



Mitteilungen des Präsidenten

- Nr. 126 -

Inhaltsübersicht	Nr.	Seite
Vorlage zur Kenntnisnahme		
über Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1986	54	2

Druckschluß: 18. November 1986

Ausgegeben am 17. Dezember 1986

Der Präsident
Peter Rebsch

Vorlage zur Kenntnisnahme

Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1986

Inhaltsverzeichnis

Der Berliner Datenschutzbeauftragte gibt zu Beginn des Jahresberichts 1986¹⁾ einen Überblick über die Situation des Datenschutzes (1). Sie ist vor allem von der fortschreitenden Verwaltungsautomation in Berlin, Gesetzgebungsvorhaben des Bundes, insbesondere dem „Sicherheitspaket“ und Vorhaben auf Landesebene geprägt. In den folgenden Abschnitten 2, 3 und 4 werden die Ergebnisse der Datenschutzkontrolle und -beratung dargelegt. Dabei wird unter 3 - entsprechend den gesetzlichen Vorschriften²⁾ - über die Beobachtungen beim Betrieb von Bildschirmtext und bei der Entwicklung anderer Neuer Medien berichtet. Weiter werden neue Entwicklungen zu Feststellungen aus den Vorjahren (5) und die Zusammenarbeit auf dem Gebiet des Datenschutzes (6) dargestellt.

1. Zur Situation

Dezentralisierung und Vernetzung: Entwicklungstendenzen der Verwaltungsautomation in Berlin

Schwierigkeiten und Fortschritte bei der Rechtsentwicklung

Beachtliche Fortschritte bei der Rechtsprechung zu Datenschutzfragen

2. Brennpunkte des Datenschutzes

2.1 Der registrierte Einwohner

Landeseinwohneramt

Praktische Einzelfälle

Ausländerwesen

2.2 Der gezählte Bürger

Volkszählung 1987

Mikrozensus 1985/1986

Bundesstatistikgesetz

Landesstatistikgesetz

Nichtamtliche Befragung ohne Auskunftszwang

2.3 Der verdatete Patient

Keine Kostensenkung auf Kosten der Patienten

Schutz der Patientendaten in Städtischen Krankenhäusern

Einsicht in medizinische Unterlagen

Universitätsklinik

3. Beobachtung der Neuen Medien

3.1 Bildschirmtext

Änderungen des Dienstes

Anbieterprüfungen

Nachträge

3.2 Kabelpilotprojekt

3.3 Fernwirkdienste

3.4 TKO - eine neue Grundordnung für die Medien?

4. Weitere Fragen aus der Kontroll- und Beratungspraxis

4.1 Besondere organisatorische und technische Fragen

Personalcomputer

Personalverwaltungssystem der Technischen Universität

Einsatz des Synchronknotens SK 12 in Datennetzen

Fernwartung bei medizinischen Systemen

Sicherung von Akten und Karteien

Fotomechanische Ausleihverbuchung in Bibliotheken

4.2 Öffentliche Sicherheit und Strafverfolgung

Gesetzgebung

Informationssystem für Verbrechensbekämpfung

Neue Verfahren

Einzelfälle

Öffentlichkeit und Ermittlungsverfahren

4.3 Personalwesen

Personalaktenführung

Personalinformationssysteme

Erhebung von Daten beim Bediensteten

Offenbarung von Personaldaten innerhalb der Behörde

4.4 Datenschutz im Bildungswesen

Hochschule

Schule

Bibliothekswesen

4.5 Organisation und Geschäftsordnung

Datenweitergabe innerhalb des Bezirksamtes

Offenbarungen im Rahmen der Aufsicht

Aktenführung

Vordrucke

Postverkehr

4.6 Umweltschutz auf Kosten des Datenschutzes?

4.7 Datenschutz im Kreditwesen

Schufa

Geldautomaten

Diskretion

Neues Rechenzentrum

5. Nachtrag zu Feststellungen aus den Vorjahren

Übersendung von ISVB-Ausdrucken an die Staatsanwaltschaft (Jahresbericht 1984, Ziff. 2.4)

Datei der Taxifahrermeldungen (Jahresbericht 1981, Ziff. 2.8; Jahresbericht 1984, Ziff. 5)

Rückverteilung von Lohnsteuerkarten (Jahresbericht 1980, Ziff. 2.6; Jahresbericht 1981, Ziff. 2.3)

Wählerverzeichnisse (Jahresbericht 1985, Ziff. 4.3)

Sozialhilfestatistik (Jahresbericht 1981, Ziff. 2.5)

Personaldaten (Jahresbericht 1985, Ziff. 4.3)

¹⁾ Nach § 26 Abs. 2 Berliner Datenschutzgesetz berichtet der Berliner Datenschutzbeauftragte dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich.

²⁾ § 3 Abs. 3 Gesetz zum Staatsvertrag über Bildschirmtext, GVBl. 83, 871 und § 55 Abs. 1 Kabelpilotprojektgesetz, GVBl. 84, 964.
Die Bestimmungen lauten gleichermaßen: „Der Berliner Datenschutzbeauftragte berichtet dem Abgeordnetenhaus von Berlin über von ihm festgestellte Mängel und über seine Vorschläge zu ihrer Behebung und zur Verbesserung des Datenschutzes“.

6. Zusammenarbeit mit anderen Stellen

Datenschutzbeauftragte des Bundes und der Länder

Abgeordnetenhaus

Aufsichtsbehörde für nichtöffentliche Stellen

7. Aufgaben des Berliner Datenschutzbeauftragten**7.1 Im Berichtsjahr 1986****7.2 Voraussichtliche Schwerpunkte****Anlagen**

1. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Januar 1986 zu den Sicherheitsgesetzen
2. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. April 1986 zur Änderung des Bundesverfassungsschutzgesetzes
3. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. April 1986 zum Entwurf einer Telekommunikationsordnung vom November 1985
4. Ergänzung der Entschließung zur Telekommunikationsordnung aufgrund der Neufassung vom April 1986
5. Ausführungsvorschriften über die Führung schriftlicher Unterlagen über Schüler (AV - Schülerunterlagen)
6. Datenschutzrechtliche Bewertung der Datenweitergabe innerhalb des Bezirksamtes - Rundschreiben des Berliner Datenschutzbeauftragten
7. Empfänger regelmäßiger Übermittlungen aus dem Melderegister - Auszug aus der DVO-MeldeG vom 4. März 1986, GVBl. S. 476
8. Anforderungen an Datenschutzregelungen in Strafverfahren

Stichwortregister

für alle seit 1979 veröffentlichten Jahresberichte

1. Zur Situation**Dezentralisierung und Vernetzung:****Entwicklungstendenzen der Verwaltungsautomation in Berlin**

Im Mittelpunkt der Diskussion um den Datenschutz standen im vergangenen Jahr heftige Auseinandersetzungen über die künftige gesetzliche Regelung der Informationsverarbeitung in den Sicherheitsbehörden. Die in der Öffentlichkeit mit viel Emotionen ausgetragene Debatte verdeckt nur zu leicht die Tatsache, daß die Automatisierung von Verwaltungsabläufen in der Landesverwaltung, aber auch auf Bundesebene erhebliche Fortschritte gemacht hat. Bemerkenswert sind vor allem folgende Entwicklungstendenzen:

Die **Dezentralisierung** der Automatisierten Datenverarbeitung (ADV) hat sich durch den immer stärkeren Einsatz von **Personalcomputern** (PC) bzw. Arbeitsplatzcomputern (APC) weiter fortgesetzt. Personalcomputer setzen sich auch in Berlin schneller als allgemein erwartet durch, insbesondere in Anwendungsbereichen, bei denen bisher an eine Automatisierung nicht gedacht werden konnte. Ich habe im letzten Jahresbericht¹⁾ die Risiken der „kleinen Großen Brüder“ ausführlich erörtert und Grundsätze für ihren datenschutzgerechten Einsatz veröffentlicht²⁾. Diese Beurteilungsgrundsätze verbunden mit Erläuterungen habe ich als eine besondere Schrift herausgegeben.

Neben der Zunahme isolierter kleiner Anwendungen von Personalcomputern verstärkt sich auch die Tendenz, den Zugriff auf große zentrale ADV-Verfahren durch den **Ausbau von Netzen** zu

verbessern. Erwähnenswert ist vor allem das Polizeinetz, welches bei Entlastung der zentralen ADV-Kapazität erheblich höheren Bedienungskomfort und verbesserte Flexibilität bieten soll. Weiter wird mit dem Aufbau des geplanten Verwaltungsnetzes in Berlin eine neue ADV-Infrastruktur geschaffen, die die vorhandenen Sternnetze integriert und somit einen kostengünstigeren und flexiblen Zugang an die großen Verwaltungsverfahren ermöglichen soll.

Gerade bei dem Aufbau vernetzter Datenverarbeitung stellt sich die Frage, ob der Datenschutz gewährleistet wird. Ich werde daher im kommenden Jahr die Vorkehrungen zur Gewährleistung des Datenschutzes auch bei den neuen Netzen in Berlin eingehend überprüfen.

Weiter ist die **Entwicklung großer ADV-Verfahren** bemerkenswert. In vielen Bereichen, wie z. B. für die Berechnung der Vergütung, die Steuerverwaltung und die Krankenhausverwaltung wird die Umstellung auf neue Großverfahren konkret geplant.

Eine Erneuerung der bisherigen großenteils veralteten und unter dem Aspekt der Zuverlässigkeit, Ordnungsmäßigkeit und Wirtschaftlichkeit nicht mehr strengen Ansprüchen genügenden Verfahren ist auch aus der Sicht des Datenschutzes zu begrüßen.

Ferner hat die Vorbereitung der **Volkszählung**, vor allem der geplante Einsatz von PC's zu Diskussionen um den Datenschutz geführt. Die Kontrolle und Beratung in diesem Bereich brachte einen Arbeitsschwerpunkt, über den unter 2.2 eingehend berichtet wird.

Auch **große ADV-Projekte auf Bundesebene** werden Bedeutung für Berlin haben, so die Automation in den Ausländerbehörden mit dem neuen Ausländerzentralregister. Auch das auf Bundesebene diskutierte internationale Fahndungsregister für Terroristen kann besondere Bedeutung gewinnen. Zweifellos sind hier neue Herausforderungen für den Datenschutz zu erwarten.

Dies gilt schließlich auch für die bevorstehende grundlegende Erneuerung des Fernmeldewesens in der Bundesrepublik durch die Einführung des **ISDN** (Integrated Services Digital Network). Die Digitalisierung und die schrittweise Integration der bisher auf unterschiedlichen Netzen basierenden Kommunikations- und Datenübertragungsdienste zu einer gemeinsamen Infrastruktur wirft nicht nur neue gesellschaftspolitische Fragestellungen auf, sondern wird auch den Datenschutz erheblich berühren. Dies wird in der Diskussion um die vorgelegte Telekommunikationsordnung deutlich.

Schwierigkeiten und Fortschritte bei der Rechtsentwicklung

Eine wichtige, die Datenschutzkontrolle flankierende Maßnahme ist die Fortentwicklung des Rechts, insbesondere die Einbeziehung der Informationsverarbeitung in die einzelnen Rechtsmaterien. Dieser Prozeß weist auf Landesebene nur geringe Fortschritte auf. So haben sich einige Gesetzesvorhaben - wie z. B. das **Archivgesetz**, die Regelung des Umgangs mit **Personaldaten** im Landesbeamtengesetz, das **Statistikgesetz** - wegen des Zusammenhangs mit entsprechenden Vorhaben auf Bundesebene verzögert. Immerhin konnte die Trennung von Polizei- und Ordnungsverwaltung durch die **Durchführungsverordnung zum Meldegesetz** wenigstens rechtlich praktisch abgeschlossen werden. Auf die näheren Einzelheiten wird weiter unten eingegangen. Bemerkenswert erscheint auch, daß auf untergesetzlicher Ebene erstmals eine umfassende Regelung des Umgangs mit Schülerdaten in der **AV-Schülerunterlagen** möglich wurde¹⁾.

Schließlich hat der Senat einen ersten Schritt unternommen, den Umgang mit **Personaldaten** durch Verwaltungsvorschrift zu regeln.

Probleme bereitet auch nach der Neufassung des Bundespersonalalausweisgesetzes die **Einführung maschinenlesbarer Ausweise**. Für Berlin haben sich die Alliierten vorbehalten, Einführung und Ausgestaltung des Personalausweises zu regeln, so daß das Personalalausweisgesetz in Berlin nicht angewendet wird. Dies bringt besondere Probleme mit sich, weil in dem Bundespersonalalausweisgesetz auch Datenschutzvorschriften enthalten sind. Für die vielen Bürger, die einen Bundespersonalalausweis besitzen und ab

¹⁾ Ziffer 2.1²⁾ Anlage 6¹⁾ Vgl. dazu unter 4.4 und Anlage 5

April 1987 einen maschinenlesbaren Ausweis erhalten können, gelten daher in Berlin weder das Bundespersonalausweisgesetz noch dessen Schutzvorschriften. Der Senat hat allerdings gegenüber dem Abgeordnetenhaus erklärt, er wolle dieses Problem lösen¹⁾.

Schwierigkeiten bereitet auch die mit dem Paßgesetz verbundene Änderung der Strafprozeßordnung (StPO). Denn der neugefaßte § 163 d verweist u. a. auf § 100 a StPO, der in Berlin aufgrund einer Anordnung der Alliierten keine Geltung hat. Weiter erscheint nach wie vor ungesichert, ob das im Gesetz geregelte Verfahren der optischen Ausweislesung in der Praxis überhaupt sicher funktioniert, was ich von Anfang an bezweifelt habe. Entsprechende Tests, die ich seit langem gefordert habe, sind bisher nicht durchgeführt worden. Allerdings hat der Senat in seiner Antwort auf Große Anfragen der F.D.P. und der AL erkennen lassen, daß er nicht plant, transportable Ausweislesegeräte einzusetzen.

Schließlich bleiben die grundsätzlichen Bedenken bestehen, die in einem Beschluß des Deutschen Bundestages vom 17. Januar 1980²⁾ und den Beschlüssen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ihren Ausdruck gefunden haben. Danach war die automatische Lesbarkeit des Ausweises nur dann für hinnehmbar erklärt worden, wenn ein datenschutzgerechtes Melderecht sowie bereichsspezifische Datenschutzregelungen für die Sicherheitsbehörden einen ausreichenden Schutz der Persönlichkeitsrechte der Bürger sicherstellen. Die für den Sicherheitsbereich geforderten Vorschriften fehlen bisher noch.

Äußerungen des Senats lassen erkennen, daß auch dort die Probleme erkannt sind und die Bereitschaft zu einer angemessenen Lösung vorhanden ist. Eine entsprechende Lösung steht allerdings noch aus.

Die bereits aufgetretenen Meinungsverschiedenheiten zwischen einzelnen Bundesländern und die offene Frage, ob der mit dem neuen Ausweis verfolgte Zweck auch erreicht werden kann, sollte Anlaß geben, das Projekt insgesamt zu überdenken. Zur Klarstellung möchte ich allerdings betonen, daß ich einen Sonderweg Berlins abweichend vom Bund oder den übrigen Bundesländern für problematisch halte³⁾. Jedenfalls bleibt der Senat aufgefordert, die offenen Fragen - soweit sie in seiner Zuständigkeit liegen - bis Ende März 1987 zu klären.

Ursache vieler Verzögerungen von wichtigen Gesetzesvorhaben auf Landesebene war die Situation auf **Bundesebene**.

