung der Beschränkung von Funkfrequenzen erheblich in Belange der öffentlichen Sicherheit eingreift, und den Bundesminister für Post- und Telekommunikation zur Wiedereinführung der Funkfrequenzbeschränkungen aufgefordert. Dies erscheint allerdings auf Grund der gebotenen Liberalisierung des Warenverkehrs im EG-Binnenmarkt als unwahrscheinlich. Eine datenschutzgerechte Lösung des Problems liegt allein in der Verschlüsselung des Sprechfunkverkehrs.

5.2 Deutschland und Europa

Datenschutz in der Telekommunikation – noch immer nicht realisiert

In die schon im Juli 1991 in Kraft getretene TELEKOM-Datenschutzverordnung (TDSV) und die seit Ende 1991 geltende Teledienstunternehmen-Datenschutzverordnung (UDSV) wurden auf Grund der Kritik der Datenschutzbeauftragten bestimmte Rechte der Telefonkunden aufgenommen[136]. Das wichtigste dieser Rechte ist das Wahlrecht des Kunden bei digitalen Sprachkommunikationsdiensten, das es dem Kunden ermöglicht, die Verbindungsdaten nach seiner Wahl entweder mit der Versendung der Entgeltrechnung vollständig löschen zu lassen, unter *Verkürzung der Zielrufnummer* um die letzten drei Ziffern speichern oder vollständig speichern zu lassen, wenn ein Einzelentgeltnachweis beantragt ist. Außerdem muß die TELEKOM die Anonymität der telefonischen Beratung bei der Erstellung von Einzelentgeltnachweisen sicherstellen, wenn die betroffenen Stellen dies beantragt haben[137]. Diese beiden – ohnehin kaum praktikablen – Regelungen sollten aber für das digitale Festnetz erst in Kraft treten, sobald die zu ihrer Durchführung erforderlichen Datenverarbeitungsprogramme verfügbar sind, spätestens am 1. Juli 1992 (§ 16 Abs. 2 Satz 1 TDSV). Für das digitale Mobilfunknetz gilt dies ausschließlich für das Wahlrecht des Telefonkunden bei der *Verbindungsdatenspeicherung* (§ 16 Abs. 2 Satz 1 UDSV).

Bereits im Frühjahr 1992 erklärte die TELEKOM, sie werde nicht in der Lage sein, die erforderlichen Datenverarbeitungsprogramme für die Rechte der Telefonkunden bis zum 1. Juli 1992 zur Verfügung zu stellen. Daraufhin legte der Bundesminister für Post- und Telekommunikation den Entwurf einer ersten Änderungsverordnung zur TDSV vor, der unter anderem vorsah, daß die Übergangsfrist in der TDSV um ein Jahr verlängert werden sollte und die TELEKOM die Befugnis erhalten sollte, in der Übergangszeit in digitalen Sprachkommunikationsdiensten und bei Verwendung von Kundenkarten Verbindungsdaten bis Ende 1992 vollständig, ab dem 1. Januar 1993 lediglich unter Verkürzung der Zielrufnummer um die letzten drei Ziffern zu speichern.

Bei einer Verwirklichung dieses Vorschlags wäre das Recht des Telefonkunden mit einem Festanschluß, die Verbindungsdaten nach Versendung der Entgeltrechnung vollständig löschen zu lassen, für ein weiteres Jahr suspendiert worden. Das Unvermögen der TELEKOM, die erforderlichen Datenverarbeitungsprogramme zur Verfügung zu stellen, wäre zu Lasten des informationellen Selbstbestimmungsrechts dieser Telefonkunden gegangen. Deshalb haben wir die Vertreter des Landes Berlin im Infrastrukturrat gebeten, dem Verordnungsentwurf nicht zuzustimmen. Vielmehr hätte die TELEKOM verpflichtet werden müssen, die Verbindungsdaten spätestens mit Versendung der Entgeltrechnung stets vollständig zu löschen, solange sie technisch nicht sicherstellen kann, daß der Kunde die Teil- oder Vollspeicherung dieser Daten ausschließen kann.

Vor dem Hintergrund des wenig später bekannt gewordenen Fangschaltungsbeschlusses des Bundesverfassungsgerichts vom 25. März 1992[138] hat der Bundesminister für Post- und Telekommunikation sein Vorhaben, die Übergangsfrist in der TDSV zu Lasten des Kunden zu verlängern, aufgegeben. Die Bundesregierung hat inzwischen erklärt, daß aus dem Beschluß des Bundesverfassungsgerichts auch Konsequenzen für die gesamte Verbindungsdatenspeicherung gezogen werden müssen.

Der Fangschaltungsbeschluß

Das Bundesverfassungsgericht hat festgestellt, daß das Fernmeldegeheimnis entgegen der Auffassung des Bundesministers für Post und Telekommunikation keine „immanenten Schranken" auf Grund betrieblicher Erfordernisse kennt. Jede Kenntnisnahme, Aufzeichnung und Verwertung von kommunikativen Daten durch die Deutsche Bundespost TELEKOM oder andere staatliche Stellen ist ein Eingriff in dieses Grundrecht. Dieser Eingriff scheidet auch nicht deswegen aus, weil das Fernmeldegeheimnis nicht zwischen den Gespächsteilnehmern gilt. Zwar dürfe jeder Fernsprechteilnehmer ohne Grundrechtsverstoß Dritte von seinen Telefongesprächen unterrichten. Daraus folge aber nicht, daß ein Fernsprechteilnehmer mit Wirkung für den anderen auch gegenüber der Deutschen Bundespost TELEKOM auf die Wahrung des Fernmeldegeheimnisses verzichten kann. Wörtlich führt das Bundesverfassungsgericht aus: „Wenn der Zweck des Fernmeldegeheimnisses darin liegt, Kommunikationsvorgänge und -inhalte gegen staatliche Zugriffe abzuschirmen, ist jede staatliche Einschaltung, die nicht im Einverständnis mit beiden Kommunikationspartnern erfolgt, Grundrechtseingriff."

Im konkreten Fall hat das Bundesverfassungsgericht auf seine Rechtsprechung zum Übergangsbonus verwiesen und die Einrichtung von *Zählervergleichseinrichtungen* und Fangschaltungen trotz fehlender gesetzlicher Grundlage vorübergehend hingenommen, um eine Lage zu verhindern, die den verfassungsrechtlichen Anforderungen noch ferner stünde als der bisherige Zustand. Es hat betont, daß ein Gesetz, welches Gesprächsbeobachtungen zur Abwehr bedrohender oder belästigender anonymer Anrufer erlaubte, bei angemessenem Ausgleich der betreffenden Grundrechte hinreichenden verfahrensrechtlichen Vorkehrungen und wirksamer Mißbrauchssicherung verfassungsmäßig wäre.

136 vgl. Jahresbericht 1991, 2.3
137 vgl. dazu ausführlich Jahresbericht 1991, 2.3
138 siehe unten

Diese Entscheidung zwingt den Gesetzgeber, nicht nur die Voraussetzungen einer Fangschaltung, sondern jede Speicherung von Verbindungsdaten durch die TELEKOM und private Netzbetreiber unverzüglich durch formelles Bundesgesetz bis zum Ende der Legislaturperiode zu regeln. Dabei kann sich der Gesetzgeber nicht damit begnügen, lediglich eine Verordnungsermächtigung in das Postverfassungsgesetz und das Fernmeldeanlagengesetz aufzunehmen. Das Gesetz selbst sollte darüber hinaus jedenfalls grundlegende inhaltliche Festlegungen dazu enthalten, in welchem Umfang die Netzbetreiber und Diensteanbieter personenbezogene Daten ihrer Kunden verarbeiten dürfen. Die anzustrebende Regelung sollte von dem Grundsatz ausgehen, daß die Verbindungsdaten nach dem Ende der Verbindung insgesamt zu löschen sind. Die Gebühren sollten in der jeweiligen Ortsvermittlungsstelle errechnet werden. Von dieser Verfahrensweise darf nur abgewichen werden, wenn der Kunde einen Einzelentgeltnachweis beantragt, auf dem seinerseits nur um mindestens vier Stellen verkürzte Zielrufnummern ausgewiesen sein dürfen. Neben einer deutlichen Einschränkung des Umfangs der Verbindungsdatenspeicherung würde damit das Regel-Ausnahme-Verhältnis des bisherigen § 6 TDSV/UDSV umgekehrt.