Dort stand das „**Sicherheitspaket**“, ein Bündel neuer Gesetzesvorhaben⁴⁾, im Mittelpunkt der heftigen von starken Emotionen geprägten Diskussion, an deren Ende nur das **Paß- und das Personalausweisgesetz** in Verbindung mit einer **Ergänzung der Strafprozeßordnung** verabschiedet wurden. Das Paket war in der vorgelegten Form - unabhängig vom politischen Standort des Betrachters - nicht richtig gepackt. Es vermengte miteinander unvereinbare Vorhaben. So kann das Bundesdatenschutzgesetz nicht den Sicherheitsgesetzen zugerechnet werden. Im Gegenteil war der Trend zu bereichsspezifischen Regelungen des Datenschutzes gerade für den Sicherheitsbereich in Rechtsprechung und Praxis so deutlich, daß die Behandlung von Sicherheitsfragen im neuen Entwurf des **Bundesdatenschutzgesetzes** einen Bruch mit den bisher erkennbaren Tendenzen bedeutet hätte. Darüber

hinaus entsprach die Zusammensetzung des Paketes nicht den tatsächlichen Notwendigkeiten. Die Konferenz der Datenschutzbeauftragten hat Forderungen zu den Sicherheitsgesetzen aufgestellt¹⁾. Darüber hinaus hat sie eingehende Vorschläge für die Novellierung der Strafprozeßordnung unterbreitet²⁾. Sinnvoll wäre es gewesen, das Gesetz mit den schwersten Informationseingriffen und den für den Bürger härtesten Folgen, die **Strafprozeßordnung**, zuerst zu regeln. Danach hätte dann abgestuft der Bereich des Polizeirechts und des Verfassungsschutzes sowie daran anschließend gegebenenfalls die Bereiche des Verkehrs- und des Ausweisrechts angegangen werden können. Gerade aber die wichtigsten Normenkreise - Strafprozeßordnung und Polizeirecht - waren kein Gegenstand der Diskussion. Stattdessen wurde die Strafprozeßordnung punktuell ergänzt, ohne daß vorhersehbar ist, ob diese Neuregelung sich in ein Gesamtkonzept einer Regelung der Informationsverarbeitung für Zwecke der Strafverfolgung einfügen wird³⁾. Die sachlichen Prioritäten und der Bedarf der Praxis wurden bisher nicht hinlänglich berücksichtigt. Es kann daher nicht verwundern, daß das Sicherheitspaket viel Unmut ausgelöst hat. Im Interesse der Sache ist diese Entwicklung sehr zu bedauern, zumal auch die fachliche Qualität der vorgelegten Entwürfe zu kritisieren war. Hier sei nur daran erinnert, daß in einem Fall keine Berlin-Klausel vorgesehen war und auch im übrigen, wie oben dargestellt, Regelungen getroffen wurden, die gerade bezüglich der Rechtssituation Berlins zu Zweifeln Anlaß geben.

Die Diskussion um das Sicherheitspaket hat bewirkt, daß an sich gut vorbereitete Gesetzesvorhaben, wie das **Archivgesetz**, vom Bundestag nicht mehr abschließend beraten werden konnten, obwohl gerade diese Materie für die Behandlung personenbezogener Daten eine große Rolle spielt - etwa für die Erforschung des Nationalsozialismus. Darüber hinaus bedeutet dies, daß sich auch auf Landesebene die notwendige gesetzliche Regelung dieser Materie verzögert.

Bei einer Bewertung der Rechtsentwicklung auf Bundesebene darf allerdings nicht übersehen werden, daß mit der Verabschiedung des **Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität** ein wesentliches, auch datenschutzrelevantes Gesetz vorliegt, das vor allem Computer und elektronische Zahlungsmittel künftig besser vor Mißbräuchen schützen soll. Auf die Notwendigkeit entsprechender Regelungen hatte ich bereits in meinem Jahresbericht 1981⁴⁾ hingewiesen. So gelang es auch mit meiner Beteiligung, den im Bundestag eingebrachten Entwurf im Laufe der Beratungen erheblich zu verbessern: Insbesondere haben Computerspionage und -sabotage nunmehr eine Regelung erfahren. Künftig wird nach § 202 a Strafgesetzbuch (StGB) bestraft, wer unbefugt Daten, die nicht für ihn bestimmt oder die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft - eine Regelung, die allerdings im wesentlichen in den Datenschutzgesetzen bereits verankert war, soweit es sich um personenbezogene Daten handelt.

Neu ist auch der Tatbestand des Computerbetruges in § 253 a StGB. Danach wird bestraft, wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Ergebnis eines Datenverarbeitungsvorganges durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt und dadurch das Vermögen eines anderen schädigt. Es kommt mithin nicht mehr auf den früher problematischen Umstand der Täuschung eines Menschen bei der Betrugshandlung an. Auch die bisher an der fehlenden Verkörperung der Daten scheiternden Urkundsdelikte wurden um die Tatbestände

¹⁾ Drucksache 10/598 und Drucksache 10/615.

Vgl. das Plenarprotokoll 10/24, S. 1376 ff.

²⁾ 196. Sitzung, Protokoll S. 15661 ff.

³⁾ Vgl. dazu die Diskussion im Abgeordnetenhaus 10/24, S. 1376 ff.

⁴⁾ Das Sicherheitspaket enthielt folgende Elemente:

- a) Gesetz zur Änderung personalausweisrechtlicher Vorschriften (verabschiedet)
- b) Paßgesetz einschließlich Änderung der Strafprozeßordnung (verabschiedet)
- c) Gesetz über die informationelle Zusammenarbeit der Sicherheits- und Strafverfolgungsbehörden des Bundes und der Länder in Angelegenheiten des Staats- und Verfassungsschutzes und nachrichtendienstlicher Tätigkeit (Zusammenarbeitgesetz)
- d) Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz)
- e) Gesetz über den Militärischen Abschirmdienst (MAD-Gesetz)
- f) Änderung des Straßenverkehrsgesetzes (mit Regelung des ZEVS)
- g) Gesetz zur Änderung des Bundesdatenschutzgesetzes einschließlich Änderung des Verwaltungsverfahrensgesetzes

¹⁾ Vgl. Anlage 1

²⁾ Vgl. Inhaltsübersicht in Anlage 8

³⁾ Inzwischen sind Bestrebungen des Bundesjustizministeriums erkennbar, zumindest Teile der Strafprozeßordnung zu überarbeiten. So sind ein „Problem-papier“ und neuerdings ein Referentenentwurf eines Gesetzes zur Regelung der rechtlichen Grundlagen für Fahndungsmaßnahmen, Fahndungshilfsmittel und für die Akteneinsicht im Strafverfahren bekannt geworden. Aus dem Haus des Bundesministers der Justiz verläutet nun auch, daß die - aus meiner Sicht längst überfällige - grundsätzliche Revision der Strafprozeßordnung angegangen werden soll. Diese Ansätze zu einer systematischen Überarbeitung werden allerdings nach dem Terroranschlag von Bonn durch die politische Diskussion um kurzfristige Änderungen der Strafprozeßordnung überdeckt.

⁴⁾ Ziff. 2.6

der Fälschung beweisbarer Daten (§ 269 StGB) und Täuschung im Rechtsverkehr bei Datenverarbeitung (§ 270 StGB) ergänzt. Schließlich werden im Zusammenhang mit den Sachbeschädigungstatbeständen die rechtswidrige Löschung, Unterdrückung, Unbrauchbarmachung oder Veränderung von Daten (§ 303 a StGB) sowie die tätliche Beeinflussung einer Datenverarbeitungsanlage in fremden Unternehmen (§ 303 b StGB) unter Strafe gestellt.

Trotz dieser von mir von jeher nachhaltig unterstützten Reformen bleiben Lücken in der Regelung: Eine zentrale Rolle wird künftig der Umgang mit Gegenständen spielen, mit deren Hilfe die Berechtigung zum Zugang zu Computern nachgewiesen wird. Hierunter fallen magnetisch oder optisch lesbare Berechtigungskarten, künftig auch Chipkarten oder ganze in Taschenrechnerformat untergebrachte Computer, die komplizierte Verschlüsselungs- und Authentifikationsrechnungen durchführen können. Der Gesetzgeber verstand sich derzeit nur dazu, den Mißbrauch von Scheck- und Kreditkarten zu regeln, von Berechtigungsnachweisen also, die im Geldverkehr eine Rolle spielen. Die deutsche Gesetzgebung bleibt damit hinter der amerikanischen zurück, die die Fälschung oder den unbefugten Gebrauch derartiger Berechtigungsinstrumente ganz allgemein bei Computern unter Strafe stellt.

Man wird sorgfältig zu beobachten haben, ob gegenüber dem nunmehr erreichten Stand der Gesetzgebung nicht weitere Initiativen erforderlich sind. Dabei wird auch das Ergebnis der Beratungen über in Österreich und in der Schweiz geplante Gesetzesänderungen zu berücksichtigen sein¹⁾.

Schließlich muß bei einer Beurteilung der Rechtsentwicklung auf Bundesebene auch berücksichtigt werden, daß es im außerrechtlichen Bereich gelang, das **Schufa-Verfahren** neu zu ordnen und die Einigung über eine neue **Schufa-Klausel** zu erreichen. Insoweit sind trotz der offengebliebenen Fragen auch bemerkenswerte Fortschritte auf Bundesebene erzielt worden.

Beachtliche Fortschritte bei der Rechtsprechung zu Datenschutzfragen

Eine Klärung verschiedener datenschutzrelevanter Fragen durch Entscheidungen des **Bundesverfassungsgerichts** ist zu erwarten. Allein in diesem Jahr hat mir das Bundesverfassungsgericht in fünf Fällen Gelegenheit zur Stellungnahme gegeben. Es handelte sich dabei um Verfahren über die Verfassungsmäßigkeit der bisherigen Schufa-Klausel, der Mitteilungen in Strafsachen (MiStra), der Veröffentlichung von Entmündigungen wegen Trunksucht, des Abhörens des Telefons - Mithören von Gesprächen durch Vorgesetzte - sowie die Verfassungsmäßigkeit der Auskunftregelung in den Datenschutzgesetzen für den Sicherheitsbereich. Zu den beiden letzten habe ich ausführlich Stellung genommen²⁾. Ich werde nach den Entscheidungen des Bundesverfassungsgerichts auf diese Verfahren zurückkommen.

Darüber hinaus ist in nahezu allen Gerichtszweigen zu beobachten, daß sich höchstrichterliche Entscheidungen vermehrt mit datenschutzrelevanten Fragen beschäftigen. Hervorzuheben ist die Rechtsprechung des Bundesverwaltungsgerichts³⁾ über den Anspruch des Bürgers auf Auskunftserteilung, wenn er sich beobachtet fühlt; die Entscheidung des Bundesarbeitsgerichts⁴⁾ über die Telefondatenerfassung, die ganz auf der in meinen früheren Jahresberichten vertretenen Linie liegt; die Entscheidung des Bundesgerichtshofs in Strafsachen⁵⁾ über die Unzulässigkeit von Gesprächsaufzeichnungen ohne Wissen der Betroffenen, sei es auch nur zur Analyse der Stimme, und die Entscheidung des Bundessozialgerichts⁶⁾ über die Weitergabe von Daten medizinischer

Unterlagen durch den Kassenarzt an kassenärztliche Vereinigungen.

2. Brennpunkte des Datenschutzes

2.1 Der registrierte Einwohner

Landeseinwohneramt

Die bedeutsamste Änderung in der Zuweisung von Verantwortlichkeiten für die Datenverarbeitung im Land Berlin stellte zweifellos die **Übertragung der Ordnungsaufgaben** vom Polizeipräsidenten auf das neu geschaffene Landeseinwohneramt dar. Dieses Ereignis, das einer in anderen Bundesländern schon frühzeitig in Gang gesetzten Entwicklung folgte, wird von mir als wesentlicher Fortschritt begrüßt. Zwar wurden in der Öffentlichkeit mehrfach Stimmen laut, die aus der Trennung der Aufgaben der Vollzugspolizei und der Ordnungsbehörde insbesondere im Hinblick auf die Abtrennung der Meldebehörde eine Gefährdung der öffentlichen Sicherheit ableiten wollten. Derartige Äußerungen vor allem aus dem Hause des Polizeipräsidenten berücksichtigen nicht, daß keine Einschränkung der tatsächlich erforderlichen Übermittlungen eingetreten ist, und daß in anderen Ländern, bei denen das Trennungsgebot frühzeitig durchgesetzt wurde, eine Beeinträchtigung der öffentlichen Sicherheit nicht zu beobachten ist.

Die Kritiker machen in der Diskussion insbesondere nicht klar, daß bestimmte Änderungen gegenüber früheren Verfahren ihre Ursache nicht in der durch das Berliner Meldegesetz vorgeschriebenen Neuorganisation, sondern in bundesrechtlichen Vorgaben haben: So wird die Löschung der Daten volljähriger Kinder im Datenbestand der Eltern sowie die entsprechende Löschung der gesetzlichen Vertreter vom Melderechtsrahmengesetz des Bundes erzwungen. Klagen der Polizei, nunmehr sei die Suche nach Angehörigen bei Unfällen und bei Ermittlungsverfahren erschwert oder gar unmöglich, müßten daher an den Bundesgesetzgeber gerichtet werden. Für Berlin hatte ich im Gesetzgebungsverfahren vorgeschlagen, die Möglichkeit der freiwilligen Speicherung von zu benachrichtigenden Personen zu schaffen; dies war vom Senator für Inneres abgelehnt worden.

Das im neuen Meldegesetz vorgesehene Landeseinwohneramt nahm fristgerecht zum 1. April 1986 seinen Dienst auf. Die **Organisation** entspricht den an diesen Bereich zu stellenden Datenschutzforderungen. Erst relativ kurz vor diesem Termin hatte sich der Senat hinsichtlich der Aufgabenzuweisung für eines von vier Modellen entschieden, die theoretisch der Umorganisation zugrundegelegt werden konnten: Gegenüber der - datenschutzrechtlich nicht vertretbaren, vom Polizeipräsidenten gleichwohl favorisierten - Minimallösung, das bisherige zentrale Einwohnermeldeamt des Polizeipräsidenten zu verselbständigen und die Meldestellen auch organisatorisch in den Polizeiausschnitten zu belassen, und anderen vermittelnden Lösungen wurde die - aus der Sicht des Datenschutzes günstigste - Entscheidung für die „große Lösung“ getroffen.

Entsprechend den unterschiedlichen Aufgabenkreisen wurde das Amt neben der internen Verwaltung in die Abteilungen Einwohnerwesen, Kraftfahrzeugwesen (Verkehrsordnungswidrigkeiten, Kraftfahrzeugzulassung, Fahrerlaubnisse) und Ausländerangelegenheiten gegliedert. Dies bedeutet allerdings nicht, daß zwischen diesen Verwaltungsbereichen personenbezogene Daten frei fließen dürfen, vielmehr handelt es sich im Hinblick auf das Gebot der informationellen Gewaltenteilung und dem daraus abgeleiteten funktionalen Behördenbegriff auch dann um Übermittlungen, wenn personenbezogene Daten von einem Aufgabenbereich in den anderen weitergegeben werden. Eine **Geschäftsanweisung Datenschutz** stellt die Beachtung der Prinzipien des Datenschutzes auch innerhalb des Amtes in erfreulicher Klarheit sicher.

Ungeachtet dieser auch datenschutzrechtlich zufriedenstellenden Lösung bleiben noch einige Fragen offen. In erster Linie zu nennen ist hier die für Berlin besonders wichtige Gewährleistung, daß auch **außerhalb der Dienstzeiten** des Landeseinwohneramtes Ausweisangelegenheiten (insbesondere die Verlängerung) gere-

¹⁾ Vgl. Entwurf einer Strafgesetzesnovelle 1985 in Österreich insbesondere § 148 a (Betrügerischer Mißbrauch einer Datenverarbeitungsanlage), § 126 a (Datenbeschädigung), § 227 a (Fälschung gespeicherter Daten) und § 229 a (Unterdrückung gespeicherter Daten).

Der Schweizer Bericht zum Vorentwurf über die Änderung des Strafgesetzbuches und des Militärstrafgesetzes enthält u. a. folgende Vorschriften: Art. 143 (Unbefugte Datenbeschaffung), Art. 147 (Betrügerischer Mißbrauch einer Datenverarbeitungsanlage) und Art. 148 (Scheck- und Kreditkartenmißbrauch).

²⁾ Zu den Verfahren liegen auch Stellungnahmen des Bundesbeauftragten und einzelner Landesbeauftragter vor.

³⁾ BVerwG 7 C 71/83, Neue Juristische Wochenschrift (NJW) 1986, S. 2329

⁴⁾ BAG I ABR 48/84

⁵⁾ BGH 3 StR 551/85, NJW 1986, S. 2261

⁶⁾ BSGH 6 RKA 14/83, NJW 1986, S. 1574

gelt werden können. Bei der bisherigen Organisation konnte dies problemlos von den Polizeiabschnitten wahrgenommen werden. Nunmehr ist dem Polizeipräsidenten für diese Fälle eine ausdrückliche Zuständigkeit in Ausweisangelegenheiten zugewiesen worden, mit der Folge, daß den Polizeibediensteten auch ein Zugriff auf die Meldedaten gewährt werden muß. Ein Verfahren, das hinreichende technische und organisatorische Vorkehrungen vorsieht, ist allerdings bislang noch nicht entwickelt worden. Dies sollte alsbald geschehen.

Ähnlich gelagert, aber weniger brisant ist der **Vollzug** von Maßnahmen des Landeseinwohneramtes. Bisher konnte sich der Senat nicht dazu entschließen, für das Landeseinwohneramt einen eigenen Außendienst einzurichten, der z. B. die Entstempelung von Kfz-Kennzeichen vornimmt oder im Bedarfsfall die von den Hotels bereitgelegten Meldescheine abholt. Auch für diesen Bereich stehen noch datenschutzrechtlich befriedigende Lösungen aus.

Zum 1. April 1986 trat auch die nach § 26 Abs. 2 Meldegesetz vom Innensenator zu erlassende **Rechtsverordnung über die regelmäßigen Übermittlungen** aus dem Melderegister an andere Behörden und sonstige öffentliche Stellen in Kraft¹⁾.

Die Verordnung sieht vor, daß an einige Stellen auch Hinweise zu den Grunddaten des § 2 Abs. 1 Meldegesetz regelmäßig mit übermittelt werden. So werden an das Entschädigungsamt Berlin nicht nur die Grunddaten des Familienstands, sondern auch der Zeitpunkt der Scheidung mitgeteilt. Im Rahmen einer vorgeschriebenen Anhörung durch den Senator für Inneres sowie im Ausschuß für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses habe ich darauf hingewiesen, daß die Übermittlung derartiger Hinweise nur unter bestimmten, engen Voraussetzungen zulässig ist und empfohlen, entsprechende Anfragen nur in Einzelfällen zu beantworten. Erörterungen mit den beteiligten Stellen ergaben daraufhin, daß ohnehin je nach Anlaß nur ein Teil der Hinweise regelmäßig übermittelt wird. Der Senator für Inneres wird eine restriktive Handhabung in besonderen Vollzugsbestimmungen vorschreiben.

Die Verordnung sieht ferner vor, daß bestimmte Behörden auf Antrag über Änderungen im Datensatz automatisch unterrichtet werden. So sollen z. B. die für Vormundschaften und Pflegschaften zuständigen Bezirksämter über Änderungen der Anschrift, des Namens und über den Tod des Betroffenen informiert werden. Gleiches gilt für das Entschädigungsamt Berlin hinsichtlich der politisch, rassistisch oder religiös Verfolgten des NS-Regimes und für das Landesversorgungsamt bei Schwerbehinderten. Es ist zu erwarten, daß die genannten Behörden ihren gesamten Personenbestand in das Melderegister einstellen. Dies führt dazu, daß der Merkmalskatalog des § 2 Meldegesetz indirekt um besonders sensible Merkmale („Mündel“, „NS-Verfolgter“, „Schwerbehinderter“) erweitert wird.

Das Landeseinwohneramt hat angesichts dieser Problematik technische Änderungen im ADV-System vorgenommen: Die erforderlichen Mitteilungen werden nunmehr zentral gefertigt; Mitarbeiter der Meldestellen und Bezirksämter haben keine Möglichkeit mehr, die (verschlüsselten) Merkmale abzurufen.

Die Anpassung des Informationssystems Einwohnerwesen an das neue Melderecht hatte bis spätestens 31. März 1986 zu erfolgen. Obwohl der Senator für Inneres auf meine die Umstellung begleitende Beratung verzichtet hat, habe ich ihm meine detaillierten Empfehlungen zur Durchführung dieser Anpassung rechtzeitig zugeleitet.

Der vom Gesetz her geforderte Termin konnte nicht gehalten werden. Vielmehr wurden die vom Landeseinwohneramt als notwendig angesehenen Änderungen erst Mitte Oktober wirksam. Eine solche Verzögerung ist bei ADV-Projekten dieser Größenordnung nicht unüblich.

Bei der Umstellung ist meinen Empfehlungen weithin Rechnung getragen worden. So ist der Zugriff auf die Daten der Einwohnerdatenbank innerhalb des Landeseinwohneramtes weiter differenziert worden und der Zugriff der Bezirkseinschreibämter auf die Datengruppen beschränkt worden, die ihnen nach dem

Meldegesetz und den dazu erlassenen Verordnungen zustehen. Die Abschottung der Bezirkseinschreibämter untereinander steht allerdings noch aus. Da jedes Bezirksamt aufgrund § 1 Abs. 4 Meldegesetz für sich und seinen Aufgabenbereich Meldebehörde ist, ist der bezirksübergreifende Zugriff auf die Meldedaten nicht mehr zulässig.

Die Anforderungen an die Protokollierung von Auskünften aus dem Melderegister sowie an die Löschung von Daten im Melderegister sind durch geeignete technische und organisatorische Maßnahmen befriedigt worden.

Praktische Einzelfälle

Über die grundsätzlichen Probleme hinaus waren im Bereich der Meldebehörde wiederum eine Reihe von Einzelfällen zu erörtern. Bereits in der Vergangenheit habe ich mehrfach darüber berichtet, daß unvollständige oder fehlerhafte Eintragungen im Melderegister zu einer Gefährdung des **Adoptionsgeheimnisses** führen können. Mir wurde erneut ein derartiger Fall vorgetragen:

Den Adoptiveltern eines angenommenen Kindes wurde in der Lohnsteuerkarte der Kinderfreibetrag gestrichen. Die Ermittlungen des Petenten ergaben, daß das Kind auch nach der Adoption weiterhin als Pflegekind geführt wurde mit der Folge, daß aufgrund einer Änderung des Steuerrechts den vorgeblichen Pflegeeltern der Steuerfreibetrag entzogen wurde. Da das Kind demnach trotz Adoption unter dem früheren Namen im Melderegister gespeichert war, wäre es in der Zwischenzeit für die leiblichen Eltern möglich gewesen, personenbezogene Daten der Adoptiveltern zu erfahren, obwohl dem bei Fremdadoptionen das Adoptionsgeheimnis entgegensteht.

Die Überprüfung deckte gleich drei Eingabe- bzw. Verarbeitungsfehler auf: Nachdem das Kind gerichtlich für nichtehelich erklärt worden war, wurde die Verknüpfung zum Ehemann der Mutter nicht gelöscht; nach der Adoption wurde nur der Name des Kindes geändert, nicht aber der frühere Name gelöscht. Schließlich wurde die Löschung auf Antrag der Adoptiveltern mit einem Programm vorgenommen, das zwar den Abruf des früheren Namens nicht mehr ermöglichte, eine Recherche jedoch weiterhin zuläßt. Durch völlige Löschung und Neuaufbau des Datensatzes wurden die Fehler schließlich beseitigt.

Obwohl das Meldegesetz eindeutig vorsieht, daß dem Betroffenen **Auskunft** über alle zu seiner Person gespeicherten Daten zu erteilen ist (§ 8), bereitete die Durchführung dieser Bestimmung in Einzelfällen Schwierigkeiten: Ein Petent vermutete, daß er eine unvollständige Auskunft aus dem Melderegister erhalten habe. Die Überprüfung ergab, daß in der Tat über folgende Daten keine Auskunft erteilt wurde: Name und Anschrift des Wohnungsgebers, protokollierte Melderegisterauskünfte, Berufsbezeichnung und die Tatsache, daß ein behelfsmäßiger Personalausweis eingezogen wurde (einschließlich Nummer und Gültigkeitsdauer). Die Unterlassung hatte verschiedene Gründe, die alle zu verwerfen sind: Hinsichtlich des nebenmeldepflichtigen Wohnungsgebers hatte der damals noch zuständige Polizeipräsident die (engen) Voraussetzungen der Datenübermittlung (§ 25) bzw. der Melderegisterauskunft (§ 28) auch der Auskunft an den Betroffenen (§ 8) zugrundegelegt. Die Protokollierung der Melderegisterauskünfte wurde irrtümlicherweise nicht zu den Daten gerechnet, über die Auskunft zu erteilen ist. Die Berufsbezeichnung war aus ökonomischen Gründen zulässigerweise noch gespeichert, obwohl das Meldegesetz eine Speicherung dieses Datums nicht mehr vorsieht (§ 32 Abs. 1). Aus der Unzulässigkeit der Nutzung folgte der Polizeipräsident, daß auch keine Auskunft an den Betroffenen erteilt werden muß. Aus ähnlichem Grund unterblieb die Auskunft über den Einzug des Personalausweises, da diese Daten künftig in einem eigenen Register geführt werden müssen. Im Ergebnis wurden alle von mir erhobenen Bedenken geteilt und dem Betroffenen eine korrekte Auskunft erteilt, wenn auch erst nach Erinnerung.

Bei eigenen Anfragen an das Melderegister zu Überprüfungszwecken stellte sich heraus, daß das Landeseinwohneramt bei Datenübermittlungen an andere Behörden oder sonstige öffentliche Stellen (§ 25) grundsätzlich das **Geburtsdatum** des Betroffenen mitteilt, und zwar auch dann, wenn die Erforderlichkeit dieses Datums für die Aufgabenerfüllung nicht dargetan wurde bzw.

¹⁾ Vgl. den auszugsweisen Abdruck in Anlage 7

davon ausgegangen werden konnte, daß die anfragende Behörde das Geburtsdatum ohnehin kennt. Bei strenger Auslegung geht in diesem Fall die Übermittlung des Geburtsdatums über den erforderlichen Umfang der Daten hinaus. Andererseits ist das Geburtsdatum ein wichtiges Hilfsmittel zur eindeutigen Identifizierung einer Person bei Namensgleichheit. Erfahrungen in anderen Fällen belegen, daß die Verwechslung von Personen erheblich größere Gefahren birgt als die Offenbarung des Geburtsdatums. Aus diesem Grunde ist es in verschiedenen Verwaltungen von jeher üblich, im Schriftwechsel (z. B. im Betreff) das Geburtsdatum der betroffenen Personen anzugeben. Eine Abwägung ergibt, daß jedenfalls bei der Übermittlung des Geburtsdatums zwischen Behörden die Erforderlichkeit für die Aufgabenerfüllung eingeräumt werden muß. Selbstverständlich bleibt es dabei, daß eine Auskunft über das Geburtsdatum an nichtöffentliche Stellen nur bei Glaubhaftmachung eines berechtigten Interesses zulässig ist (§ 28 Abs. 2).

Ausländerwesen

Von besonderer Bedeutung für Berlin ist angesichts der hohen Anzahl ausländischer Mitbürger die Arbeit der Abteilung Ausländerangelegenheiten. Angesichts des Umfangs der dort vorzuhaltenden personenbezogenen Daten sowie der vielfältigen Anforderungen an die Bearbeitung der Daten (z. B. Erteilung und Verlängerung von Aufenthaltserlaubnissen und -berechtigungen, Bearbeitung von Einreisevorgängen, Bearbeitung der Aufenthaltsanzeige, Wahrnehmung der verschiedensten Mitteilungspflichten), liegt der Einsatz der automatisierten Datenverarbeitung nahe. Eine Projektgruppe hat hierzu einen **Voruntersuchungsbericht** gefertigt, der allerdings neuen Gegebenheiten angepaßt werden muß.

Abhängig ist die Einführung eines automatisierten Verfahrens vor allem auch vom Ergebnis der Beratung um die Neukonzeption des **Ausländerzentralregisters**, das - bislang ohne geeignete Rechtsgrundlage - vom Bundesverwaltungsamt geführt wird. Der Datenaustausch mit diesem Register wird eine wesentliche Funktion eines automatisierten Ausländerregisters im Land Berlin darstellen. An einem Arbeitskreis der Datenschutzbeauftragten des Bundes und der Länder, der sich sowohl mit der Neuorganisation des Ausländerzentralregisters als auch mit der gesetzlichen Regelung befaßt, habe ich mich beteiligt. Die Ergebnisse werden bei der Umsetzung im Land zu berücksichtigen sein.

Zu den Aufgaben des Landeseinwohneramtes gehört die Durchführung des **Asylverfahrens**. Die große Anzahl von Personen, die in diesem Jahr politisches Asyl suchten, machte eine Beschleunigung des Verfahrens erforderlich. Der Senat hat daher im August 1986 die umgehende Konzipierung eines Automationsverfahrens zur Bearbeitung von Asylanträgen beschlossen.

Ziel des Verfahrens ist eine computergesteuerte, möglichst abschließende und einheitliche Sachbearbeitung, durch die sichergestellt wird, daß das Bundesamt für die Anerkennung ausländischer Flüchtlinge am selben Tag informiert wird, an dem der Asylantrag in Berlin entgegengenommen wird. Die bisher auf einem Textautomaten gefertigten Schriftstücke sollen in das ADV-Verfahren integriert werden. Geprüft wird, in welcher Form eine Verbindung mit dem Berliner Ausländerregister möglich ist.

2.2 Der gezählte Bürger

Volkszählung 1987

Zu einem Arbeitsschwerpunkt und zum Gegenstand erneuter öffentlicher Diskussionen wurde bereits in diesem Jahr die **Volkszählung 1987**, die auf der Grundlage des Volkszählungsgesetzes im November 1986 mit der Gebäudezählung begonnen hat. Dabei fielen nunmehr zahlreiche rechtliche und technisch-organisatorische Detailfragen auf, die während des Gesetzgebungsverfahrens noch nicht vorhergesehen wurden, weil die Durchführung der Erhebung im einzelnen erst nach dem Inkrafttreten des Gesetzes geplant worden ist.

Gegen die zu befürchtenden Akzeptanzprobleme hält man besondere Vorkehrungen - wie den Computereinsatz zur Rücklaufkontrolle - und Bußgeldandrohungen für erforderlich.

Von entscheidender Bedeutung bei der Vorbereitung und Durchführung der Volkszählung ist die strikte Trennung (**Abschottung**) zwischen Statistik und Verwaltungsvollzug, die das Volkszählungsgesetz im Anschluß an das Bundesverfassungsgesetz für die Erhebungsstellen vorschreibt. Diese Regelung ist auf Landesebene durch die **Verordnung** zur Durchführung des Volkszählungsgesetzes 1987 konkretisiert worden. Sie sieht in jedem Bezirksamt die Einrichtung eines besonderen Amtes für Volkszählung als örtliche Erhebungsstelle vor, das für die unmittelbare Durchführung der Zählung zuständig ist. In meiner Stellungnahme zum Entwurf dieser Verordnung habe ich empfohlen, in den Ämtern für Volkszählung von vornherein keine Personen einzusetzen, bei denen aufgrund ihrer bisherigen beruflichen Tätigkeit oder aus anderen Gründen zu befürchten ist, daß Erkenntnisse aus der Tätigkeit in der Erhebungsstelle zu Lasten der Auskunftspflichtigen genutzt werden (z. B. Mitarbeiter der Bezirkseinswohnerämter und der Abteilungen für Sozialwesen). Der Verordnungsgeber ist meiner Empfehlung insoweit nicht gefolgt; stattdessen hat der Senator für Inneres in den **Ausführungsvorschriften** die Bezirke lediglich dazu verpflichtet, bei der Auswahl des Erhebungsstellenpersonals darauf zu achten, daß keine Interessenkollisionen mit seinen sonstigen dienstlichen Tätigkeiten eintreten.

Im übrigen sind meine Empfehlungen und Hinweise bei der Abfassung der Verordnung und der Ausführungsvorschriften berücksichtigt worden. Insbesondere die Ausführungsvorschriften enthalten detaillierte Regelungen über die Organisation der örtlichen Erhebungsstellen, die Zutrittsbefugnis zu den Räumen, die Einsichtnahme in Erhebungsunterlagen, die Auswahl, Ausbildung, Belehrung und Verpflichtung der Zähler. Als Zähler dürfen keine Berufsrichter, Staats- oder Amtsanwälte, Gerichtsvollzieher, Polizeivollzugsbeamte, Bedienstete des Landesamtes für Verfassungsschutz oder Finanzbeamte eingesetzt werden. Diese Regelungen werden ergänzt durch eine Geschäftsanweisung, die der Leiter jedes Amtes für Volkszählung an seine Mitarbeiter richtet. Dieses dichte Netz von gesetzlichen Vorschriften und untergesetzlichen Regelungen ist eine wesentliche Voraussetzung für die datenschutzgerechte Durchführung der Volkszählung 1987.

Im April 1986 fand eine bundesweite **Testerhebung zur Volkszählung** auf freiwilliger Basis statt, bei der in zwei Berliner Bezirken 400 Haushalte angesprochen wurden. Datenschutzrechtliche Probleme traten hierbei nicht auf.

Bereits vor Beginn der Gebäudezählung, die die Volkszählung einleitet, habe ich alle **bezirklichen Ämter für Volkszählung** besucht, um möglichst frühzeitig die baulichen, organisatorischen und technischen Verhältnisse und Planungen kennenzulernen. Dabei habe ich ebenfalls Empfehlungen und Hinweise zur Verbesserung der räumlichen und organisatorischen Abschottung gegeben. Nach meinem gegenwärtigen Kenntnisstand sind in allen Bezirken trotz der sehr unterschiedlichen örtlichen Gegebenheiten die Voraussetzungen für die gebotene strikte Trennung zwischen Statistik und Verwaltungsvollzug bei der Volkszählung 1987 geschaffen worden.