Die anzustrebende gesetzliche Regelung der Datenverarbeitung in einem *Bundestelekommunikationsgesetz* müßte auch einheitliche Verarbeitungsregeln für die Sprachkommunikation und sonstige Dienste (z. B. Telefax, Telebox etc.) enthalten. Die Unterscheidung zwischen der Sprachkommunikation und sonstigen Diensten in TDSV und UDSV kann vor dem Hintergrund der technischen Entwicklung nicht mehr aufrechterhalten werden.

Schließlich würde die vorgeschlagene Neuregelung auch einen wirksameren Schutz von *Beratungseinrichtungen* gewährleisten, die selbst oder deren Mitarbeiter besonderen Verschwiegenheitsverpflichtungen unterliegen. Daß die bisherige Regelung in § 6 Abs. 9 TDSV nicht praktikabel ist, zeigt sich daran, daß die TELEKOM bisher nicht in der Lage war, entsprechende Datenverarbeitungsprogramme bereitzustellen.

Nach dem Fangschaltungsbeschluß des Bundesverfassungsgerichts kann auch kein Zweifel mehr daran bestehen, daß *§ 12 Fernmeldeanlagengesetz,* der eine Auskunftserteilung über Verbindungsdaten für jedes beliebige Strafverfahren zuläßt, im Zuge der Digitalisierung der öffentlichen Telekommunikationsnetze verfassungswidrig geworden ist[139]. Seine Streichung ist deshalb vordringlich.

Für den gegenwärtigen Rechtszustand ist festzustellen, daß die *Speicherung von Verbindungsdaten* in öffentlichen und privaten Telefonnetzen (Festnetz- und Mobilfunknetze) derzeit ohne die erforderliche gesetzliche Grundlage erfolgt. Der im Fangschaltungsbeschluß als Rechtfertigung genannte Übergangsbonus greift hier nicht ein, da die Verbindungsdatenspeicherung - im Gegensatz zu einer Fangschaltung bei anonymer Bedrohung - nicht zum Schutz des Grundrechts auf körperliche Unversehrtheit eines Telefonkunden erforderlich ist. Verbindungsdaten dürften deshalb allenfalls auf der Grundlage der Einwilligung des Telefonkunden bis zur Versendung der Entgeltrechnung gespeichert werden. Anschließend müssen sie bereits jetzt vollständig gelöscht werden, wenn der Kunde nicht einen Einzelentgeltnachweis beantragt hat oder sich für die Speicherung der Zielrufnummern ohne die letzten drei Ziffern entschieden hat.

Der Fangschaltungsbeschluß des Bundesverfassungsgerichts läßt die übrigen Rechte der Telefonkunden aus der TDSV und UDSV unberührt. Die Kunden können nach wie vor der *Eintragung ins Telefonbuch* ohne Begründung und ohne zusätzliche Kosten widersprechen. Sie können außerdem der Nutzung ihrer Bestandsdaten zu Beratungs-, Werbungs- und Marktforschungszwecken durch die Deutsche Bundespost TELEKOM und durch Dritte widersprechen. Allerdings hat die TELEKOM im Berichtszeitraum die Kunden noch immer nicht hinreichend auf ihre Rechte hingewiesen.

Die TELEKOM beharrt auch nach wie vor darauf, daß der Kunde kein Recht zum Widerspruch gegen die Aufnahme seiner Daten in *elektronische Teilnehmerverzeichnisse* (CD-ROMs) hat und sie ihn hierauf auch nicht hinzuweisen braucht[140]. Jeder Kunde, der verhindern will, daß seine im Telefonbuch enthaltenen Daten entweder direkt von der TELEKOM auf elektronischen Datenträgern vermarktet oder von Dritten über Belegleser (Scanner) in Rechner eingelesen und anschließend auf solchen Datenträgern gespeichert und für eine Vielzahl unkontrollierbarer Zwecke genutzt werden, sollte dem Telefonbucheintrag deshalb insgesamt widersprechen. Eine Begründung ist dafür nicht erforderlich.

Seit Juli 1992 bieten die Deutsche Bundespost TELEKOM und die Mannesmann-Mobilfunk GmbH zwei konkurrierende *Mobilfunknetze* (D 1 und D 2) an. In den beiden D-Netzen kann man bereits in das europäische Ausland (Schweiz, Dänemark, Schweden und Finnland) telefonieren. Sinkende Preise für Mobiltelefone und ständig handlicher werdende Telefonapparate, im Fachjargon „Handies" oder „Porties", werden Mobiltelefone in naher Zukunft zu einem Massenartikel machen. Dabei hat der Wettbewerb zwischen den beiden Betreibern der D-Netze noch nicht dazu geführt, daß dem Kunden auch eine möglichst datenschutzgerechte Technik angeboten wird. Es verfestigt sich im Gegenteil der Eindruck, daß aus Kostengründen etwa der Betreiber des D 2-Netzes schon jetzt Einzelentgeltnachweise anbietet, ohne die datenschutzrechtlichen Vorkehrungen der UDSV zu berücksichtigen. Während die Datenschutzbeauftragten gehofft hatten, daß bei zwei konkurrierenden Netzbetreibern dem Kunden zumindest als eine Option auch ein „Mehr" an Datenschutz angeboten würde, als der rechtliche Mindeststandard es vorschreibt, scheint es inzwischen so, als führe der Wettbewerb zu einer Unterschreitung dieses Mindeststandards.

Die aggressive Vermarktung des Mobilfunks streicht immer wieder den Wert der ständigen Erreichbarkeit heraus. Vor dem Hintergrund der informationellen Selbstbestimmung ist allerdings zu fragen, ob *Erreichbarkeit* damit nicht zum Fetisch gemacht wird. Dem läßt sich nicht entgegenhalten, jeder könne frei entscheiden, ob er ein solches Gerät benutzt oder nicht. Insbesondere Arbeitnehmer riskieren ihren Arbeitsplatz, wenn ihr Arbeitgeber sie mit einem Mobiltelefon ausrüstet und ihnen vorschreibt, dies stets empfangsbereit zu halten[141]. Wenn Kommunikation zur Pflicht wird, ist auch die informationelle Selbstbestimmung in Gefahr.

Auf *europäischer Ebene* sind die Bemühungen für eine *Datenschutzrichtlinie für digitale Telekommunikationsnetze* im Berichtszeitraum praktisch nicht vorangekommen.

Im Gegensatz zur allgemeinen Datenschutzrichtlinie hat die EG-Kommission ihren gleichzeitig beschlossenen Vorschlag für eine Richtlinie zum Datenschutz in digitalen Kommunikationsnetzen[142] bisher nicht überarbeitet, obwohl das Europäische Parlament auch zu diesem Vorschlag Stellung genommen hat. Damit ist der notwendige Zusammenhang zwischen der allgemeinen Datenschutzrichtlinie und der ersten bereichsspezifischen Datenschutzrichtlinie vorerst aufgehoben und die Verwirklichung eines einheitlichen europäischen Telekommunikations-Binnenmarktes erschwert worden. Die Gründe hierfür liegen zum einen in dem anhaltenden Widerstand der nationalen Telekommunikationsorganisationen (insbesondere der Deutschen Bundespost TELEKOM), zum anderen könnte dem ein verfehltes Verständnis des Subsidiaritätsprinzips zugrundeliegen. Dieser Grundsatz, der im Zusammenhang mit der öffentlichen Diskussion über den *Europäischen Unionsvertrag von Maastricht* eine zunehmende Rolle spielt, würde mißverstanden, wenn die Gemeinschaft in Zukunft in so wesentlichen Bereichen wie dem der Telekommunikation dem nationalen Gesetzgeber wieder den Vorrang einräumen und auf Harmonisierung verzichten würde. Schon das Regelungsinstrument der Richtlinie ist ihrer Art nach Ausdruck des Subsidiaritätsprinzips, weil sie den Mitgliedstaaten die Wahl der Mittel überläßt, mit denen die Ziele der jeweiligen Richtlinie innerstaatlich umzusetzen sind[143].

---

139 vgl. Jahresbericht 1991, 2.3, S. 46

140 vgl. hierzu Jahresbericht 1991, 2.3

141 vgl. Urteil des OLG Graz v. 7. 3. 1990. Entsprechende Urteile der deutschen Arbeitsgerichte sind bisher nicht bekannt

142 vgl. Jahresbericht 1991

143 vgl. Art. 189 EWGV

Der Vertrag von Maastricht hebt darüber hinaus die Bedeutung transeuropäischer Netze im Bereich der Verkehrsplanung, der Energieversorgung der Telekommunikation hervor.