Da dies in der öffentlichen Diskussion neuerdings immer stärker in den Vordergrund tritt, weise ich nachdrücklich darauf hin, daß bei der Durchführung der Volkszählung keinerlei Abstriche an der gebotenen Abschottung unter Hinweis auf die zweifellos hohen Kosten gemacht werden dürfen, auch und gerade wenn diese Kosten zunächst unterschätzt worden sind. Eine unzureichende Finanzzuweisung an das Land Berlin oder die Bezirke rechtfertigt keine Verletzung des informationellen Selbstbestimmungsrechts der Auskunftspflichtigen.

Das Statistische Landesamt plant, in den Ämtern für Volkszählung zur Unterstützung der Rücklaufkontrolle isolierte **Personalcomputer** einzusetzen. In der örtlichen Erhebungsstelle soll der in Übereinstimmung mit dem Volkszählungsgesetz auf Datenträgern übermittelte Auszug aus dem Melderegister gespeichert werden. Hinter dem Namen des jeweiligen Auskunftspflichtigen soll dann vermerkt werden, wann die Erhebungsunterlagen ausgegeben wurden und gegebenenfalls ob ihre Rückgabe angefordert worden ist.

Einzelne, auf den Erhebungsbogen eingedruckte Heftnummern, die den Zugriff auf die Unterlagen einer bestimmten Person ermöglichen würden, sollen nicht gespeichert werden.

Es besteht keine Verbindung zum Statistischen Landesamt, das als überörtliche Erhebungsstelle damit keinen Zugriff auf die in den Bezirken anfallenden Daten der Rücklaufkontrolle hat. Nach Abschluß der unmittelbaren Erhebung druckt das Amt für Volkszählung eine Liste derjenigen Personen aus, die trotz Mahnung ihrer Auskunftspflicht nicht nachgekommen sind. Während diese Liste zusammen mit den ausgefüllten Erhebungsbogen dem Statistischen Landesamt zugeleitet wird, werden alle automatisierten Dateien physisch gelöscht. In jedem Bezirk soll außerdem ein Personalcomputer für Zwecke der Kommunikation mit dem Statistischen Landesamt aufgestellt werden, in dem jedoch keine personenbezogenen Daten verarbeitet werden sollen.

Unter folgenden Voraussetzungen habe ich hiergegen keine Einwände erhoben:

- Der Einsatz der Personalcomputer muß äußerst sorgfältig unter Beachtung aller Vorschriften über die Datenverarbeitung und der Grundsätze für organisatorische und technische Maßnahmen zum Datenschutz beim Einsatz von Personalcomputern¹⁾, vorbereitet werden;
- der Bürger muß rückhaltlos über die Datenverarbeitungsprozesse in der örtlichen Erhebungsstelle aufgeklärt werden;
- vom Bürger erhobene Daten dürfen in der örtlichen Erhebungsstelle nicht elektronisch gespeichert werden;
- personenbezogene Daten der Auskunftspflichtigen dürfen bei der Rücklaufkontrolle ausschließlich dezentral verarbeitet werden.

Trotz der grundsätzlichen rechtlichen Zulässigkeit habe ich erhebliche Zweifel geäußert, ob die zur Verfügung stehende Zeit für eine sorgfältige Vorbereitung des Einsatzes der Personalcomputer ausreicht. Aus diesem Grund habe ich ausdrücklich vom Einsatz der Personalcomputer bei der Volkszählung 1987 abgeraten.

Die Erhebungsmerkmale aus der Volkszählung werden im **Landesamt für Elektronische Datenverarbeitung** verarbeitet und ausgewertet. Ich habe die entsprechenden Datenverarbeitungsanlagen und Räume besichtigt und Hinweise zur Abschottung der Einzeldatensätze aus der Volkszählung von anderen ADV-Verfahren gegeben. Die daraufhin gefundene Lösung stellt sicher, daß ausschließlich Mitarbeiter des Statistischen Landesamtes auf Erhebungsmerkmale aus der Volkszählung zugreifen können. Innerhalb des Statistischen Landesamtes müssen allerdings noch technisch-organisatorische Maßnahmen zur Datensicherung getroffen werden.

Das Statistische Landesamt erwägt, im Rahmen der Gebäudezählung von der Einleitung von **Bußgeldverfahren** bei Auskunftsverweigerung abzusehen. Dies entspricht der Aufforderung des Bundesverfassungsgerichts, die amtliche Statistik solle in erster Linie auf Kooperation mit dem Bürger setzen, da staatlicher Zwang auf Dauer gesehen den Umfang und die Genauigkeit statistischer Informationen verringern würde. Wenngleich nach geltendem Recht die Möglichkeit (nicht die Pflicht!) besteht, eine Auskunftsverweigerung bei der Volkszählung mit der Verhängung eines Bußgeldes zu ahnden oder Maßnahmen der Verwaltungsvollstreckung zu treffen, wäre es deshalb sehr zu begrüßen, wenn die Statistikbehörden im Rahmen des Opportunitätsgrundsatzes von dieser Möglichkeit auch bei der eigentlichen Haupterhebung keinen Gebrauch machen würden.

Mikrozensus 1985/86

Unabhängig von der Volkszählung wurden 1985 und 1986 Mikrozensususerhebungen durchgeführt. Die Aufbereitung der Daten habe ich im Statistischen Landesamt überprüft. 1985 bestand aufgrund der internen Arbeitsorganisation die Gefahr, daß versehentlich Mahnschreiben zusammen mit ausgefüllten Erhebungsunterlagen Dritter hätten verschickt werden können. Ich habe diesen Mangel beanstandet. Das Statistische Landesamt

hat daraufhin die erforderlichen Maßnahmen getroffen, um das Risiko der Offenbarung personenbezogener Daten an Dritte auszuschließen.

Erhebliche Bedeutung messe ich der **freiwilligen Mikrozensus-Testerhebung** bei, die 1986 zum zweiten Mal durchgeführt wurde. Sie soll nach dem Willen des Bundesgesetzgebers Erkenntnisse darüber liefern, unter welchen Voraussetzungen statistische Erhebungen ohne Auskunftspflicht durchgeführt werden können. Nach Angaben des Statistischen Landesamtes lag die Antwortquote bei der freiwilligen Testerhebung 1985 in Berlin bei 42,5 % und war damit niedriger als in den meisten anderen Bundesländern. Die Testerhebung 1985 unterschied sich von der Mikrozensus-Haupterhebung nur durch den Verzicht auf die Auskunftspflicht. Die Ergebnisse dieser Erhebung sollen als Ausgangs- und Vergleichsbasis für die Testerhebungen in den Jahren 1986 und 1987 dienen. Nach Auffassung des Wissenschaftlichen Beirats, der bei der Festlegung der Testverfahren mitwirkt, war die relativ geringe Antwortquote auch auf die plakative Betonung der Freiwilligkeit in den Erhebungsunterlagen zur Testerhebung zurückzuführen. Bei der Testerhebung 1986 wurden deshalb alternative Erhebungsunterlagen verwandt, in denen der Hinweis auf die Freiwilligkeit unterschiedlich stark hervorgehoben wurde. Ich habe hiergegen unter der Voraussetzung keine Einwände erhoben, daß die befragten Personen sowohl schriftlich als auch mündlich vom Interviewer auf die Freiwilligkeit hingewiesen werden und der mündliche Hinweis vom Interviewer protokolliert wird.

Bei der Testerhebung 1985 wurden von den Interviewern in anonymisierter Form (Strichliste) und ohne Haushaltsbezug Angaben zur **Befragungssituation** erhoben, um einen Überblick über die Zahl der notwendigen Besuche des Interviewers und die Art der eventuell geäußerten Bedenken der Befragten zu erhalten. Dieses Vorgehen stand im Einklang mit dem Mikrozensusgesetz, da keine zusätzlichen personenbezogenen Daten erhoben wurden.

Für die Testerhebung im Herbst 1986 plante das Statistische Bundesamt die haushaltsbezogene Erhebung dieser Angaben zur Befragungssituation ohne Information der Befragten sowie eine Verknüpfung dieser Angaben mit den zur Organisation der Erhebung übermittelten Meldedaten sowie ggf. mit den Erhebungsmerkmalen.

Diese verdeckte Erhebung über subjektive Einstellungen, Meinungen und Bedenken identifizierbarer Personen hätte sowohl gegen das Mikrozensusgesetz als auch gegen das informationelle Selbstbestimmungsrecht insbesondere derjenigen Befragten verstoßen, die nicht an der Erhebung teilnehmen wollen.

Meinen Einwänden ist durch den Verzicht auf den Haushaltsbezug entsprochen worden.

Bundesstatistikgesetz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits im März 1984 aus dem Volkszählungsurteil des Bundesverfassungsgerichts den Schluß gezogen, daß das **Bundesstatistikgesetz** insbesondere das Statistikgeheimnis neu formuliert werden muß. Ein Entwurf liegt dem Innenausschuß des Deutschen Bundestages zur Beratung vor, der zunächst aufgrund der Auseinandersetzungen um das „Sicherheitspaket“ nicht die erforderliche Zeit für die Beratung dieses vordringlichen Gesetzgebungsvorhabens hatte. Am 8. September 1986 fand eine Anhörung von Sachverständigen vor dem Innenausschuß statt, bei der auch der Bundesbeauftragte für den Datenschutz zahlreiche Änderungs- und Verbesserungsvorschläge machte, die zuvor im zuständigen Arbeitskreis der Konferenz der Datenschutzbeauftragten erörtert worden waren. Der Entwurf geht in verfassungsrechtlich bedenklicher Weise vom Regelfall der Auskunftspflicht aus, von dem in späteren Einzelstatistikgesetzen Ausnahmen gemacht werden können. Zugleich wird bisher nicht hinreichend klar zwischen Erhebungs- und Hilfsmerkmalen unterschieden. Auch stellt der Gesetzentwurf Bundesstatistiken, die auf älteren Rechtsgrundlagen beruhen, auf unbestimmte Zeit von den Anforderungen des Bundesverfassungsgerichts frei.

Während sich der Bundesgesetzgeber bei den Personalausweis- und Paßgesetzen unnötigerweise selbst unter Zeitdruck gesetzt

¹⁾ Vgl. Jahresbericht 1985, Anlage 6

hat, war im Bereich der Statistikgesetzgebung seit dem Urteil des Bundesverfassungsgerichts vom 18. Dezember 1983 der Novellierungsbedarf für das Bundesstatistikgesetz vor der nächsten Volkszählung bekannt. Die jetzt entstandene Situation verringert zwangsläufig die Akzeptanz der Volkszählung, sei es, daß ein nicht ausgereiftes Gesetz rechtzeitig in Kraft tritt, sei es, daß die Bundesstatistik vor der Volkszählung nicht mehr auf die erforderliche neue Gesetzesgrundlage gestellt werden kann.

Landesstatistikgesetz

In den vergangenen Jahren habe ich mehrfach auf die Notwendigkeit einer landesgesetzlichen Regelung für die amtliche Statistik hingewiesen¹⁾. Aus diesem Grunde begrüße ich es, daß der Senator für Inneres noch im Jahre 1985 einen ersten Referentenentwurf für ein Landesstatistikgesetz erarbeitet hat.

Dazu habe ich grundlegende Änderungen und Ergänzungen vorgeschlagen, die aus meiner Sicht nach dem Volkszählungsurteil des Bundesverfassungsgerichts geboten sind. So müssen amtliche Statistiken entweder durch Gesetz oder aufgrund eines Gesetzes durch Rechtsverordnung angeordnet werden, bloße Verwaltungsvorschriften reichen hierzu nicht aus.

Der Umstand, daß auch der Entwurf des Landesstatistikgesetzes von der **Auskunftspflicht** des Befragten als Regelfall ausgeht, widerspricht der vom Bundesverfassungsgericht in den Vordergrund gestellten Pflicht des Gesetzgebers, vor jedem speziellen Statistikgesetz erneut zu prüfen, ob die Weiterentwicklung der statistischen Methoden einen Verzicht auf die generelle Auskunftspflicht zuläßt. Zumindest fordert das Gericht die Umkehrung des Regel-Ausnahme-Verhältnisses: Die Beantwortung einer rechtmäßig angeordneten Frage erfolgt grundsätzlich auf freiwilliger Basis, es sei denn, der Gesetzgeber hat nach pflichtgemäßer Prüfung der Methodenfrage eine Auskunftspflicht vorgesehen.

Das Landesstatistikgesetz soll erstmals eine gesetzliche Grundlage für ein **Statistisches Informationssystem** (früher: Struktur- und Planungsdatenbank) schaffen. Ich habe Vorschläge zur normenklaaren Ausgestaltung der entsprechenden Regelungen gemacht. Insbesondere sind an die Zweckbindung von personenbezogenen Informationen, die beim Verwaltungsvollzug erhoben worden sind, strenge Anforderungen zu stellen. Zumindest durch eine Rechtsverordnung müssen der Verwendungszweck und der Umfang der zu übermittelnden Daten bestimmt werden.

Leider sind die Vorarbeiten am Entwurf eines Landesstatistikgesetzes bisher nicht so weit fortgeschritten, daß das Gesetz mit Sicherheit vor der Volkszählung 1987 in Kraft treten kann. Der Senator für Inneres verweist zur Begründung auf das laufende Gesetzgebungsverfahren für ein Bundesstatistikgesetz, dessen Ausgang abgewartet werden müsse. Ich habe wiederholt bekräftigt, daß die Vorarbeiten für ein Landesstatistikgesetz in Berlin so weit vorangetrieben werden sollten, daß nach der Verabschiedung des Bundesgesetzes auch das Landesstatistikgesetz binnen kürzester Frist das Abgeordnetenhaus passieren kann. Dies betrifft insbesondere die für den Landesgesetzgeber im Vordergrund stehenden Problembereiche, die ausschließlich und ohne Rückgriff auf das Bundesrecht auf Landesebene geregelt werden müssen, wie das Statistische Informationssystem, die Aufgabenzuweisung für das Statistische Landesamt und das besondere Amtsgeheimnis für Landesstatistiken. Auch wenn in Berlin die rechtmäßige Durchführung der Volkszählung 1987 nicht davon abhängt, daß der Landesgesetzgeber zuvor regelt, ob und an wen das Statistische Landesamt Einzelangaben übermitteln darf, weil eine solche Übermittlung (z. B. an die Bezirke) nicht vorgesehen ist, halte ich es dennoch im Interesse einer möglichst hohen Akzeptanz der Volkszählung für wünschenswert, daß das Landesstatistikgesetz vor dem 25. Mai 1987 in Kraft tritt. Zumindest sollte der Gesetzentwurf dem Abgeordnetenhaus vor dem Erhebungsstichtag zugeleitet werden, wobei der Senat sich politisch verpflichten könnte, jedenfalls diejenigen Regelungen des Entwurfs vor dessen Verabschiedung anzuwenden, die dem Schutz der Auskunftspflichtigen dienen.

Daß die Verabschiedung eines Landesstatistikgesetzes auch in anderem Zusammenhang vordringlich ist, zeigt folgendes Beispiel:

Der Polizeipräsident plant die Verlagerung der **Polizeilichen Kriminalstatistik (PKS)** auf das Statistische Landesamt. Insbesondere das statistische Jahrbuch „Kriminalität in Berlin“ und zusätzliche Sonderauswertungen sollen in Zukunft vom Statistischen Landesamt erstellt werden. Zu diesem Zweck ist auch vorgesehen, daß das Statistische Landesamt Einzeldatensätze aus dem polizeilichen Informationssystem für Verbrechensbekämpfung (ISVB) erhält und diese mit selbst erhobenen Daten verknüpft. Ich habe aufgrund meiner eingehenden Prüfung des ISVB²⁾ Bedenken gegen eine Weitergabe personenbezogener Daten aus diesem Informationssystem. Diese Bedenken habe ich den beteiligten Stellen mitgeteilt und um eine präzise Darstellung der geplanten Datenübermittlungen gebeten. Sowohl der Übermittlung von personenbezogenen Daten als auch die Übertragung der Verantwortung für die PKS auf das Statistische Landesamt bedürfen einer gesetzlichen Grundlage, die in das Landesstatistikgesetz aufzunehmen wäre.

Nichtamtliche Befragungen ohne Auskunftszwang

Wie unterschiedlich Erhebungen außerhalb der amtlichen Statistik ausgestaltet sein können, zeigen drei Befragungen im Bereich der Verkehrsplanung.

Bei der im Auftrag der BVG und des Senators für Verkehr und Betriebe durchgeführten **Haushaltsbefragung** zur Ermittlung der voraussichtlichen **Verkehrsnachfrage** ist meinen Empfehlungen für die Durchführung der Erhebung und die Gestaltung der Erhebungsunterlagen in vollem Umfang Rechnung getragen worden. Die von der Gesellschaft für Informationsverarbeitung, Verkehrsberatung und angewandte Unternehmensforschung mbH verwandten Begleitschreiben und grafischen Informationen, mit denen die Befragten detailliert über die Art und Weise der Verarbeitung ihrer personenbezogenen Daten und die Dauer ihrer Speicherung aufgeklärt wurden, halte ich für vorbildlich. Ich führe es nicht zuletzt auf diese umfassende Information der Befragten zurück, daß bei der Haushaltsbefragung eine Antwortquote von 59,8 % erreicht wurde, die erheblich über der Antwortquote der freiwilligen Testerhebung für den Mikrozensus 1985 lag. Auch wenn die amtliche Statistik bisher die gesetzliche Auskunftspflicht für nicht verzichtbar hält, ist sie verfassungsrechtlich gehalten, ständig Methoden zu erproben, die ihr den Übergang zum milderen Mittel der freiwilligen Auskunftserteilung ermöglichen. Diese Methoden werden seit langem von privaten Forschungsinstituten, die sich nicht auf eine gesetzliche Auskunftspflicht stützen können, weiterentwickelt und effektiver gestaltet, so daß diese Ideen und Anregungen von der amtlichen Statistik nutzbringend aufgegriffen werden könnten.

Dies gilt umso mehr, als einzelne Senatsverwaltungen ohnehin zunehmend dazu übergehen, ihren Datenbedarf für Planungszwecke durch die Vergabe von Erhebungsaufträgen an private Forschungsinstitute zu decken, weil nach ihrer Auffassung die amtliche Statistik die gewünschten Daten nicht liefern kann.

Die Haushaltsbefragung zur Verkehrsnachfrage wurde von der Direktionsabteilung Verkehrsplanung der BVG und dem Senator für Verkehr und Betriebe in Auftrag gegeben. Kurz vor Beginn der Haupterhebungsphase veröffentlichte die Direktionsabteilung Öffentlichkeitsarbeit der BVG eine „Sonderinformation für unsere Fahrgäste - BVG-Trümpfe“. Dieses Faltblatt enthielt u. a. auch einen Antrag für die neue **BVG-Jahresnetzkarte**, auf dessen Rückseite ein Fragebogen abgedruckt war, mit dem das bisherige und zukünftige Verkehrsverhalten des Zeitkarteninhabers erfragt werden sollte. Auf diese Weise waren die personenbezogenen Angaben des Antragstellers untrennbar mit seinen Antworten auf dem Fragebogen verbunden. Der Hinweis auf die Freiwilligkeit der Teilnahme an dieser Befragung war nicht hinreichend hervorgehoben. Auch enthielt das Faltblatt keine genauen Hinweise darauf, ob und in welcher Form die Antworten auf dem Fragebogen automatisiert verarbeitet werden. Die Information der Leser über die Ziele der Befragung war ebenfalls unzureichend. Ich habe deshalb datenschutzrechtliche Mängel

¹⁾ Jahresberichte 1983, Ziff. 2.2; 1984, Ziff. 1; 1985, Ziff. 1, Anlage 1

²⁾ Jahresbericht 1985, Ziff. 2.3

bei der Ausgestaltung dieses Fragebogens festgestellt und insbesondere bedauert, daß zeitgleich mit dem Beginn der sorgfältig vorbereiteten und ebenfalls von der BVG in Auftrag gegebenen Haushaltsbefragung diese datenschutzrechtlich unzureichend gestaltete Befragung der Antragsteller für Jahresnetzkarten von der BVG selbst durchgeführt wurde. Nach meiner Auffassung wäre es mit geringem - nicht unverhältnismäßigem - Aufwand möglich gewesen, den Fragebogen von dem Antragsformular zu trennen und den Hinweis auf die Freiwilligkeit deutlicher ausfallen zu lassen.

Im Auftrag des Bundesministers für Verkehr und des Senators für Verkehr und Betriebe führten drei private Forschungsinstitute an sechs Stichtagen eine **Verkehrszählung und Befragung der Reisenden von und nach Berlin** durch. Die Erhebung wird an zwei weiteren Stichtagen im März 1987 abgeschlossen werden. Die Teilnahme an der Befragung ist freiwillig. Bei der Zählung des Straßenverkehrs an den Grenzkontrollpunkten in Berlin und im Bundesgebiet werden jeweils nur die Buchstaben des Ortskennzeichens, nicht aber das vollständige Kfz-Kennzeichen erhoben. Auch für die Durchführung dieser Erhebung habe ich Empfehlungen gegeben. Bei der Zählung des Pkw- und Busreiseverkehrs war geplant, daß die Grenzschutz- bzw. Zollbeamten am Beginn der Transitstrecken an den Stichtagen stets den Zielort (Grenzübergangsstelle) erfragen und die anwesenden Zähler die Antworten mitschreiben. Ich habe darauf hingewiesen, daß ein solches Verfahren bei den Befragten irri- ge Vorstellungen über die Freiwilligkeit der Antwort und die Zweckentfremdung amtlich erhobener Daten zur Folge gehabt hätte. Es wurde ein bürgerfreundliches Verfahren gefunden, das zu keinen zusätzlichen Verzögerungen im Reiseverkehr führte.

2.3 Der verdatete Patient

Keine Kostensenkung auf Kosten der Patienten

Der Kostendruck im Gesundheitswesen zwingt die Kostenträger zu einer zunehmenden Kontrolle der Wirtschaftlichkeit bei den Beteiligten. Diese Kontrolle setzt notwendigerweise die Offenbarung, unter Umständen auch Speicherung und Verarbeitung medizinischer Daten voraus. Wegen der Systematik des Krankenversicherungssystems stellen sich die damit verbundenen Probleme bei Krankenhäusern und Kassenärzten auf verschiedene, allerdings vergleichbare Weise dar.

Eine einschneidende Änderung bei den Krankenhäusern trat dadurch ein, daß im Juli 1985 die Krankenkassen das bisherige Verfahren kündigten, die **Kostenübernahme für Krankenhausbehandlungen** auf unbestimmte Zeit bei entsprechender Selbstkontrolle durch die Krankenhäuser zu übernehmen. Die Kostenübernahme wird je nach Art der Erkrankung zunächst nur noch für einen bestimmten Zeitraum gewährt. Für die Fortführung muß ein weiterer Antrag gestellt werden, mit dem die Krankenkasse von den Krankenhäusern eingehende medizinische Daten erhebt. Von verschiedener Seite wurde vorgebracht, daß die dadurch erzwungene Offenbarung medizinischer Daten ohne Einwilligung der Patienten rechtlich nicht abgedeckt sei. Die Schwierigkeit entsteht in erster Linie dadurch, daß § 100 Sozialgesetzbuch (SGB X) zwar den Arzt verpflichtet, dem Leistungsträger im Einzelfall auf Verlangen Auskunft zu erteilen, dies aber an die Voraussetzungen bindet, daß der Betroffene im Einzelfall eingewilligt hat oder die Offenbarung gesetzlich zugelassen ist. Eine Vorschrift, die eine derartige Befugnis beinhaltet, existiert allerdings nicht. Vielmehr verweist § 372 Reichsversicherungsordnung (RVO) lediglich auf Vereinbarungen der Landesverbände der Krankenkassen mit den Krankenhäusern bzw. deren Vereinigungen unter anderem über die allgemeinen Bedingungen der Abwicklung der Kosten. Vereinbarungen, die dieser Bestimmung genügen, bestehen ebenfalls nicht.

Zwar hat das Bundessozialgericht inzwischen mehrfach bekräftigt, daß die Funktionsfähigkeit des gesetzlich geregelten kassenärztlichen Versorgungssystems eine Befugnis zur Offenbarung bestimmter Daten gebietet und damit die Beteiligten auch zur Offenbarung berechtigt; entsprechende Überlegungen müssen im Verhältnis zwischen Krankenhaus und Krankenkasse gelten. Das Bundessozialgericht betont aber auch den Grundsatz der Erforderlichkeit einerseits, die Notwendigkeit hinreichend nor-

menklarer Bestimmungen über den Umfang der Offenbarung andererseits.

Diese Unklarheiten können nur beseitigt werden, wenn vom Bundessozialgericht für ausreichend erachtete Vereinbarungen über den zulässigen und erforderlichen Umfang der zu übermittelnden Daten getroffen werden. Der Patient muß wissen, worauf er sich einläßt. Nur dann kann er eine Entscheidung im Sinne des informed consent treffen, ob er nämlich über die ärztliche Leistung versicherungsrechtlich oder privatrechtlich abrechnen lassen will.

Eine andere Frage wäre, ob nicht der Offenbarungskatalog des Landeskrankenhausgesetzes, wie von mir bereits bei der letzten Novellierung vorgeschlagen, um eine entsprechende Bestimmung ergänzt werden sollte. Den versicherungsvertraglich festgelegten Pflichten würden dann korrespondierende landesrechtliche Offenbarungstatbestände gegenüberstehen.

Auf Seiten der **Kassenärzte** steht die entsprechende Frage, in welchem Umfang diese eine Verpflichtung zur Offenbarung medizinischer Daten gegenüber den Prüfungs- und Beschwerdeausschüssen der Kassenärztlichen Vereinigung haben. Anfragen nach der Befugnis der Kassenärztlichen Vereinigung habe ich mit dem Hinweis auf die dort bestehenden normklaren Bestimmungen beantwortet, die eine hinreichende Rechtsgrundlage auch nach der Rechtsprechung des Bundessozialgerichtes darstellen.

Eine weitere Maßnahme zur Bekämpfung der Kostenexplosion ist die in der am 1. Januar 1986 in Kraft getretenen Bundespflege-satzverordnung festgelegte Verpflichtung der Krankenhäuser, eine **Diagnosestatistik** mit Angaben über durchgeführte Operationen, zur Verweildauer und das Alter der Patienten zu erstellen und künftig bei den Pflegesatzverhandlungen vorzulegen.

Gleich zu Beginn der Erhebungen gingen bei mir erste Beschwerden ein, die sich dagegen richteten, daß das Datenmaterial personenbezogen gespeichert wurde. In der Tat stellte sich heraus, daß die Verwendung personenbezogener Erhebungsbögen (z. B. unter Verwendung von Patientenetiketten) die erforderliche Anonymität nicht gewährleistete. In Beratungen mit der Senatsverwaltung für Gesundheit und Soziales sowie Vertretern der Städtischen Krankenhäuser wurden Wege gefunden, die es ermöglichen, nicht nur auf den Namen, sondern auch auf die im Krankenhaus überall gebräuchliche Aufnahme- und Verzeichnisnummer zu verzichten. Die personenbezogenen Daten würden in diesem Fall bei der die Krankenakte führenden Stelle bleiben, trotz Anonymität wären bei diesem Verfahren Richtigkeitskontrollen und Korrekturen möglich. Ein Teil der Krankenhäuser hat dieses Verfahren eingeführt.

Schutz der Patientendaten in Städtischen Krankenhäusern

Seit dem 1. Januar 1985 muß die Offenbarung medizinischer Daten in Krankenhäusern an den Bestimmungen des Landeskrankenhausgesetzes gemessen werden (§ 15 Abs. 2 und 3). Eine Reihe von Einzelfällen gab Anlaß, die Anwendung der Vorschrift in der Praxis zu prüfen.

Aufgrund einer parlamentarischen Anfrage hatte der Gesundheitssenator eine Umfrage in den Städtischen Krankenhäusern durchgeführt, wie viele **Sterilisationen debiler Frauen** in der Vergangenheit vorgenommen worden seien. Daraufhin hat das Amtsgericht Tiergarten auf Antrag der Staatsanwaltschaft die Durchsuchung dieser Kliniken angeordnet. Eine Verletzung der ärztlichen Schweigepflicht konnte ich hier nicht feststellen, da Patientendaten auf gerichtlichen Beschluß dann beschlagnahmt werden können, wenn die behandelnden Ärzte selbst einer Straftat oder einer Teilnahme an einer solchen Tat verdächtig sind (§ 97 Abs. 2 Satz 3 StPO). Offenbart der behandelnde Arzt insoweit Patientendaten, um einem gerichtlichen Beschluß zu genügen, so handelt er nicht unbefugt. Die Beschlagnahmefreiheit von Patientendaten soll nur den Patienten schützen, nicht jedoch den Arzt, der einer Straftat an seinem Patienten verdächtig ist. Da nach § 15 Abs. 2 Satz 1 Landeskrankenhausgesetz die Krankenhausleitung verpflichtet ist, zu gewährleisten, daß im Krankenhaus auf Patientendaten nur im erforderlichen Umfang zugegriffen wird, hat sie dafür Sorge zu tragen, daß der Staatsanwaltschaft und ihren Hilfsbeamten keine personenbezogenen Daten

unbeteiligter Patienten offenbart werden. Daraus kann sogar eine Verpflichtung zur Mitwirkung bei der Durchsuchung abgeleitet werden.

Der Rechnungshof trug dem Präsidenten der Freien Universität die Bitte vor, im Rahmen der Prüfung der **Nebentätigkeiten von Hochschullehrern** des Universitätsklinikums Charlottenburg Einsicht in die Patientenakten von Privatpatienten nehmen zu dürfen. Dieser Vorgang hat im Zusammenhang mit einer Ende Juni verkündeten „Verordnung über Abführung bei privater Liquidation“ erhebliches Aufsehen verursacht.

Die materiell-rechtliche Prüfungsbefugnis des Rechnungshofes kann aus § 15 Abs. 3 Nr. 1 Landeskrankenhausgesetz in Verbindung mit §§ 90 Nr. 2, 91 Abs. 1 Nr. 2 und 95 Landeshaushaltsordnung hergeleitet werden, obwohl dieser Regelungszusammenhang nicht die gebotene Normenklarheit aufweist. Wenngleich nicht hinreichend deutlich ist, daß sich die materiell-rechtliche Befugnis zur Rechnungsprüfung auch auf Stellen wie die hier betroffenen Ärzte erstreckt, die neben der Verwaltung und Verwendung öffentlicher Mittel auch erheblichen Nutzen aus diesen Mitteln ziehen, entspricht der Sachverhalt jedoch dem gesetzlich geregelten so weitgehend, daß es sachwidrig erschiene, wollte man ihn von der verfassungsrechtlich verankerten Prüfungskompetenz des Rechnungshofes ausnehmen. Allerdings hat der Rechnungshof zu beachten, daß er auf Patientendaten nur in dem zur Erfüllung seiner Aufgaben erforderlichen Umfang zugreifen darf. § 95 Abs. 1 Landeshaushaltsordnung ist insofern eine Ausprägung des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes. Ich habe angeregt, angesichts der nicht befriedigenden Normenklarheit bei der nächsten Novellierung der Landeshaushaltsordnung eine klarstellende Vorschrift aufzunehmen.

Von manchen Krankenhausverwaltungen wurde verlangt, daß die Ärzte in den zur Aufzeichnung der **Bereitschaftsdienstbelastungen** ausgehängten Bogen den vollen Namen des behandelten Patienten eintragen. Nach den Empfehlungen der Vereinigung kommunaler Arbeitgeber sollen die Aufzeichnungen jedoch lediglich eine Kennzeichnung des Patienten, bei dem die Arbeitsleistung vorgenommen wurde, unter Beachtung der ärztlichen Schweigepflicht enthalten. Der Grundsatz der Erforderlichkeit in § 15 Abs. 2 Landeskrankenhausgesetz verpflichtet die Krankenhausleitung sicherzustellen, daß keine weiteren Patientendaten entstehen. Denn Kontrollmöglichkeiten über die Richtigkeit der angegebenen Dauer des Bereitschaftsdienstes können auch in anderer Weise geschaffen werden.

Wiederum haben sich Patienten darüber beschwert, daß an ihren **Krankenbetten** Behandlungsdaten über sie offen ausgehängt waren. Dies wurde aufgrund meiner Beanstandung geändert. Gleichzeitig habe ich dem Krankenhausbetrieb empfohlen, auch auf die Angabe des Namens nach Möglichkeit zu verzichten, sofern ein Patient dies ausdrücklich wünscht und therapeutische Gründe dies angezeigt erscheinen lassen.