5.3 Weltweite Telekommunikation per Satellit

Telekommunikation erfolgt bereits jetzt häufig mit Hilfe von *künstlichen Satelliten.* Vor allem interkontinentale Telefongespräche werden zunehmend über geostationäre Fernmeldesatelliten abgewickelt. Für die Mitte der 90er Jahre plant ein Computerhersteller den Aufbau eines satellitengestützten weltweiten Mobilfunknetzes, bei dem 77 niedrig fliegende erdnahe Satelliten die jederzeitige Erreichbarkeit jedes Netzteilnehmers sicherstellen soll („Iridium"-Projekt, so genannt nach dem von 77 Elektronen umkreisten Iridium-Atom).

Herkömmliche *Fernmeldesatelliten,* die sich synchron zur Erdoberfläche bewegen, also von der Erde aus gesehen scheinbar fest in der Atmosphäre stehen, strahlen die Verbindungsdaten, die von Erdfunkstationen zu ihnen hinaufgefunkt werden, auf einer anderen Frequenz sofort wieder zu einer anderen Erdfunkstation ab. Es gibt aber auch andere, modernere Satellitentypen *(„Postboten- Satelliten"),* die Daten für eine gewisse Zeit speichern und sie von einem Punkt der Erdatmosphäre zu einem anderen transportieren, um sie dort wieder abzustrahlen. In beiden Fällen findet die Datenverarbeitung im Weltall oder auf dem Umweg über das All statt. Nationales Datenschutzrecht kann auf diese Weise ebenso umgangen werden wie regionales (z. B. EG-weit geltendes) Datenschutzrecht[144]. Hier sind dringend weltweite völkerrechtliche Vereinbarungen notwendig, um die Rechte des Einzelnen effektiv zu schützen[145].

Satelliten können auch noch zu anderen als Fernmeldezwecken eingesetzt werden. Der wichtigste Einsatzbereich ist die Verteilung von Fernsehprogrammen. Solange diese nicht interaktiv (etwa bei *Pay-TV)* erfolgt, werden keine personenbezogenen Daten verarbeitet. Stärker ins Visier gerät der Einzelne allerdings bei anderen Einsatzbereichen von Satelliten, nämlich der weltweiten

- Positionsbestimmung *(Fernortung),*
- beim *Fernmessen* und *Fernwirken* sowie
- bei der *Fernerkundung*[146].

Bereits seit längerem navigieren Schiffe mit Hilfe von Satelliten und können Reedereien die Positionen ihrer Schiffe feststellen. Aber nicht nur zu Wasser, sondern auch zu Lande findet dieses *Flottenmanagement* statt. Neuerdings werden LKW-Flotten satellitengestützt dirigiert, bei denen jedes Fahrzeug mit einem kleinen Satellitenempfänger ausgerüstet ist, mit dessen Hilfe die Position des Fahrzeugs (bei Kühlwagen auch die Temperatur im Kühlraum) festgestellt und kontrolliert werden kann. Zugleich können dem Fahrer alternative Routenempfehlungen gegeben werden, damit er schneller an sein Ziel kommt. Dies hat zweifellos Vorteile für alle Beteiligten, es führt aber zugleich zur Erstellung von *Bewegungsprofilen der LKW-Fahrer.* Mit Hilfe von Satelliten will die Autoindustrie demnächst auch den Standort von gestohlenen Fahrzeugen ermitteln können. Auch dies wäre zweifellos ein erheblicher Vorteil für den Bestohlenen. Gleichzeitig muß aber die Frage gestellt werden, wie verhindert werden kann, daß hier eine generelle Überwachung der Bewegung von einzelnen (auch nicht gestohlenen) Fahrzeugen stattfindet. Es wird nicht mehr lange dauern, bis man mit Hilfe eines Satelliten aus dem Weltall die Schlagzeile einer Zeitung lesen kann, die jemand an einer Bushaltestelle liest. Dieses Beispiel verdeutlicht die zunehmende Sehschärfe von Fernerkennungssatelliten.

Die Satellitentechnologie wirft also Fragen auf, die die herkömmliche Struktur des nationalen Datenschutzrechts sprengen. In kleinerem Rahmen stellen sich nach der Aufhebung der Genehmigungspflicht für *Luftbildaufnahmen* ähnliche Fragen auch bei der Herstellung von Luftaufnahmen vom Stadtgebiet[147].

144 vgl. dazu das Grünbuch der EG-Kommission zur Satellitenkommunikation, KOM (90) 490 endg. S. 105
145 vgl. Anlage 3
146 vgl. dazu im einzelnen Anlage 3
147 vgl. dazu die Antwort des Senats auf die Kleine Anfrage Nr. 2709 der Abgeordneten Gloatz vom 25. 8. 1992, LPD vom 15. 10. 1992, S. 6

6. Datenschutz auf dem Weg durch die Institutionen

6.1 Das neue Berliner Datenschutzgesetz

Während des gesamten Berichtszeitraumes galt das neue Berliner Datenschutzgesetz noch mit der Einschränkung, daß diejenigen Verfahren zur Verarbeitung personenbezogener Daten, die bei Inkrafttreten des Gesetzes bereits angewandt wurden, in dem Umfang fortgeführt werden durften, als dies zur rechtmäßigen Aufgabenerfüllung der datenverarbeitenden Stelle erforderlich war. Damit galt praktisch der Rechtszustand nach dem alten Berliner Datenschutzgesetz für diese Verfahren während der Übergangszeit fort, so daß die strengen Voraussetzungen des § 6 BlnDSG, wonach jede Datenverarbeitung nur auf Grund einer besonderen Rechtsvorschrift oder mit der Einwilligung des Betroffenen zulässig ist, suspendiert waren.

Immer wieder versuchten einzelne Verwaltungen, die Übergangsvorschrift des neuen Berliner Datenschutzgesetzes, die eine Datenverarbeitung nach altem Recht zuließ, möglichst weit auszulegen und auch auf Verfahren anzuwenden, die zwar bei Inkrafttreten des neuen Gesetzes noch nicht existierten, aber durch die Vereinigung der Stadt erforderlich geworden waren. In den meisten Fällen konnten praktikable Lösungen erzielt werden.

Von Anfang an galten ohne Schonfrist für die Verwaltung diejenigen Vorschriften des neuen Datenschutzgesetzes, die die Rechte der Bürger auf Auskunft, Berichtigung, Sperrung und Löschung von Daten gegenüber dem alten Rechtszustand erweiterten. Lediglich die neu eingeführte Pflicht der Verwaltung, jeden Bürger von der Tatsache zu informieren, daß seine Daten automatisiert verarbeitet werden, wurde erst mit dem Inkrafttreten der neuen Dateienregisterverordnung[148] wirksam, da die Benachrichtigung mit einem Hinweis auf die Meldung zum Dateienregister verbunden sein muß.

Nach dem Ablauf der Übergangsfrist am 31. Januar 1993 müssen die öffentlichen Stellen des Landes Berlin allerdings das Datenschutzgesetz in aller Strenge umsetzen. Dies zu kontrollieren, wird eine der Hauptaufgaben des Datenschutzbeauftragten im Jahr 1993 sein.

Insgesamt kann festgestellt werden, daß die erweiterten Bürgerrechte in den ersten beiden Jahren der Geltung des neuen Berliner Datenschutzgesetzes die Tätigkeit der Verwaltung keineswegs – wie teilweise befürchtet worden war – behindert oder gar zum Erliegen gebracht haben.

6.2 Informationsverarbeitungsgesetz

Das *Informationsverarbeitungsgesetz (IVG),* das am 21. Oktober 1992 in Kraft trat[149], enthält für einen bestimmten Sektor der Verwaltungstätigkeit die erforderliche bereichsspezifische Rechtsgrundlage zur Verarbeitung personenbezogener Daten. Im einzelnen herrscht allerdings in der Verwaltung noch große Unsicherheit über den Anwendungsbereich dieses Gesetzes. Teilweise wird es dahingehend mißverstanden, daß jede Verarbeitung personenbezogener Daten für die Zwecke der Verwaltungstätigkeit im Rahmen des zur Aufgabenerfüllung Erforderlichen zulässig ist. Sinn des Informationsverarbeitungsgesetzes ist es jedoch nicht, auf diese Zulässigkeitsvoraussetzungen des alten Berliner Datenschutzgesetzes von 1979 für jede Form der Verarbeitung personenbezogener Daten in der Berliner Verwaltung zurückzufallen.

Das IVG ist vielmehr ein unvollkommener erster Versuch, die Organisation der manuellen und automatisierten Datenverarbeitung im Lande Berlin gesetzlich zu regeln, soweit eine Regelung in anwendungsbezogenen Spezialgesetzen nicht sinnvoll ist. Bereits der Titel des Gesetzes ist mit dem Begriff „Informationsverarbeitung" irreführend, weil er den Fehlschluß nahelegt, das Gesetz enthalte Rechtsgrundlagen für jede Form der Informationsverarbeitung. In Wirklichkeit beschränkt sich das Gesetz auf die Schaffung einer Rechtsgrundlage für spezialgesetzlich nicht regelbare, jedoch notwendige Verarbeitungsformen von perso-

148 GVBl. 1992, S. 175
149 GVBl. 1992, S. 305

nenbezogenen Daten bei der *allgemeinen Vorgangsbearbeitung.* Eher beiläufig enthält es auch eine Rechtsgrundlage für das *Abgeordnetenhaus-Dokumentations- und Informationssystem (ADIS).*

Damit sind in diesen beiden Bereichen Rechtsgrundlagen geschaffen worden, die auch wir stets für erforderlich gehalten haben. Allerdings ist dieses schwer verständliche Gesetz sehr erläuterungsbedürftig.

Viele Fachverwaltungen gingen irrtümlich davon aus, daß mit dem Informationsverarbeitungsgesetz die Notwendigkeit entfallen sei, bereichsspezifische Datenverarbeitungsbefugnisse für die fachliche Aufgabenerledigung zu schaffen.

Demgegenüber enthält das Informationsverarbeitungsgesetz keine Generalermächtigung im Sinne einer Auffangklausel für die Verarbeitung personenbezogener Daten in der Verwaltung. Es regelt vielmehr ausschließlich die allgemeine Verwaltungstätigkeit, soweit hierfür keine besonderen gesetzlichen Vorschriften gelten oder im Hinblick auf das informationelle Selbstbestimmungsrecht erforderlich sind (§ 1 Abs. 1). Mit dieser Formulierung hat der Gesetzgeber deutlich gemacht, wie der Rechtsanwender vorzugehen hat:

Er muß stets als erstes prüfen, ob personenbezogene Daten auf einer spezialgesetzlichen Grundlage oder im Rahmen eines spezialgesetzlich geregelten Aufgabengebiets verarbeitet werden sollen. Ist dies der Fall, so ist kein Raum mehr für die Anwendung des Informationsverarbeitungsgesetzes. Dies gilt auch und gerade dann, wenn die spezialgesetzliche Grundlage der Verwaltungstätigkeit (noch) keine Regelung über die Verarbeitung personenbezogener Daten enthält. Dann ist die Verarbeitung dieser Daten nach § 6 Abs. 1 Satz 1 Nr. 2 BlnDSG nur dann rechtmäßig, wenn der Betroffene eingewilligt hat.

Was ist nun unter *allgemeiner Verwaltungstätigkeit* zu verstehen? Das Informationsverarbeitungsgesetz zählt hierzu die Vorgangsverwaltung, die Dokumentation der Vorgänge und der Verfahrensbeteiligten, die Bürokommunikation sowie sonstige zur ordnungsgemäßen Erledigung der behördlichen Aufgaben erforderliche organisatorische Tätigkeiten, insbesondere den dafür notwendigen Schriftwechsel innerhalb der Verwaltung und nach außen sowie die Erstellung, Verwaltung oder Archivierung der im Rahmen des Geschäftsgangs notwendigen Aufzeichnungen. Als allgemeine Verwaltungstätigkeit gilt auch die Bearbeitung von Anträgen und Vorgängen, die keinem gesetzlich geregelten Sachgebiet zugeordnet werden können, ferner die Durchführung von Rechtsstreitigkeiten.

Zur allgemeinen Verwaltungstätigkeit zählen deshalb vor allem zwei Bereiche, nämlich

- *„Verwaltung der Verwaltung",* bei der zwangsläufig personenbezogene Daten von verwaltungsintern an der Verwaltungstätigkeit Beteiligten (z. B. Sachbearbeitern) verarbeitet werden und
- die *Korrespondenz mit Bürgern,* die sich mit allgemeinen Anliegen (nicht Anträgen auf Grund eines besonderen Gesetzes) an die Verwaltung gewandt haben.

Zur Verwaltung der Verwaltung, die auf das Informationsverarbeitungsgesetz gestützt werden kann, gehört z. B. die Führung von *Textdateien* im Rahmen der automatisierten Textverarbeitung, die lediglich nach Bearbeitern, nicht aber nach Adressaten ausgewertet werden können. Auch zählen hierzu Dateien über bestimmte Funktionsträger innerhalb der Berliner Verwaltung wie z. B. Fortbildungs- und sonstige Beauftragte, Hausmeister oder „Multiplikatoren" der Behörde. Auch Daten der Bearbeiter in sogenannten Benutzerdateien mit ihren individuellen Zugriffsberechtigungen in Bürokommunikationssystemen fallen unter das Informationsverarbeitungsgesetz. Allerdings dürfen derartige interne Dateien nicht mit der allgemeinen Verarbeitung von Personaldaten z. B. in Personalinformationssystemen verknüpft werden, für die die Datenschutzbeauftragten seit jeher eine bereichsspezifische gesetzliche Regelung gefordert haben. Personaldatenverarbeitung ist also gerade keine allgemeine Verwaltungstätigkeit, auch wenn die gesetzliche Grundlage bisher erst in Ansätzen z. B. durch das 9. Gesetz zur Änderung dienstrechtlicher Vorschriften[150] geschaffen worden ist.

[150] s. o. 4.27

Auch die Verarbeitung personenbezogener Daten durch Sachbearbeiter bei Gesprächsprotokollen, Telefonnotizen, elektronischen Nachrichten oder bei der Dokumentenerstellung und -übermittlung in Bürokommunikationssystemen kann einen schwerwiegenden Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen bedeuten. Deshalb ist jeweils gesondert zu prüfen, ob es sich um eine Form der allgemeinen Verwaltungstätigkeit handelt, für die im Hinblick auf das informationelle Selbstbestimmungsrecht keine besonderen gesetzlichen Vorschriften erforderlich sind, wenn sie nicht bereits gelten.

Im Rahmen der *Vorgangsverwaltung* und der *Vorgangsdokumentation* kann auf das Informationsverarbeitungsgesetz lediglich eine manuelle oder automatisierte Speicherung von *Aktenzeichen und Namen der Betroffenen* (Aktennachweis- oder Aktenfindungsdatei) gestützt werden. Die Verarbeitung von personenbezogenen Datensätzen, die weitere Informationen für den Verwaltungsvollzug enthalten, bedarf dagegen einer bereichsspezifischen Rechtsvorschrift oder der Einwilligung der Betroffenen.

Wenn das Informationsverarbeitungsgesetz als Befugnisnorm zur Verarbeitung personenbezogener Daten nach den genannten Kriterien herangezogen werden kann, so bestehen die Rechte des Betroffenen nach dem Berliner Datenschutzgesetz, insbesondere auf Auskunft, Berichtigung, Löschung oder Sperrung dennoch. Das Informationsverarbeitungsgesetz nimmt die Dateien für Zwecke der allgemeinen Verwaltungstätigkeit lediglich von der Pflicht der datenverarbeitenden Stelle aus, eine *interne Dateibeschreibung* anzulegen und sie zum *Dateienregister* beim Berliner Datenschutzbeauftragten zu melden (§ 2 Abs. 2 IVG). Um ein Mindestmaß an Transparenz auch im Bereich der allgemeinen Verwaltungstätigkeit zu gewährleisten, verpflichtet allerdings das Gesetz die datenverarbeitenden Stellen, auch für allgemeine Verwaltungsdateien in einer Kurzbeschreibung die Bezeichnung der Datei, ihre Zweckbestimmung, die Art der gespeicherten Daten und den Kreis der Betroffenen schriftlich festzulegen. Diese Dateikurzbeschreibungen sind nicht nur im Interesse der datenverarbeitenden Stelle sinnvoll, sie werden auch für den Berliner Datenschutzbeauftragten bei Prüfungen wichtige Anhaltspunkte für die Kontrolle der rechtmäßigen Datenverarbeitung liefern.