Aufgeworfen wurde das Problem der Anfertigung von **Patientenfotos** und deren weitere Verwendung. Im Rahmen des Behandlungsvertrages ist das Anfertigen einer Fotografie (einschließlich Röntgenaufnahme) zu Behandlungszwecken ohne weiteres zulässig. Das Recht am eigenen Bild als besondere Ausprägung des informationellen Selbstbestimmungsrechts wird jedoch verletzt, wenn es entgegen § 22 Kunsturhebergesetz ohne Einwilligung des Abgebildeten zur Schau gestellt oder verbreitet wird. Ohne Einwilligung des Patienten dürfen Patientenfotos daher nicht zu Lehr- oder Forschungszwecken verwendet werden.

Soweit keine Einwilligung vorliegt, sollten die Bilder vernichtet werden.

Von besonderer Bedeutung ist diese Frage in der Psychiatrie, wo aus therapeutischen Gründen auch mit **Videoaufzeichnungen** gearbeitet wird und ein Bedarf danach besteht, diese Aufzeichnungen zu Lehr- und Forschungszwecken auszuwerten. Zum Schutz der Persönlichkeitsrechte der Patienten ist hier besonderer Wert auf den Inhalt der Einwilligungserklärung zu legen, damit der Patient sich trotz seiner Erkrankung eine Vorstellung davon machen kann, welchen Verwendungszwecken die ihn betreffenden Aufzeichnungen zugeführt werden. Die erklärte Einwilligung ist jederzeit für die Zukunft widerrufbar. Bei der

Archivierung der Aufzeichnungen bedarf es besonderer organisatorischer Maßnahmen, damit sichergestellt wird, daß die Aufzeichnungen nicht zweckentfremdet werden.

Dem Patienten ist Gelegenheit zu geben, den Wortlaut seiner Erklärung nachzuprüfen und insbesondere Einsicht in die über ihn gemachten Aufzeichnungen zu nehmen.

Einsicht in medizinische Unterlagen

Bei den Beratungen zur letzten Novellierung des **Landeskrankenhausgesetzes** wurde die Umsetzung meiner Empfehlungen zur Regelung des Einsichtsrechts aufgeschoben, um eine eingehende Beratung zu ermöglichen. Zwischenzeitlich hat auf Einladung des Senators für Gesundheit und Soziales ein Fachgespräch mit den Chefärzten der Städtischen Krankenhäuser und der Ärztekammer stattgefunden. Meine Forderung nach einer gesetzlichen Garantie des Einsichtsrechts fand erfreulicherweise Bestätigung aus der Fachrichtung der Psychiatrie, obwohl hier der Bundesgerichtshof in seinen letzten Entscheidungen noch weitgehende Zurückhaltung gezeigt hatte.

Die vom Bundesgerichtshof getroffene Unterscheidung zwischen subjektiven und objektiven Daten ist auch in der **Psychiatrie** kein taugliches Abgrenzungskriterium. Gerade der wissenschaftliche Anspruch ärztlicher Behandlung impliziert zugleich auch die Subjektivität beinahe jeder diagnostischen Wertung. Unbefriedigend ist ferner, daß einerseits von einem Recht auf Selbstschädigung des Patienten ausgegangen werden müsse, andererseits jedoch ein Arzt dem Patienten das sogenannte Therapieprivileg entgegenhalten kann, wenn er es aus therapeutischen Gründen für unzulässig hält, den Patienten über seinen Gesundheitszustand zu informieren. Diese Auffassung ist widersprüchlich und daher nicht geeignet, Konflikte zwischen Ärzten und Patienten zu lösen.

Demgegenüber habe ich vorgeschlagen, daß dem Patienten auf Anfrage Auskunft über die zu seiner Person gespeicherten Daten sowie Einsicht in die Krankengeschichte zu gewähren ist. Dies muß auch während oder nach einer psychiatrischen Behandlung gelten. Es muß sichergestellt sein, daß dieses Recht auch für Patienten, die sich durch Krankheit in einem die freie Willensbildung ausschließenden Zustand der Geistestätigkeit befinden, durch einen rechtswirksam bestellten Vertreter ohne Nachteile für die Durchführung der Therapie gewährleistet ist. Sind gesundheitliche Beeinträchtigungen des Patienten zu befürchten, sollte unbeschadet dieser Rechte der wesentliche Inhalt durch einen Arzt vermittelt werden.

Eine solche Regelung wird auch auf die Führung von Krankengeschichten Auswirkungen haben. Diese werden deutlicher den Charakter eines Behandlungsprotokolls über die ordnungsgemäße Durchführung der Behandlung tragen.

Subjektive Beurteilungselemente werden sich auf die wichtigsten Behandlungsaspekte konzentrieren und damit den kompromittierenden Charakter für die Ärzte verlieren. Bei der Vermittlung schwerer Erkrankungsbilder an den Patienten wird die therapeutische Befähigung des Arztes allerdings stärker herausgefordert. Dies kann insgesamt jedoch dazu beitragen, Unstimmigkeiten schon durch rechtzeitige Behandlung ihrer Ursachen zu vermeiden, so daß ein Bedürfnis nach Einsicht bzw. umgekehrt nach Verweigerung der Einsichtnahme gar nicht entsteht. Leidtragende der jetzigen unklaren Rechtslage sind gleichermaßen Patienten und Ärzte.

Universitätsklinik

Die Gewährleistung des Datenschutzes in den Universitätsklinikum wirft weiterhin Probleme auf. Anlässlich der Pensionierung eines Hochschullehrers des Universitätsklinikums Steglitz habe ich überprüft, in welchem Zustand sich die Patientendatei der Abteilung befand, für die dieser Hochschullehrer zuständig war. Bei der Gesamtüberprüfung des Klinikums im Jahre 1983 hatte ich zu diesem Verfahren Mängel hinsichtlich der Ordnungsmäßigkeit festgestellt, die offensichtlich nicht behoben worden waren. Die erneute Überprüfung ergab, daß nach der Pensionierung des Hochschullehrers dem Klinikum die Sicherungsbstände der Patientendatei ohne Unterschied, ob es sich um privatärztliche Daten oder Daten des Universitätsklinikums han-

delte, nicht mehr zugänglich war. Das galt auch für Akten mit den Untersuchungsbefunden. Ich hatte empfohlen, unverzüglich einen Zustand wieder herzustellen, bei dem zumindest Nachteile für die Patienten und die behandelnden Ärzte ausgeschlossen werden konnten. Dazu war es nötig, eine ordnungsgemäße Übergabe vorzunehmen. Das Universitätsklinikum hat in einer Stellungnahme bestätigt, daß inzwischen eine ordnungsgemäße Übergabe stattgefunden habe, und daß die Patientendatei nunmehr wieder in vollem Umfang den Ärzten für Rückgriffe auf Vorbefunde zur Verfügung stehe.

Die **Aufbewahrung medizinischer Unterlagen** in den Klinika ist weiterhin eine erhebliche Schwachstelle.

So stellte ich in der Zahnklinik Süd der Freien Universität fest, daß die Behandlungskartei des zahnärztlichen Notdienstes (Nacht) ungesichert in einem Raum untergebracht war, in dem Studenten und Mitarbeiter ein- und ausgingen und auch für die Öffentlichkeit ein Zugang leicht möglich war. An gleicher Stelle befanden sich ebenfalls ungesicherte Aktenordner mit bezahlten Liquidationen. Ich habe daher die unzureichende Unterbringung dieser personenbezogenen medizinischen Unterlagen formell beanstandet und eine kurzfristige Beseitigung des Mißstandes gefordert. Dabei kam erschwerend hinzu, daß bereits bei einer früheren Prüfung durch das Gesundheitsamt Wilmersdorf die unzureichende Unterbringung medizinischer Dateien beanstandet worden war. Die Freie Universität hat mitgeteilt, daß meinen Beanstandungen Rechnung getragen wurde, indem das nicht mehr benötigte Aktenmaterial ordnungsgemäß vernichtet und die noch benötigten Unterlagen unter Verschuß genommen wurden.

3. Beobachtung der Neuen Medien

3.1 Bildschirmtext

Änderungen des Dienstes

Zur Jahresmitte wurden bei Bildschirmtext (Btx) wichtige Änderungen wirksam:

Stufe 2 wurde mit einer Reihe neuer Leistungsmerkmale in Betrieb genommen. Neben der **Regionalisierung** der Bildschirmtextangebote und der **Abrufstatistik** für Anbieter gibt es einige neue wichtige Merkmale, die für den Datenschutz von Bedeutung sind:

- Teilnehmer können zu ihrem Btx-Anschluß **Mitbenutzerberechtigungen** einrichten. Diese Mitbenutzer erhalten eine besondere Teilnehmernummer (durch eine Ergänzung der Nummer des Hauptteilnehmers um vier Ziffern). Sie verfügen über ein eigenes Kennwort und können daher selbst Mitteilungen senden und empfangen sowie eigenständige Berechtigungen in geschlossenen Benutzergruppen erhalten.

War es bisher bereits Gegenstand von datenschutzrechtlichen Beanstandungen, daß die mangelnde Vertraulichkeit einer Mitteilung beim Empfänger vom Absender nicht beachtet wurde, so kann jetzt der Mitteilungsempfang auf den einzelnen Mitbenutzer beschränkt werden, sofern für den empfangenden Teilnehmeranschluß das neue Leistungsmerkmal in Anspruch genommen wurde. In diesem Falle ist die Übersendung von Mitteilungen nicht mehr mit dem Postkartenversand, sondern mit dem Briefversand vergleichbar.

- Der **Zugang zum Eingabesystem** kann jetzt mit einem besonderen Kennwort gesichert werden, welches vom Kennwort, das für andere Funktionen benutzt werden muß, unabhängig ist. Damit stehen dem Teilnehmer unterschiedliche Berechtigungen für die Seitenbearbeitung und für die Benutzerverwaltung zur Verfügung. Für die Eingabe von Btx-Seiten über Magnetband kann ein weiteres Kennwort bestimmt werden.

Damit folgt die Post einer alten Forderung der Datenschutzbeauftragten, die Anbieterfunktionen eigens durch Kennwort zu schützen, damit in dem Fall, daß ein Dritter unbefugt das Teilnehmerkennwort erfährt oder die Befugnis zum

Seitenabruf unter der Kennung des Teilnehmers erhält, dieser nicht auch Änderungen des Programms vornehmen kann.

- Die **Anzeige von Gebühren und Entgelten** wurde geändert. Während früher die Anzeige von Summenwerten für Abrechnungszeiträume möglich war, kann man sich jetzt nur noch die Gebühren- und Entgeltdaten für die laufende Verbindung anzeigen lassen. Allerdings liegen auch Beschwerden darüber vor, daß dieses neue Verfahren dem rechtmäßigen Teilnehmer die Möglichkeit nimmt, rechtzeitig festzustellen, ob Unbefugte seit seiner letzten Sitzung ohne sein Wissen Gebühren durch den Abruf gebührenpflichtiger Seiten verursacht haben.

Neben der Einführung der Stufe 2 werden nunmehr auch die bislang ausgesetzten Btx-, Verkehrs- und -speichergebühren zur Hälfte erhoben. Dies hat für den Datenschutz deshalb Bedeutung, weil nunmehr aus Kostengründen die Überflutung durch ungewünschte Werbemitteilungen unterbunden worden ist.

Anbieterprüfungen

In Zusammenarbeit mit den anderen Aufsichtsbehörden für Btx, dem Senator für Inneres und dem Senator für Kulturelle Angelegenheiten, wurden erste systematische Überprüfungen bzw. Beobachtungen von Anbieterprogrammen durchgeführt. Sie konzentrierten sich zunächst auf einige Kreditinstitute und einige sogenannte Kleinanbieter. Darüber hinaus habe ich weitere Anbieterprogramme beobachtet.

Bei den routinemäßigen Überprüfungen und Beobachtungen von Anbietern wurden keine gravierenden Verstöße gegen den Btx-Staatsvertrag festgestellt. Allerdings sind nicht viele Programme vollständig mangelfrei. Typische und wiederholt auftretende Mängel sind folgende:

- Kleinanbieter behalten sich das öfteren die Veröffentlichung ihnen zugesandter Mitteilungs- oder Antwortseiten vor. Dies ist unproblematisch, sofern der Anbieter den Absender einer Antwortseite in jedem Fall auf diesen Sachverhalt hinweist. Dies kann nur sichergestellt werden, wenn der Teilnehmer vor dem Abruf der Antwortseite zwangsläufig über eine Seite geführt wird, die den Hinweis auf die Veröffentlichungsabsicht enthält. Es reicht z. B. nicht aus, dies pauschal im Impressum zu tun, da diese Seiten nicht notwendigerweise vom absendenden Teilnehmer zur Kenntnis genommen werden.
- Nach Vorgabe des Anbieters blendet die Btx-Zentrale der Deutschen Bundespost in die Antwortseite **Daten des Absenders** ein. Dabei ist festzustellen, daß die Anbieter sich bei der Vorgabe nicht auf die Daten beschränken, die für die Identifizierung des Absenders und die eventuelle Weiterbearbeitung der Antwort erforderlich sind. In diesem Fall liegt ein Verstoß gegen Art. 9 Abs. 6 Btx-Staatsvertrag vor.

Darüber hinaus habe ich aufgrund von Hinweisen bestimmte Programme besonders untersucht und die jeweiligen Aufsichtsbehörden im Bundesgebiet von meinen Ergebnissen unterrichtet.

Im Falle eines Anbieters, der Angebote zur **amourösen Freizeitgestaltung** veröffentlichte, habe ich untersucht, inwieweit die Veröffentlichung personenbezogener Kontaktanzeigen auf der Einwilligung der Inserenten beruhte. Die stichprobenhaft von mir angeschriebenen angeblichen Inserenten bestätigten mir, daß von ihnen weder ein Auftrag noch eine Einwilligung zur Veröffentlichung einer solchen Btx-Anzeige vorlag.

Auf die Vorhaltungen der von mir unterrichteten Aufsichtsbehörde bestätigte der Anbieter, er habe die Anzeigen aus Tageszeiten entnommen und ohne Einwilligung der Betroffenen veröffentlicht. Die gegen den Btx-Staatsvertrag verstoßende Praxis wurde unverzüglich eingestellt.

In zwei Fällen bin ich auf Bildschirmtext-Meinungsumfragen von Anbietern hingewiesen worden, deren Korrektheit nach Art. 11 Btx-Staatsvertrag zu überprüfen war.

In einem Fall handelte es sich um eine Umfrage der Projektgesellschaft Kabelkommunikation zum Kabelpilotprojekt. Eine

Überprüfung ergab, daß die Umfrage und die Weiterverarbeitung der Ergebnisse den Anforderungen des Art. 11 Abs. 2 Btx-Staatsvertrag entsprach.

In einem anderen Fall handelte es sich um eine Umfrage einer süddeutschen Tageszeitung zur Koalition in Hessen, auf die ich die zuständige Aufsichtsbehörde hinwies, da nicht auszuschließen war, daß sie gegenwärtig parlamentarisch behandelte Angelegenheiten betraf und somit gegen Art. 11 Abs. 1 Btx-Staatsvertrag verstieß.

Nachträge

In einer Reihe von Fällen, die zum Teil auch öffentliche Resonanz gefunden haben, haben sich weitere Entwicklungen gegenüber meinem vorjährigen Bericht ergeben:

- Zu den vom Hamburgischen Datenschutzbeauftragten federführend durchgeführten Untersuchungen zum spektakulären Fall des Hamburger „Hacker-Clubs“, der unter der Identität eines Kreditinstituts für 135 000,- DM gebührenpflichtige Seiten abgerufen hatte, berichtete ich im Vorjahr über den damals als sicher geltenden Erkenntnisstand, daß unbedachter Umgang mit dem geheimen Kennwort ursächlich sei und nicht ein Fehler des Btx-Systems.

Da zwischen dem Redaktionsschlußtermin des Berliner und des Hamburgischen Datenschutzbeauftragten zum Jahresbericht 1985 der Bundesbeauftragte für den Datenschutz aufgrund eines Amtshilfeersuchens des Hamburgischen Datenschutzbeauftragten bei der Prüfung des Btx-Systems zu dem Ergebnis gekommen war, daß ein technischer Mangel des Btx-Systems als Ursache nun doch nicht auszuschließen war, ergab sich somit ein Unterschied zwischen der Darstellung des Hamburgischen Datenschutzbeauftragten und meinen Ausführungen, der von der Bildschirmtext-Fachpresse als Meinungsunterschied interpretiert wurde. Selbstverständlich ist die Darstellung des Hamburgischen Datenschutzbeauftragten letzter Stand in der Angelegenheit.