Das Informationsverarbeitungsgesetz enthält zudem ein Gebot der *Trennung von Verfahren,* in denen personenbezogene Daten auf Grund besonderer gesetzlicher Vorschriften verarbeitet werden, von Verfahren der allgemeinen Verwaltungstätigkeit, „soweit nicht die Verbindung am Arbeitsplatz erforderlich ist" (§ 2 Abs. 4 Satz 1 IVG). Inwieweit sich dieses strikte Trennungsgebot und die damit verknüpfte Zweckbindung von Daten der allgemeinen Verwaltungstätigkeit in der Praxis wird realisieren lassen, bleibt abzuwarten. Sicherlich kann das Trennungsgebot nicht in dem Sinne verstanden werden, daß jeder Mitarbeiter einer Behörde, in der personenbezogene Daten automatisiert verarbeitet werden, mindestens zwei Computer auf seinem Tisch haben muß. Eine hardwaremäßige Trennung verlangt das Gesetz ohnehin nicht. Eine programmgesteuerte Zugriffsdifferenzierung reicht hierfür aus.

Für alle automatisierten Verfahren der allgemeinen Verwaltungstätigkeit schreibt das Informationsverarbeitungsgesetz eine *Risikoanalyse* vor (§ 4). Dies bedeutet, daß die datenverarbeitende Stelle vor der Entscheidung über den Einsatz oder die wesentliche Änderung eines automatisierten Verfahrens der allgemeinen Verwaltungstätigkeit prüfen muß, ob und in welchem Umfang mit der Nutzung der Informationstechnik Gefahren für die Rechte der Betroffenen oder für die Funktionsfähigkeit der Verwaltung verbunden sind. Automatisierte Verfahren dürfen nur eingesetzt oder wesentlich geändert werden, soweit derartige Risiken durch technische oder organisatorische Maßnahmen beherrscht werden können. Die Entscheidung trifft der Leiter der datenverarbeitenden Stelle. Er unterrichtet den Berliner Datenschutzbeauftragten über die Entscheidung.

Die Pflicht zur Erstellung einer Risikoanalyse gilt unabhängig davon, ob das automatisierte Verfahren der allgemeinen Verwaltungstätigkeit nach § 1 Abs. 1 IVG einer besonderen gesetzlichen Grundlage bedarf oder ob es diese Grundlage im IVG selbst findet. Insofern hat das IVG auch Bedeutung für alle automatisierten Datenverarbeitungsverfahren, die auf einer bereichsspezifischen Rechtsgrundlage durchgeführt werden oder für die eine solche Grundlage noch geschaffen werden muß.

Für das *Abgeordnetenhaus-Dokumentations- und Informationssystem* sieht das IVG vor, daß auch die Berliner Verwaltung und die *Öffentlichkeit Daten aus diesem System abrufen dürfen.* Dies gilt für Dokumente, die personenbezogene Daten enthalten, allerdings nur dann, wenn sie zur Veröffentlichung bestimmt sind und wenn diese Daten Gegenstand öffentlicher Sitzungen des Abgeordnetenhauses oder seiner Gremien waren oder wenn schutzwürdige Belange Betroffener einer Veröffentlichung nicht entgegenstehen. Nicht zur Veröffentlichung bestimmte Dokumente sind durch geeignete technische Maßnahmen von Dokumentations- und Informationssystemen getrennt zu halten (§ 3 IVG).

Wir haben bereits im vergangenen Jahr[151] darauf hingewiesen, daß der Gesetzgeber sich mit dem jetzt in Kraft getretenen Informationsverarbeitungsgesetz nicht begnügen darf. Vielmehr sind weitere Regelungen nach dem Vorbild der *Organisationsgesetze* in einigen anderen Bundesländern erforderlich. So ist eine Neukonzeption des Verwaltungsnetzes oder der Aufbau der neuen Telekommunikationsinfrastruktur ohne gesetzliche Grundlage ebensowenig akzeptabel wie die Verarbeitung personenbezogener Daten für Zwecke der IuK-Dienstleistung durch das Landesamt für Informationstechnik (LIT). Insofern bleibt das Informationsverarbeitungsgesetz ein Provisorium, das dringend der Ergänzung durch ein *Gesetz über den Einsatz der Informationstechnik im Land Berlin* bedarf. Die Senatsverwaltung für Inneres sollte ihre jahrelangen Vorarbeiten hierfür alsbald in einen Gesetzentwurf münden lassen.

6.3 Das Berliner Dateienregister

Im Zuge der Novellierung des Berliner Datenschutzgesetzes wurde auch eine Neufassung der *Dateienregisterverordnung* (DateiRegVO)[152] erforderlich, da sich auf Grund der vielen Neuerungen die Meldemodalitäten wesentlich verändert hatten und einer näheren Regelung bedurften. So wurden der Datei-Begriff neu definiert und manuelle Dateien erstmals der Meldepflicht unterworfen.

Eine weitere wichtige Neuerung stellt die Pflicht dar, auch Geräte, mit denen personenbezogene Daten gespeichert werden, zum Geräteregister anzumelden. Die Gesamtheit der Neuerungen machte es erforderlich, die Vordrucke für die Dateiregistermeldungen neu zu gestalten. Im Mai 1992 trat die neue Verordnung in Kraft.

Die *Meldepflicht* erstreckt sich auf alle Behörden und sonstige öffentliche Stellen des Landes Berlin, soweit sie für sich oder im Auftrag für andere Daten verarbeiten. Sie betrifft ferner private Stellen, bei denen dem Land Berlin die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht, sofern sie im Auftrag von öffentlichen Stellen Daten verarbeiten. Auch andere nicht-öffentliche Stellen sind betroffen, wenn sie Aufgaben der öffentlichen Verwaltung wahrnehmen (§§ 2 Abs. 3, 4 BDSG, 2 Abs. 1 BlnDSG). Besonders behandelt werden landesunmittelbare Anstalten des öffentlichen Rechts, die am Wettbewerb teilnehmen (Landesbank Berlin, Feuersozietät - Berliner Leben); die Dateien dieser Stellen werden in einem besonderen Register geführt, das nicht zur öffentlichen Einsichtnahme vorgesehen ist.

Das Recht zur Meldung zum *Besonderen Dateienregister* kann aber auch unter bestimmten Voraussetzungen für das Landesamt für Verfassungsschutz, die Staatsanwaltschaften und bestimmte Bereiche der Polizei und der Landesfinanzbehörden gelten. Wird hierauf Anspruch erhoben, muß ein Antrag bei der zuständigen Aufsichtsbehörde gestellt werden, über den nach Anhörung des Berliner Datenschutzbeauftragten entschieden wird.

Betraf die Meldepflicht bisher nur die gleichmäßig aufgebauten, automatisiert geführten Dateien mit personenbezogenen Daten, so ist sie jetzt erweitert worden auf *nicht-automatisierte Dateien,* aus denen an Dritte übermittelt wird, und automatisierte Datenbestände, die neuerdings unter den Dateibegriff fallen, weil der gleichmäßige Aufbau keine Rolle mehr spielt (z. B. Textmengen).

Die bisher vorgeschriebene Veröffentlichung im Amtsblatt ist entfallen.

Zur Unterstützung beim Ausfüllen der Meldeformulare haben wir eine *Ausfüllanleitung* entwickelt. In Fällen, in denen bereits Meldungen nach altem Recht abgegeben wurden, wurde eine Übersicht aller von dieser Stelle bisher gemeldeten Dateien zur Prüfung der Meldepflicht zur Verfügung gestellt.

Die *Formvorschriften* der DateiRegVO (Verwendung von Originalformularen, Ausfüllung mit üblichen Schreibmaschinentypen) haben den Zweck, die rationelle automationsgestützte Weiterverarbeitung zu ermöglichen. Zu prüfen war, ob die *Meldungen unter Verwendung automatisierter Datenverarbeitung* gefertigt werden können. Dies ist unbedenklich, wenn damit das angestrebte Ziel ebenso erreicht werden kann. So sind bereits verschiedene öffentliche Stellen an uns herangetreten, um von dieser Möglichkeit Gebrauch zu machen. Zum Teil sollen datenbankgestützte Erfassungssysteme, zum Teil Textverarbeitungssysteme eingesetzt werden, um das interne Register zu führen und uns im Wege des Datenträgeraustausches die Meldungen zuzuleiten. In einem Merkblatt wurden die Bedingungen zusammengestellt, die für die automatisierte Meldung gestellt werden müssen. Zusätzlich zur Meldung auf magnetischen Datenträgern müssen allerdings lesbare Ausdrucke abgegeben werden, die dem Originalformular nachempfunden sind, damit die Einsichtsrechte der Bürger gewahrt werden können.