- In dem im letzten Jahresbericht erwähnten Fall eines Berliner Teilnehmers, unter dessen **Teilnehmerkennung** ein Dritter gebührenpflichtige Seiten aufgerufen hatte, weil er sich dem System gegenüber als freizügig deklariert hatte und unbedachter Umgang mit dem Kennwort nicht auszuschließen war, haben die staatsanwaltschaftlichen Ermittlungen anhand der Überprüfung der Protokolle über die Systemnutzung ergeben, daß der unbefugte Zugriff unter falscher Kennung über ein Terminal erfolgte, welches im Bereich einer Fernsprechentstörungsstelle der Deutschen Bundespost in Berlin aufgestellt war. Die Identität des Täters selbst konnte jedoch bisher nicht ermittelt werden.
- Ich habe im letzten Jahresbericht auf einen **Trick** hingewiesen, bei dem sich Anbieter personenbezogene Daten von Mitteilungsabsendern auf der Kopfzeile der Mitteilung übermitteln ließen, ohne daß der Absender die Möglichkeit hatte, dieses zu erkennen, da dort offen automatisch die Angaben des Anbieters erscheinen. Die Deutsche Bundespost hat bestätigt, daß aufgrund eines Programmfehlers die Anlage solcher Antwortseiten für eine gewisse Zeit möglich war. Derartige Seiten können zwar jetzt nicht mehr editiert werden, es kann aber nicht ausgeschlossen werden, daß sie nach wie vor im System vorkommen. Die Deutsche Bundespost hat im Rahmen der Stufe 2 mit einem neuen Leistungsmerkmal eine Möglichkeit geschaffen, daß Teilnehmer solche Seiten erkennen können. Die Teilnehmer können sich jetzt alle auf einer Dialogseite enthaltenen Daten über den Absender mit der Funktion *05# darstellen lassen.
- Im Zusammenhang mit der lästigen Praxis der massenweisen Übermittlung von **Werbemitteilungen** habe ich mehrere Hinweise und Eingaben zur Praxis privater Robinson-Listen und ihrer Zusammenstellung erhalten, auf die ich unter Einschaltung der zuständigen Aufsichtsbehörden eingegangen bin. Aufgrund der oben erwähnten Einführung einer Kostenpflicht für die Versendung von Mitteilungsseiten hat sich das Problem in der Praxis weitgehend erledigt, so daß ich hier nicht näher darauf eingehen muß.

Zusammenfassend ist festzustellen, daß die bekannten datenschutzrechtlich bedeutsamen technischen Probleme des Btx-Systems mit der Inbetriebnahme der Stufe 2 und der Realisierung zusätzlicher Schutzmaßnahmen erheblich verringert worden sind. Dies bedeutet, daß ich meine Prüfungen zunehmend der datenschutzgerechten Benutzung und Anwendung des Systems vor allem durch Anbieter widmen werde.

3.2 Kabelpilotprojekt

Im Rahmen des Kabelpilotprojektes werden derzeit nur einfache Verteildienste angeboten, bei denen eine Verarbeitung personenbezogener Daten nicht erforderlich ist. Datenschutzrechtliche Probleme entstanden daher beim Betrieb nicht.

Die Situation wird sich ändern, wenn das Programmangebot um **Verteildienste auf Abruf** erweitert wird: Die Entgeltspflichtigkeit dieser Angebote macht es erforderlich, personenbezogene Daten über die Berechtigten und die entstandenen Entgelte zu erheben und zu verarbeiten. Die derzeitigen Planungen sehen vor, daß in der Zentrale lediglich zur Feststellung der Berechtigung Daten vorgehalten werden; die entstandenen Entgelte werden beim Teilnehmer selbst in Speichereinrichtungen von zuvor eingelesebenen Guthaben abgezogen. Das Teilnahmeverhalten ist somit nicht mehr nachvollziehbar. Diese Lösung entspricht der seit Anfang an von den Datenschutzbeauftragten erhobenen Forderung, nutzungsneutrale Zählrichtungen bei den Teilnehmern einzurichten.

Bezüglich der Angebotsdaten wird die in Aussicht genommene vermehrte Nutzung des **Videotextdienstes** über das Kabelpilotprojekt zu beobachten sein: Da hier dem Btx-Staatsvertrag entsprechende Regelungen gelten, könnten hier ähnliche Probleme wie beim Btx-Angebot auftreten.

Die letzte Ausbaustufe des Kabelpilotprojekts, die einen **individuellen Abruf einzelner Programme** erlaubt, läßt sich über das bestehende Breitbandverteildienstnetz nicht realisieren, da die Übertragungskapazität hierfür nicht ausreicht. Die Projektgesellschaft plant deshalb, erste Versuche im Rahmen des von der Deutschen Bundespost initiierten „Berliner Kommunikationssystems“ (BERKOM) durchzuführen, das die Möglichkeiten digital vermittelter Breitbandnetze erprobt. Soweit absehbar, werden bei diesen Versuchen ebenfalls noch keine personenbezogenen Daten verarbeitet, sie werden aber im Hinblick auf die künftigen Entwicklungen sorgfältig zu beobachten sein.

Nach § 4 Kabelpilotprojektgesetz (KPPG) hat der Senat sicherzustellen, daß das Kabelpilotprojekt **wissenschaftlich begleitet** und ausgewertet wird.

Bei der Durchführung eines Forschungsauftrages, der an einen Hochschullehrer des Zentralinstituts für sozialwissenschaftliche Forschung der Freien Universität vergeben wurde, ergaben sich datenschutzrechtliche Fragen zur Beschaffung der erforderlichen Teilnehmerdaten. § 4 Abs. 3 KPPG macht die Erhebung und Speicherung personenbezogener Daten für die Begleitforschung von der Einwilligung der Teilnehmer abhängig. Eine unmittelbare Übermittlung von Teilnehmerdaten von der Deutschen Bundespost an den Auftragnehmer kam daher nur dann in Betracht, wenn die Einwilligung der Teilnehmer zumindest unterstellt werden konnte. Hierzu habe ich es für zulässig erachtet, daß die Landespostdirektion von sich aus die Teilnehmer über das Forschungsvorhaben informiert und auf die Möglichkeit eines Widerspruches gegen die Übermittlung personenbezogener Daten hinweist. Entsprechend diesen Vorgaben konnte das Forschungsprojekt in die Wege geleitet werden.

3.3 Fernwirkdienste

Die Bemühungen der Deutschen Bundespost, unter Benutzung des Fernmeldenetzes erste Betriebsversuche mit Fernwirkdiensten durchzuführen, wurden fortgeführt. § 53 KPPG steckt hierfür einen **nutzungsrechtlichen Rahmen** ab.

Die Landespostdirektion hat erneut Einwendungen gegen die Anwendbarkeit von § 53 KPPG erhoben. Im wesentlichen wird auf die Kompetenzen des Bundes zum Fernmeldewesen einerseits, zum bürgerlichen Recht sowie dem Recht der Wirtschaft andererseits hingewiesen.

Bereits im Zusammenhang mit den Auseinandersetzungen über die Regelung zum Bildschirmtext hatte ich demgegenüber darauf hingewiesen, daß die Fernmeldekompetenz sich in der Regelung des Netzbetriebes, d.h. des reinen Transports der Daten erschöpft. Werden zusätzliche Funktionen übernommen (insbesondere Speicherung, Selektion und Veränderung von Daten), ist der Bereich des Fernmeldewesens verlassen und die Materie unterfällt der „Telekommunikationsmedienkompetenz“. Damit steht den Ländern immer dann Einfluß zu, wenn ein Dienst notwendigerweise mit der Wahrnehmung derartiger Funktionen verknüpft ist.

Was die materiellen Kompetenzen betrifft, ist festzustellen, daß der ordnungsrechtliche Aspekt der zulässigen Nutzung von Medien neben den materiellrechtlichen Vorgaben über Zustandekommen und Abwicklung von Vertragsverhältnissen steht. Während letzterer Bereich zweifelsohne von der Gesetzgebung des Bundes abgedeckt wird (z. B. bürgerliches Recht, Energiewirtschaftsrecht – einschlägig bei Fernmeßdiensten –, Bundesdatenschutzgesetz), fällt die ordnungsrechtliche Kompetenz mangels Zuweisung an den Bundesgesetzgeber in den Zuständigkeitsbereich der Länder. Die Nutzung der Neuen Medien ist damit auf einer abstrakten Ebene vergleichbar mit dem Bauordnungsrecht, das ebenfalls Rahmenbedingungen für die Entfaltung der im übrigen bundesrechtlich geregelten wirtschaftlichen Betätigung schafft.

Ungeachtet dieser Meinungsverschiedenheiten ist von der Bundespost trotz einiger Vorbehalte die Bereitschaft gezeigt worden, bei der Lösung der anstehenden Probleme auf der Basis des § 53 KPPG zu kooperieren. So trat Anfang Juni auf Einladung der Landespostdirektion ein Gremium zusammen, in dem Anwender und Interessenten am TEMEX-System, die Bundespost und meine Dienststelle vertreten sind. Auf einer ersten Veranstaltung habe ich Anbieter und Anwender auf datenschutzrechtliche Probleme hingewiesen und auch dort die Bereitschaft beobachtet, sich mit den Datenschutzproblemen auseinanderzusetzen. Insbesondere war festzustellen, daß bei den Anbietern und Anwendern gleichermaßen wie bei mir die Überzeugung vorherrscht, daß der wirtschaftliche Erfolg der TEMEX-Dienste mit der datenschutzrechtlichen Gewährleistung steht oder fällt.

Als ein Erfolg ist es anzusehen, daß von einem Anbieter (Berliner Wasserwerke) die von mir stets geforderte Anzeigevorrichtung in Form eines Zählwerks, aus dem die Anzahl der vorgenommenen Messungen ersichtlich ist, nicht nur akzeptiert, sondern nunmehr sogar auch favorisiert wird. Ein entsprechendes Produkt wird inzwischen von einem Hersteller angeboten.

3.4 TKO - eine neue Grundordnung für die Medien?

Die Regelung der Inanspruchnahme der verschiedenen Fernmeldedienste findet sich derzeit in einer Reihe von Fernmeldebenutzungsordnungen, die sowohl in Inhalt als auch Aufbau äußerst unübersichtlich sind und materiell zufriedenstellende Datenschutzregelungen vermissen lassen. Über die Probleme, eine angemessene Regelung des Datenschutzes beim Bildschirmtextdienst zu erreichen, hatte ich mehrfach berichtet.

Nach mehrjähriger Arbeit hat im Dezember 1985 der Bundespostminister den Entwurf einer Telekommunikationsordnung vorgelegt, in dem die einzelnen Benutzungsregelungen für die Fernmeldedienste zusammengefaßt und strukturiert werden sollen. Auch der Datenschutz soll hier eine Regelung finden. Die Telekommunikationsordnung ist nicht nur im Hinblick auf die Kompetenzen des Bundes im Fernmeldewesen von höchstem Interesse, sondern hat auch weitreichende Einwirkungen in den in die Zuständigkeit der Länder fallenden Nutzungsbereich, insbesondere bei den Neuen Medien, die im Rahmen der Telekommunikationsordnung nur eine Gruppe von Diensten (Mehrwertdienste) neben den traditionellen, auf den Transport von Informationen ausgerichteten Fernmeldediensten darstellen.

Die Konferenz der Datenschutzbeauftragten hat sich intensiv mit dem Entwurf befaßt und zur datenschutzfreundlichen Gestaltung eine Entschließung gefaßt¹⁾.

Bevor die Telekommunikationsordnung Ende Juni 1986 vom Postverwaltungsrat endgültig verabschiedet wurde, wurden allerdings nur geringfügige, in der Entschließung angesprochene Forderungen berücksichtigt. Folgende wesentliche Forderungen wurden bislang nicht berücksichtigt:

- Verpflichtung der Deutschen Bundespost zur Aufklärung über nicht vermeidbare Risiken bei der Datensicherung;
- präzise Umschreibung der öffentlichen Telekommunikationsdienste einschließlich Definition des jeweils erforderlichen Datenprofils;
- angemessene Regelung über die Zulassung einer Benutzung des öffentlichen Netzes für sonstige Telekommunikationszwecke;
- übersichtliche Definition der für den Datenschutz relevanten Grundbegriffe;
- genaue Umschreibung der vom Teilnehmer beantragbaren „anderen Art der Verarbeitung“ von Verbindungsdaten;
- Datenschutz bei der Entstehung von Gebührendaten;
- Regelungen zu den Inhalten der Informationen;
- Nutzungsbeschränkung der personenbezogenen Daten auf die Zwecke der jeweils in Anspruch genommenen Dienste statt allgemein zu „Telekommunikationszwecken“;
- Ausschluß der Verbindungsdaten von jeglicher Übermittlung;
- gesteigerte Anforderung an die Datensicherung bei allen Diensten;
- Beseitigung des „Zwangseintrags“ für Teilnehmerverzeichnisse auch im Telefondienst;
- Regelung der Verarbeitung von Daten über einzelne Telefonverbindungen, Vergleichszählungen und Feststellen ankommender Wählverbindungen („Fangschaltung“), insbesondere auch bei Funktelefondiensten;
- Angebot eines Dienstes zur Verschlüsselung von Nachrichten;
- Möglichkeit der Gebührenzählung beim Teilnehmer.

Neben diesen Detailanforderungen sind die Datenschutzbeauftragten der Länder der Auffassung, daß auch die Länder Initiativen entwickeln müssen, um im Rahmen ihrer Zuständigkeit nach Möglichkeit einheitliche Regelungen für die (datenschutzfreundliche) Nutzung der über den Datentransport hinausgehenden Dienste zu schaffen. Dies betrifft bereits die Frage, in welchem Umfang die Länder bei der Einführung neuer, nutzungsrelevanter Dienste beteiligt werden müssen (Diensteinführungsentscheidung). Ist die Entscheidung für einen bestimmten Dienst gefallen, werden die Länder aufgerufen, im erforderlichen Umfang den Nutzungsbereich zu strukturieren. Ein bereits praktiziertes Beispiel ist neben dem Btx-Staatsvertrag die im Berliner Kabelpilotprojektgesetz verankerte Nutzungsregelung zur Einführung von Fernwirkdiensten.

4. Weitere Fragen aus der Kontroll- und Beratungspraxis

4.1 Besondere organisatorische und technische Fragen

Personalcomputer

Im Vorjahr habe ich die Problematik des Einsatzes von Personalcomputern ausführlich erörtert. Mit den „Grundsätzen zum Datenschutz bei isolierten Rechnern und Personalcomputern“ habe ich nunmehr den Anwendern solcher Techniken einen Leitfaden in die Hand gegeben, mit dessen Hilfe der Einsatz von Personalcomputern datenschutzgerecht organisiert werden kann. Es deutet sich an, daß der Schwerpunkt der datenschutzbezogenen Probleme beim Personalcomputer-Einsatz in der Einhaltung der Grundsätze zur ordnungsgemäßen Datenverarbeitung liegen wird, deren Bedeutung vor allem bei Stellen leicht unterschätzt wird, die erstmalig die Gelegenheit zur Automatisierung von In-

¹⁾ Siehe Anlage 3

formationsverarbeitung ergreifen. Disketten mit Betriebs- und Anwendungssoftware sind in vielen Kaufhäusern erhältlich, leicht austauschbar und können beliebig in Personalcomputerverfahren eingebracht werden. Benutzer können auf dem heimischen Personalcomputer leicht Programmänderungen oder Neuprogrammierungen durchführen und dann im dienstlichen Rahmen einsetzen. Dies wirft zumindest bei personenbezogenen ADV-Anwendungen für die Abwicklung öffentlicher Aufgaben Probleme auf, für die zuvor eine wirksame Lösung gefunden werden muß. Ich habe in meinen Grundsätzen auch hierfür Lösungsansätze entwickelt und werde bei personenbezogenen PC-Anwendungen schwerpunktmäßig diese Problemstellungen überprüfen.

Erfreulicherweise wurden die „PC-Grundsätze“ von den für die ADV-Planung zuständigen Gremien und Stellen der Berliner Verwaltung akzeptiert. Die Koordinierungsgruppe ADV hat inzwischen deren Anwendung empfohlen¹⁾.