Das LIT führt derzeit das Projekt einer *IuK-Datenbank (IUKDB)* durch, das den Verwaltungen die rationelle Bestandsführung und die interne Registrierung ihrer IuK-Geräte nach § 19 Abs. 4 BlnDSG ermöglichen soll und gleichzeitig die Unterrichtungspflichten an das Abgeordnetenhaus von Berlin (IuK-Gesamtübersicht für den Unterausschuß Kommunikations- und Informationstechnik - KIT - des Hauptausschusses), an den Rechnungshof von Berlin und das Geräteregister beim Berliner Datenschutzbeauftragten erfüllen soll. Durch ein entsprechendes Report-Programm soll auch die Schriftfassung der Meldung der Form des Originalformulars angeglichen werden. Laut Angaben des LIT wird das Verfahren IUKDB Ende 1993 einsatzreif sein. Gegenüber den Bezirken haben wir bereits erklärt, daß wir von Beanstandungen absehen werden, wenn uns übergangsweise verkürzte Geräteübersichten bereitgestellt werden, bis die IUKDB für rationelle Meldungen zur Verfügung steht.

Das LIT ist auch bereit, bei Bedarf *Datenerfassungsprogramme für das Dateienverzeichnis* zu entwickeln und für die meldepflichtigen Behörden bereitzustellen.

Trotz der Festlegung in der DateiRegVO und den Hinweisen in der Ausfüllanleitung gehen immer wieder Meldungen ein, die handschriftlich verfaßt wurden. Weiterhin sind wichtige Grundinformationen, auf die nicht verzichtet werden kann, wie z. B. Dateibezeichnung, Rechtsgrundlage, betroffener Personenkreis, häufig nicht eingetragen. Besonders erschwerend ist die Tatsache, daß in den meisten bisher erhaltenen Meldungen der Bezug von der Datei- zu der Gerätemeldung nicht herbeigeführt werden kann, weil das entsprechende Ordnungsmerkmal bei der datenverarbeitenden Stelle fehlt.

Um den Informationsbedarf der meldepflichtigen Stellen zu der Umsetzung der Meldepflichten zum Dateien- und Geräteregister zu befriedigen, haben wir in der Reihe „Materialien zum Datenschutz" den Band 16 „Informationen zum Berliner Dateienregister" herausgegeben.

6.4 Bestellung behördlicher Datenschutzbeauftragter

Nach § 19 Abs. 5 BlnDSG haben die Behörden und sonstigen öffentlichen Stellen behördliche Datenschutzbeauftragte zu bestellen, um die in § 19 Abs. 1, 2 und 4 BlnDSG beschriebenen Aufgaben (Sicherstellung der Ausführung des Berliner Datenschutzgesetzes und anderer Rechtsvorschriften zum Datenschutz, Führung der internen Datei- und Geräteverzeichnisse) zu erfüllen. Über die Verweisung auf §§ 36 und 37 BDSG werden weitere Anforderungen an den behördlichen Datenschutzbeauftragten beschrieben und ihm weitere Aufgaben zugeteilt.

Zum Jahresende 1992 waren uns von ca. 540 öffentlichen Stellen, davon 430 Schulen, behördliche Datenschutzbeauftragte offiziell bekanntgegeben worden. Von den 23 Bezirken hatten 13 behördliche Datenschutzbeauftragte benannt, von den 19 obersten Landesbehörden 10. Bei den nachgeordneten Behörden der

[151] Jahresbericht 1991, 2.1
[152] GVBl. 1992, S. 175

Hauptverwaltung, den rechtsfähigen und nicht rechtsfähigen Anstalten, den sonstigen Körperschaften und Stiftungen des öffentlichen Rechts haben uns ca. ein Drittel ihre behördlichen Datenschutzbeauftragten bekanntgegeben.

Insgesamt ist davon auszugehen, daß weniger als die Hälfte aller Stellen, die behördliche Datenschutzbeauftragte zu ernennen haben, dieser gesetzlichen Pflicht bisher nachgekommen sind. Nur in sehr seltenen Fällen sind behördliche Datenschutzbeauftragte ernannt worden, die kein weiteres Amt ausüben müssen.

Bei der Bestellung behördlicher Datenschutzbeauftragter ist also leider ein erhebliches *Vollzugsdefizit* in der Berliner Verwaltung festzustellen.

Wegen der außerordentlichen Vielfalt der gesetzlichen Aufgaben, die die *Bezirksämter* zu vollziehen haben, sowie der Vielfalt verschiedener Typen von ADV-Systemen, die in den Bezirksämtern betrieben werden, werden an den behördlichen Datenschutzbeauftragten eines Bezirkes besondere Anforderungen hinsichtlich der Qualifikation gestellt.

Wir haben sehr früh in Informationsveranstaltungen mit Vertretern der Bezirke und der Hauptverwaltung darauf hingewiesen, daß wir angesichts des Aufgabenspektrums eines behördlichen Datenschutzbeauftragten davon ausgehen, daß in größeren Behörden wie z. B. in Bezirksämtern die Tätigkeit des behördlichen Datenschutzbeauftragten mindestens eine Vollzeitkraft ausschließlich in Anspruch nimmt. Hinnehmbar wäre höchstens eine Personalunion mit dem schon seit längerer Zeit zu bestellenden Datenschutzbeauftragten nach dem Sozialgesetzbuch.

Für den Fall, daß eine Behörde für den behördlichen Datenschutzbeauftragten eine eigene volle Stelle bereithält, erübrigt sich auch die leidige Abwägung, mit welchen anderen Ämtern das Amt des behördlichen Datenschutzbeauftragten von der Interessenlage her kompatibel ist. Insbesondere in den Bezirksämtern gibt es kaum Mitarbeiter, die nicht mit personenbezogenen Daten umzugehen haben bzw. an der Gestaltung informationstechnischer Verfahren beteiligt sind.

Die Bezirke haben daher zu Recht darauf hingewiesen, daß der behördliche Datenschutzbeauftragte im Stellenplan berücksichtigt werden muß und (mindestens) eine volle Stelle für ihn zur Verfügung gestellt werden muß. Sie haben uns gebeten, sie bei der Einrichtung entsprechender Stellen zu unterstützen.

Bereits im Oktober 1991 haben wir die für den Stellenplan zuständige Abteilung der Senatsverwaltung für Inneres darauf hingewiesen, daß insbesondere die Bezirksämter sich nicht in der Lage sähen, ihrer Pflicht zur Bestellung behördlicher Datenschutzbeauftragter nachzukommen. Sie verwiesen darauf, daß die notwendigen stellenplanmäßigen Voraussetzungen fehlten und sie durch Aufgabenumschichtungen entsprechend qualifiziertes Personal aus dem Bestand nicht bereitstellen könnten.

In der Antwort hat die Senatsverwaltung für Inneres keinen Zweifel daran gelassen, daß sie erwartet, daß die Bezirke ihren Pflichten zur Bestellung behördlicher Datenschutzbeauftragter nachkommen. Auch wurde nicht explizit in Frage gestellt, daß für die Aufgaben eine volle Stelle bereitstehen müsse. Aber es müsse bei Bedarf die Personalwirtschaftsstelle durch Ausschöpfung aller im eigenen Stellenrahmen vorhandenen Möglichkeiten zur Entlastung des behördlichen Datenschutzbeauftragten beitragen. Erst wenn sich nach Ausschöpfung aller eigenen Möglichkeiten der Personalwirtschaftsstelle herausstellen sollte, daß der bestellte Datenschutzbeauftragte darüber hinaus weiterer Entlastung bedarf, wäre die Senatsverwaltung bereit zu prüfen, ob in unabweisbaren Einzelfällen eine Fortschreibung des Stellenplanes oder der Beschäftigungsplanung zur Unterstützung des behördlichen Datenschutzbeauftragten, ohne für diesen selbst eine Stelle einzurichten, zwingend geboten erscheint.

Die Senatsverwaltung für Inneres geht also offenbar davon aus, daß in den Bezirken ausreichend Spielräume in der Stellenausstattung vorhanden sind, um Mitarbeiter in geeigneten Einstufungen so weit zu entlasten, daß sie das Amt des behördlichen Datenschutzbeauftragten ausfüllen können und bürdet ihnen auf, das Gegenteil zu beweisen, bevor die Senatsverwaltung einen Stellenbedarf prüft.

Nach den Erfahrungen, die inzwischen gewonnen wurden, werden die Bezirksämter kaum in der Lage sein, entsprechend qualifizierte Mitarbeiter für das Amt des behördlichen Datenschutzbeauftragten von anderen Aufgaben abzuziehen. Wenn diese Funktion in den Bezirksämtern ernsthaft wahrgenommen werden soll, reicht es nicht aus, daß Mitarbeiter, die noch andere Aufgaben wahrzunehmen haben, nur zur Erfüllung der Befriedigung des Gesetzeswortlautes pro forma zum Datenschutzbeauftragten bestellt werden, wie einige Bezirksämter es gezwungenermaßen tun. Die Anforderungen des Berliner Datenschutzgesetzes werden daher erst erfüllt werden können, wenn in den Bezirken angemessene Stellen für die behördlichen Datenschutzbeauftragten geschaffen werden.

Fast alle Bezirksämter haben uns gegenüber erklärt, daß sie in Dienstkräfteanmeldungen für 1993 bzw. 1994 Stellen für behördliche Datenschutzbeauftragte eingeplant haben, die zumindest für 1993 alle abgelehnt wurden. Ebenfalls wurde es abgelehnt, den kw-Vermerk an den Stellen der bezirklichen Planungsbeauftragten zu streichen, um die Stellen für die behördlichen Datenschutzbeauftragten zu verwenden. Parlamentarische Vorstöße des Rates der Bürgermeister und der Fraktion Bündnis 90/Grüne wurden abgelehnt.

Zusammenfassend vermittelt sich hier folgender Eindruck: Die Notwendigkeit der Bestellung behördlicher Datenschutzbeauftragter wird allgemein gesehen. Der politische Wille geht aber nicht so weit, die personellen und materiellen Ressourcen im notwendigen Maß bereitzustellen. Dies gilt sowohl für die Bezirke, die keine Prioritätenverlagerung zugunsten des Datenschutzes für notwendig halten, als auch für die Senatsverwaltung für Inneres, die Wünsche nach entsprechenden Stellenerweiterungen ohne Prüfung ablehnt. Unter diesen Umständen ist nur verständlich, daß auch das Parlament angesichts der dramatischen Berliner Finanzlage bisher die Haltung der Hauptverwaltung nicht korrigiert.

Wir haben uns mit Beanstandungen wegen eines Verstoßes gegen § 19 Abs. 5 BlnDSG bisher zurückgehalten. Als allerdings ein Bezirk offen bekannte, daß er das Berliner Datenschutzgesetz unter den gegebenen Voraussetzungen nicht umzusetzen gedächte, wurde eine erste Beanstandung ausgesprochen. In zwei weiteren Fällen, in denen sich aus den Stellungnahmen der Bezirke erhebliche Zweifel an der Ernsthaftigkeit ergaben, das Problem zu lösen, wurden Beanstandungen ausgesprochen, die in einem Fall mit der Bestellung eines behördlichen Datenschutzbeauftragten zufriedenstellend erledigt wurde. Alle Beanstandungen betrafen Bezirke aus dem Westteil der Stadt. Bei den östlichen Bezirken haben wir bisher auf Beanstandungen verzichtet.

Im November wurden alle Bezirke zu einer ersten Koordinierungssitzung der behördlichen Datenschutzbeauftragten eingeladen, auch jene ausdrücklich, die noch keinen bestellt hatten. Der Einladung folgten 14 Bezirke. Die Teilnehmer der Sitzung gaben erste Erfahrungsberichte über die Situation in den Bezirken ab. Dabei wurde ohne jede Ausnahme beklagt, daß selbst die zwingenden formalen Aufgaben zur Erfüllung des Berliner Datenschutzgesetzes (Aufbau interner Dateien- und Geräteverzeichnisse, Meldungen zum Dateienregister beim Berliner Datenschutzbeauftragten) kaum nebenamtlich bewältigt werden könnten. Selbst jene, die schon zu behördlichen Datenschutzbeauftragten bestellt worden waren, mußten einhellig bekennen, daß ihre Bestellung nur zur Erfüllung des Gesetzeswortlauts erfolgte, an eine inhaltliche Ausfüllung des Amtes unter der gegebenen Stellensituation aber nicht zu denken sei.

6.5 Der Berliner Datenschutzbeauftragte

Die Dienststelle

Am 14. Oktober 1992 verstarb plötzlich und unerwartet im Alter von 54 Jahren unser Mitarbeiter Diplom-Ingenieur Günter Knodel. Er war stellvertretender Leiter des Bereichs Technik und Organisation. In den sechs Jahren, die er unserer Dienststelle angehörte, erschloß und betreute er mit dem Datenschutz bei offenen und vernetzten Systemen Dimensionen des technischen Datenschutzes, deren Beherrschung heute unabdingbar ist. Sein Verlust wird in diesem Bereich noch lange eine Lücke hinterlassen.

Besetzt werden konnte eine für den Haushalt 1992 bewilligte neue Stelle insbesondere für den Geschäftsbereich des Polizeipräsidenten. Eine deutliche Entlastung im technischen Bereich brachte der Einsatz eines aus der Magistratsverwaltung übernommenen Datenverarbeitungs-Facharbeiters, der mit dem Haushalt 1993 zu unserer Dienststelle versetzt wurde. Trotz der nicht zu bewältigenden Fülle an Aufgaben wurde angesichts der Haushaltslage des Landes auf die Geltendmachung eines weiteren Stellenbedarfs verzichtet.

Um die Arbeitsweise in unserer Dienststelle für alle Interessierten deutlich zu machen, fügen wir diesem Jahresbericht erstmals einen Auszug aus dem Geschäftsverteilungsplan bei[153].

Seit fast zehn Jahren befindet sich die Dienststelle in von der Bauberufsgenossenschaft angemieteten Räumen in Wilmersdorf, Hildegardstraße 29/30, Berlin 31. Wegen Eigenbedarfs kündigte der Vermieter an, daß er eine Mietoption auf weitere fünf Jahre nicht mehr akzeptieren werde. Es ist gelungen, zusammen mit dem Rechnungshof einen Teil eines Verwaltungsgebäudes der AOK in Schöneberg anzumieten. Voraussichtlich ab 1. Oktober 1993 lautet die Adresse des Berliner Datenschutzbeauftragten:

Pallasstraße 25, 10781 Berlin.

Aufgabenentwicklung

Die Zahl der *Beschwerden* und Beratungswünsche von Bürgern ist im Berichtsjahr auf dem hohen Niveau des Vorjahres geblieben.

Die meisten Beschwerden richteten sich auch diesmal gegen den Geschäftsbereich der Innenverwaltung (insbesondere Sicherheitsbereich und Meldewesen), gefolgt von den Sozialämtern der Bezirke. Ein Anstieg der Bürgerbeschwerden war im Personalbereich zu verzeichnen. Zu zahlreichen Anfragen und Beschwerden hat insbesondere die Befragung übernommener Mitarbeiter der ehemaligen DDR-Behörden geführt. Auch im Geschäftsbereich der Senatsverwaltung für Finanzen beschwerten sich - besonders wegen der Übermittlung von Alteigentümerdaten vom LAROV[154] - viele Bürger.

Die *Beratungsersuchen* der Verwaltung hatten auch im vergangenen Jahr wieder einen erheblichen Umfang. Hier stehen die Bereiche Bildung und Forschung sowie Gesundheit und Soziales nach wie vor vorn. Der Bereich Technik und Organisation führte ebenfalls eine große Anzahl von Beratungen bei verschiedensten Verwaltungen durch. Schwerpunkte waren diesmal der Schulbereich und die Justiz.

Abgeordnetenhaus

Auch im Berichtsjahr hat der Berliner Datenschutzbeauftragte anläßlich der parlamentarischen Beratung des Jahresberichtes 1991 von seinem Rederecht vor dem Abgeordnetenhaus Gebrauch gemacht[155].

Schwerpunkt der Beratungen im Unterausschuß Datenschutz des Ausschusses für Inneres, Sicherheit und Ordnung war die Gesetzgebung, beginnend mit einer überaus intensiven Beratung des Allgmeinen Sicherheits- und Ordnungsgesetzes. Sehr positiv anzumerken ist, daß es gelungen ist, noch vor Jahresende das Artikelgesetz[156] zu Ende zu beraten, damit es vor Ablauf des Übergangsbonus in Kraft treten konnte.

Auch die anderen Ausschüsse des Hauses wurden bei einschlägigen Gesetzesmaterien beraten. Der Petitionsausschuß hat uns mehrfach zu ihm vorliegenden Fragen datenschutzrechtlichen Charakters angehört.

Kooperation

Entsprechend seiner gesetzlichen Verpflichtung hat der Berliner Datenschutzbeauftragte mit allen Stellen zusammengearbeitet, die wie er die Aufgabe haben, die Einhaltung der Vorschriften über den Datenschutz zu kontrollieren (§ 24 Abs. 4 BlnDSG). Dies sind in Berlin einerseits die behördlichen Datenschutzbeauftragten, andererseits die externen Kontrollinstanzen für diejenigen Gesellschaftsbereiche, die nicht in den Zuständigkeitsbereich des Berliner Datenschutzbeauftragten fallen: die Senatsverwaltung für Inneres als Aufsichtsbehörde nach dem Bundesdatenschutzgesetz für den nicht-öffentlichen Bereich, der Beauftragte für den Datenschutz des Senders Freies Berlin für den journalistisch-redaktionellen Bereich des Senders sowie die Datenschutzbeauftragten der öffentlich-rechtlich verfaßten Religionsgesellschaften.

Von besonderer Bedeutung für die Effektivität der Arbeit ist die Zusammenarbeit mit dem Bundesbeauftragten sowie den anderen Landesbeauftragten für den Datenschutz. Sie konzentriert sich in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie deren Arbeitskreisen. Unter dem Vorsitz der Landesbeauftragten für den Datenschutz Baden-Württembergs fanden zwei ordentliche und eine außerordentliche Sitzung des Plenums in Stuttgart statt; die dort gefaßten Beschlüsse sind im Anhang abgedruckt.

Nachdem der Bayerische Landesbeauftragte sich geweigert hatte, turnusgemäß den Vorsitz der Konferenz zu übernehmen, wurde der Berliner Datenschutzbeauftragte gebeten, die Konferenz im Jahre 1993 zu leiten. Wir sind bemüht, daß in diesem Jahr deutliche Impulse zur Verbesserung des Datenschutzes von der Bundeshauptstadt ausgehen.

Außer Thüringen haben zwischenzeitlich auch die neuen Bundesländer Datenschutzbeauftragte bestellt; mit dem brandenburgischen Landesbeauftragten wurde eine intensive Zusammenarbeit begonnen, die auch konkrete Hilfen beim Aufbau der Dienststelle umfaßte. Für die alle neuen Länder und Berlin gleichermaßen betreffenden Probleme mit dem informationellen Nachlaß der DDR wurde eine besondere Arbeitsgruppe gebildet, die versuchte, zu einer Reihe von Einzelfragen - allen voran zur Abwicklung des ZER - eine einheitliche Meinung zu bilden.

Auf der Ebene der Arbeitskreise der Konferenz hat sich der Berliner Datenschutzbeauftragte von Anfang an im Bereich Medien und Telekommunikation besonders engagiert[157]. Auch die Internationale Konferenz der Datenschutzbeauftragten hat uns den Vorsitz in einer entsprechenden Arbeitsgruppe übertragen. Ihre Arbeitsergebnisse wurden bei der diesjährigen 14. Sitzung der Konferenz in Sydney zustimmend zur Kenntnis genommen[158].

Aus- und Fortbildung

Die Umsetzung des Datenschutzes setzt außer einem grundsätzlichen Verständnis des Grundanliegens der informationellen Selbstbestimmung juristische und technisch-organisatorische Kenntnisse voraus, die nicht nur nicht trivial, sondern häufig hochkomplex sind. Dies bedeutet, daß Aus- und Fortbildung eine wesentliche Voraussetzung für die Wahrung dieses Grundrechts sind.

Die hierfür erforderlichen Lehrkapazitäten stehen dem Berliner Datenschutzbeauftragten trotz häufiger Nachfragen nicht zur Verfügung. Um wenigstens einen gewissen Grundbedarf abzudecken, waren Mitarbeiterinnen und Mitarbeiter wiederum bereit, in der Freizeit Lehrveranstaltungen in den verschiedensten Bildungseinrichtungen durchzuführen.

Öffentlichkeitsarbeit

Die Öffentlichkeitsarbeit war auch in diesem Jahr ein Schwerpunkt unserer Arbeit. In unserem unregelmäßig erscheinenden Informationsdienst haben wir weiterhin über aktuelle Datenschutzprobleme berichtet und über unsere neuen Broschüren informiert.

Zu besonderen Themen haben wir auch im vergangenen Jahr wieder Informationsmaterialien herausgegeben. Im Vordergrund stand dabei die Verbreitung der *Gesetzesmaterialien* sowie von

153 vgl. Anlage 5
154 siehe oben Ziff. 3.3
155 vgl. Anlage 1
156 vgl. oben 1.2
157 vgl. oben 5
158 vgl. Anlage 3

Materialien zu deren Erläuterung. So gingen zahlreiche Anforderungen zu einem Band zur Umsetzung der Dateienregisterverordnung[159] ein, die zeigen, daß die Verwaltung hierin ein wichtiges Hilfsmittel sieht.

Im Rahmen der *Internationalen Funkausstellung 1991* hatten wir anerkannte Experten aus dem In- und Ausland zu dem Symposium „Komfort und Freiheit des Kunden in der Telekommunikation" eingeladen. Über die gehaltenen Vorträge haben wir einen Dokumentationsband in deutscher und englischer Sprache herausgegeben, der - trotz dieses Spezialthemas - auch bundesweit rege nachgefragt wird.

Beschwerden von Bürgern, insbesondere aus dem Ostteil der Stadt, über die *Werbeflut* in ihren Briefkästen und persönlich an sie gerichtete Werbeschreiben haben uns dazu angeregt, den Bürgern insoweit eine praktische Hilfe an die Hand zu geben.

Nach dem Bundesdatenschutzgesetz dürfen Unternehmen - z. B. Banken, Kaufhäuser oder der Versandhandel - die Daten ihrer Kunden für Zwecke der Werbung oder Markt- und Meinungsforschung nutzen. Deshalb kann es dazu führen, daß ein Kunde, der sich z. B. beim Versandhandel Gartenmöbel bestellt, demnächst Werbebriefe für andere Gartenprodukte erhält. Seine Adresse - ergänzt um die Information, daß er Gartenbesitzer ist - kann auch an Adressenhändler weitergegeben werden, was dann zu weiteren Werbemaßnahmen führen kann. Dagegen kann der Betroffene sich wehren, indem er dieser Nutzung seiner Daten widerspricht. Wir haben auf einem Bogen, der in die Brieftasche paßt, zur Vereinfachung Aufkleber entwickelt, die auf jeden Vertrag und jedes Bestellformular passen und mit dem die Betroffenen einer Nutzung und Übermittlung ihrer Daten für Zwecke der Markt- oder Meinungsforschung widersprechen können:

> Ich widerspreche der Nutzung oder Übermittlung meiner Daten für Werbezwecke oder für die Markt- und Meinungsforschung (§ 28 Abs. 3 Bundesdatenschutzgesetz).

Dieser Aufkleber kann neben die Unterschrift geklebt werden. Der Vertragspartner darf dann die Daten nicht mehr für Werbebriefe oder andere derartige Aktionen verwenden.

Auch diesmal versuchten wir, den Datenschutz auf humorvolle Weise zu präsentieren. Ein Aufkleber, der in seiner Aufmachung an allgemein bekannte Verbotsschilder erinnert, richtet sich diesmal an die Datenverarbeiter:

> Unbefugter Zugriff verboten.
>
> Verarbeiter haften für ihre Daten.

Berlin, 22. März 1993

Dr. Hansjürgen Garstka
Berliner Datenschutzbeauftragter

159 vgl. oben 6.3