Personalverwaltungssystem der Technischen Universität

Die Technische Universität plant die Einführung eines neuen Personalverwaltungssystems PSA, welches zwar personalvertretungsrechtliche, aber wegen der zuvor erfolgten Überprüfung durch meine baden-württembergische Kollegin kaum noch datenschutzrechtliche Fragen aufwarf. Problematisch war dagegen, ob es hinsichtlich der Sicherung vor unbefugtem Zugriff hingenommen werden könne, das System auf einem vorhandenen Rechner im Rechenzentrum der Technischen Universität Berlin anzusiedeln. Der gleiche Rechner sollte nämlich weiterhin trotz möglicher Kapazitätsengpässe für den freien und unbeschränkten Zugang zum Teilnehmerbetrieb für Forschungs- und Unterrichtszwecke der Technischen Universität und einiger Schulen offenbleiben. Ich habe empfohlen, für das Personalverwaltungssystem einen eigens für Verwaltungsaufgaben der Technischen Universität Berlin gewidmeten Rechner einzusetzen. Dabei war für mich folgende Argumentation ausschlaggebend:

Bei Anwendern im Teilnehmerstatus, die trotz wirkungsvoller Datenschutzsoftware die Möglichkeiten des Betriebssystems flexibel nutzen können, ist bei entsprechender Fachkenntnis nicht auszuschließen, daß diesen unbefugte Zugriffe auf das PSA-Verfahren gelingen. Die erforderliche Fachkenntnis vieler Teilnehmer am System ist aber anzunehmen, wenn man bedenkt, daß auch Studenten und sonstige Angehörige des Fachbereichs Informatik der Technischen Universität Berlin dazugehören. Hinzu kommt, daß das System heftig umstritten ist.

Einsatz des Synchronknotens SK 12 in Datennetzen

Zur Übertragung von Daten von einer Zentrale auf Datenendgeräte wird sehr häufig der Synchronknoten SK 12 als Schnittstellenvervielfacher in Datennetzen eingesetzt. Die von der Zentrale kommenden und für ein bestimmtes Endgerät bestimmten Signalen werden von dem SK 12 aus auf alle von ihm zu Endgeräten gehenden Leitungen gegeben. Erst das Endgerät selektiert die Signale und macht die Daten sichtbar, die für das Endgerät bestimmt sind.

Aufgrund eines aufgedeckten Datenmißbrauchs in einem anderen Bundesland bin ich auf ein Datenschutzproblem beim Einsatz des sehr verbreiteten Synchronknotens SK 12 in Datennetzen hingewiesen worden. Bei entsprechender Manipulation der Endgeräte ist es möglich, den für andere Endgeräte vorgesehenen Datenverkehr sichtbar zu machen. Aufgrund dieser Erfahrung haben die Datenschutzbeauftragten in Bund und Ländern grundlegende Bedenken zum Einsatz des Synchronknotens SK 12 geltend gemacht.

Meine Umfrage bei Netzbetreibern in der Berliner Verwaltung ergab, daß weder beim Polizeipräsidenten noch im Bereich des Landesamtes für Elektronische Datenverarbeitung der SK 12 eingesetzt wurde, daß sich jedoch das Landesamt für Elektronische Datenverarbeitung im Rahmen der Ausschreibung des neuen Verwaltungsnetzes auch mit Angeboten auseinanderzusetzen hatte, die den Einsatz des SK 12 vorsahen. Allerdings sollten die

Endgeräte nicht unmittelbar hinter den SK 12 geschaltet werden. Es sollte vielmehr stets eine intelligente Mehrfachsteuerung zwischengeschaltet werden, die die Selektion und gezielte Weiterleitung der ankommenden Signale übernimmt. Da hierbei nicht das für Manipulationen leicht zugängliche Datenendgerät, sondern die physisch abschottbaren Mehrfachsteuerungen Gefahrenpunkte sind, habe ich meine Bedenken zurückgestellt. Die mittlerweile getroffene Auswahlentscheidung für das neue Verwaltungsnetz sieht den Einsatz des SK 12 nicht mehr vor, bis zur Realisierung des neuen Netzes war jedoch vorübergehend der Einsatz des SK 12 mit dahintergeschalteter physisch abgeschotteter Mehrfachsteuerung erforderlich. Dies habe ich als vertretbar angesehen.

Fernwartung bei medizinischen Systemen

Eine Klinik der Freien Universität Berlin hat mich zur Beratung bei der Einführung eines neuen ADV-Systems zur Patienten-datenverwaltung und -abrechnung hinzugezogen. Eine alle Aspekte umfassende Stellungnahme konnte ich zum derzeitigen Planungsstand noch nicht abgeben. Jedoch fiel bei erster Durchsicht auf, daß bei dem ausgewählten ADV-System Fernwartung eingesetzt werden sollte, bei der die Übertragung personenbezogener Daten, die der medizinischen Schweigepflicht unterliegen, in die Wartungszentren des Herstellers nicht ausgeschlossen werden konnte. Dieser wies lediglich darauf hin, daß seine Techniker in geeigneter Weise auf den Datenschutz verpflichtet worden seien.

Einerseits ist die Fernwartung eine verbreitete und kostengünstige, wenngleich auch aus Servicegründen nicht unumstrittene Dienstleistung der Hersteller zur Verbesserung der Systemverfügbarkeit. Aus datenschutzrechtlicher Sicht ist allerdings die zumindest bei der Software-Fernwartung nicht auszuschließende Offenbarung personenbezogener Daten problematisch: Zwar kann nach den Datenschutzgesetzen eine Weitergabe personenbezogener Daten im Rahmen einer Auftragsdatenverarbeitung erfolgen, damit ist die Fernwartung grundsätzlich zulässig, wenn der Hersteller überprüfbare Zusicherungen für den Datenschutz machen kann und gewisse Mindestbedingungen während der Fernwartung eingehalten werden. Die abschließend aufgeführten Offenbarungstatbestände bei medizinischen Daten im Landeskrankenhausesgesetz sowie in der Berufsordnung der Ärztekammer Berlin sehen eine solche Offenbarung jedoch nicht vor. Mit Fug und Recht wird den medizinischen Daten ein höherwertiger Schutz vor Offenbarung gegenüber Dritten eingeräumt. Ich habe daher eine Reihe von einschränkenden Maßnahmen bei der Durchführung der Fernwartung empfohlen, die aufgrund der Fernwartungskonzeption des betroffenen Herstellers realisierbar sind:

- Es ist sicherzustellen, daß die einschlägigen Empfehlungen zu den „technischen und organisatorischen Datensicherungsmaßnahmen bei Wartung und Fernwartung von DV-Systemen“, die in meinem letzten Jahresbericht²⁾ veröffentlicht wurden, umgesetzt werden;
- es ist ferner sicherzustellen, daß der Kommunikationspartner bei der Fernwartung stets die Betreuungszentrale des Herstellers ist;
- bei der vorgesehenen Fernwartung ist sicherzustellen, daß ein Zugriff auf besonders sensible Datenbereiche ausgeschlossen ist. Ist dies nicht möglich, weil etwa gerade ein Fehler zu prüfen ist, der den Zugriff auf diesen Datenbereich betrifft, so hat die Fernwartung zu unterbleiben und die Wartung hat in üblicher Weise vor Ort stattzufinden;
- die Protokolle des Bildschirmdialogs, die bei dem Hersteller anfallen, sind grundsätzlich anzufordern und zu überprüfen.

Sicherung von Akten und Karteien

Bei fast allen systematischen Überprüfungen, insbesondere in den Bezirken, hatte ich - wie in früheren Jahresberichten mehr-

¹⁾ Vgl. Rundschreiben des Senators für Inneres VI Nr. 74/1986 vom 8. Oktober 1986

²⁾ Anlage 7

fach erwähnt - die unzulängliche Unterbringung sensibler manueller Datensammlungen (Akten, Karteien) bemängelt.

Im Rahmen der Sitzungen der bezirklichen Kontaktpersonen für den Datenschutz, an denen ich regelmäßig teilnehme, wurde in diesem Zusammenhang das Ausschreibungsverfahren für Büromöbel seitens des Landesverwaltungsamtes kritisiert, vor allem wurde darauf hingewiesen, daß bei Aktenschränken und Schreibtischen keine Sicherheitsschlösser gefordert werden.

Daher bin ich an das Landesverwaltungsamt mit der Bitte herangetreten, bei den künftigen Ausschreibungen Sicherheitsschlösser als Mindeststandard vorzusehen.

Das Landesverwaltungsamt teilte mir mit, daß nunmehr derartige Büromöbel serienmäßig mit Stangensicherheits- bzw. Zylinderschloß geliefert werden. Ich habe die Bezirksämter von dieser Absicht des Landesverwaltungsamtes unterrichtet und werde bei den folgenden Bezirksamtsprüfungen untersuchen, inwieweit sich die neue Ausschreibungspraxis des Landesverwaltungsamtes auf die Ausstattung der Bezirksämter auswirkt.

Fotomechanische Ausleihverbuchung in Bibliotheken

In einer Eingabe wandte sich ein Bürger gegen die fotomechanische Ausleihverbuchung der Stadtbüchereien. Die Überprüfung ergab, daß in millionenfacher Anzahl die Daten von Ausleihvorgängen auf Filmrollen festgehalten und gespeichert wurden. Pro Jahr werden auf diese Weise ca. 12 Millionen Ausleihvorgänge fotomechanisch erfaßt. Die durch dieses Verfahren festgehaltenen Datensätze werden seit Jahren gespeichert, weil die zuständigen Stellen von der Auffassung ausgehen, daß es erforderlich sei, all diese Daten präsent zu haben, um bei einem einzelnen Ausleihvorgang die Begründetheit von Regreßansprüchen nachzuweisen.

Ich habe dieses beanstandet. Daten der Bibliotheksbenutzer, die sich an die Benutzungsordnung halten, dürfen nicht zweckentfremdet werden, um gegen Benutzer vorzugehen, die die Benutzungsordnung mißachten. Daher habe ich die Vernichtung der Filmrollen empfohlen. Es sollen nur noch die Daten derjenigen Bibliotheksbenutzer aufbewahrt werden, die zur Abwicklung des Benutzungsverhältnisses erforderlich sind. Da die Filmrollen mit dem fotomechanischen Ausleihbeleg nur mit Einwilligung der betroffenen Benutzer einem Gericht vorgelegt werden dürfen, sind diese ohnehin praktisch in einem gerichtlichen Beweisverfahren nicht verwendungsfähig.

4.2 Öffentliche Sicherheit und Strafverfolgung

Gesetzgebung

Zu den verabschiedeten Sicherheitsgesetzen - insbesondere dem Zweiten Gesetz zur Änderung personalausweisrechtlicher Vorschriften - habe ich oben Stellung genommen. Die übrigen Gesetze wurden zurückgestellt und sollen in der nächsten Legislaturperiode des Bundestages erneut beraten werden.

Die in dem „Siebenerpaket“ nicht enthaltenen Vorstellungen der Innenverwaltungen zum Polizeirecht werden derzeit ebenfalls nicht weiterentwickelt: Die Innenministerkonferenz nahm zu Beginn des Jahres einen Entwurf des Arbeitskreises II zur entsprechenden Änderung des Musterentwurfs für ein einheitliches Polizeigesetz zur Kenntnis, erteilte aber dann den Auftrag, zunächst eine Abstimmung mit den Justizverwaltungen über die geplanten Änderungen der Strafprozeßordnung vorzunehmen.

Ich habe gegenüber dem Innensenator die Auffassung vertreten, daß in Berlin durchaus schon jetzt Überlegungen angestellt werden könnten, auf welche Weise das Berliner Polizeirecht an die neue verfassungsrechtliche Situation angepaßt werden kann. Da hier eine Reihe von Sonderproblemen zu lösen ist (z. B. die Frage des Zusammenhangs zwischen Ordnungsverwaltung und Polizeivollzugsdienst im derzeit geltenden einheitlichen Allgemeinen Sicherheits- und Ordnungsgesetz), könnten ohne weiteres bereits jetzt entsprechende Vorarbeiten beginnen. Dies ist umso leichter möglich, als aufgrund der Beratungen in der Innenministerkonferenz der Regelungsspielraum, der den Innenverwaltungen zur Verfügung steht, bekannt ist.

Informationssystem für Verbrechensbekämpfung

Mit dem Polizeipräsidenten wurde die Erörterung der im Vorjahr vorgenommenen Prüfung des Informationssystems für Verbrechensbekämpfung (ISVB) fortgesetzt. Folgende Maßnahmen sind nachzutragen:

- Von den Datensätzen aller Personen, die zum Zeitpunkt der Eingabe in das ISVB Tatverdächtige oder Betroffene, **Kinder oder Jugendliche** waren, hat der Polizeipräsident den von mir erbetenen Listenausdruck erstellt. Danach sind die Kriminalakten überprüft und zum weitaus überwiegenden Teil vernichtet worden. Die restlichen Kriminalakten wurden mit Lösungsfristen zur Wiedervorlage versehen;
- für die Übermittlung von Daten im INPOL-Verbund über das Gebiet der DDR wird ein **Verschlüsselungsgerät** durch das Bundeskriminalamt beschafft;
- die von mir empfohlene **Nachdokumentation** soll spätestens mit Abschluß der Umstellungsarbeiten des ISVB auf ein neues Betriebssystem dem aktuellen Stand entsprechen;
- der Senator für Inneres hat den Polizeipräsidenten gebeten, mit dem Senator für Justiz und Bundesangelegenheiten ein automatisiertes **Rückmeldeverfahren** über den Ausgang von Strafverfahren bis Mitte 1987 zu ermöglichen. Wegen der Personalsituation beim Polizeipräsidenten wurde diese Frist auf 1988 hinausgeschoben;
- über die Notwendigkeit der Speicherung **personengebundener Hinweise** und den Umfang der Zugriffsmöglichkeiten auf diese Daten (insbesondere hinsichtlich des Merkmals „Suizidgefahr“) wird derzeit in der Innenministerkonferenz beraten. Der Polizeipräsident sieht sich nicht in der Lage, losgelöst von etwaigen Ergebnissen dieser Diskussion eigene Regelungen zu schaffen.

Der personengebundene Hinweis „Freitodgefahr“ spielte eine entscheidende Rolle in einem Strafverfahren, bei dem zum wiederholten Male der **unbefugte Abruf von Daten** aus dem ISVB durch einen Polizeibeamten zu verhandeln war: Der Beamte hatte sich Erkenntnisse über Mitbewohner, mit denen er im Streit lag, verschafft und weitergegeben. So teilte er mit, daß der Sohn der Nachbarin freitodgefährdet sei. Das Gericht verhängte eine spürbare Geldstrafe.

Nachzutragen ist ferner der Ausgang eines von mir geschilderten Falles des unbefugten Abrufs personenbezogener Daten aus dem ISVB durch einen Polizeibeamten¹⁾: Zwar hatte in diesem Fall die Beschwerdeführerin keinen Strafantrag gestellt und das Verfahren mußte demnach gem. § 170 Abs. 2 StPO eingestellt werden. Gleichwohl hat der Polizeipräsident ein förmliches Disziplinarverfahren eingeleitet, das mit dem Ausspruch einer Gehaltskürzung für den Polizeibeamten endete.

Ich habe gegenüber dem Polizeipräsidenten nochmals klargestellt, daß der Abruf personenbezogener Daten zu privaten Zwecken einen erheblichen datenschutzrechtlichen Mangel darstellt, dem mit allen zur Verfügung stehenden Mitteln entgegenzuwirken muß. Die von mir bei der ISVB-Prüfung vorgeschlagene Protokollierung des Abfragegrundes kann hier einen wichtigen Beitrag leisten.

Da die Fraktionen der CDU und der F.D.P. im Abgeordnetenhaus einen **Entschließungsantrag** über automatisierte Datenverarbeitung bei der Polizei eingebracht haben, der einvernehmlich beschlossen wurde, ist der Senat aufgerufen, zu den Hauptproblemen des Prüfberichts abschließend Stellung zu nehmen.

Abgesehen von eigenen Detailproblemen bleiben noch folgende grundsätzliche Fragen ungeklärt:

1. Die für eine ordnungsgemäße Fortentwicklung und Durchführung des ISVB-Verfahrens notwendige **Funktionentrennung** zwischen technisch verantwortlichen DV-Entwicklern und -Planern einerseits und den fachlich verantwortlichen DV-Anwendern andererseits ist nach wie vor nicht transparent organisiert. Eine Organisationsanweisung, die dieses regeln könnte, liegt trotz der Zusage des Polizeipräsidenten, die Transparenz zu verbessern, immer noch nicht vor. Eine

¹⁾ Jahresberichte 1983, Ziff. 2.5; 1985, Ziff. 2.3

formale Regelung des Freigabeverfahrens für neue ADV-Programme hält der Polizeipräsident für entbehrlich, da er im Gegensatz zu mir keine Probleme darin sieht, wenn die Zweckmäßigkeit der ADV für die Aufgaben der Polizei von Seiten der DV-Fachleute beurteilt wird.

2. Es wird nach wie vor von mir für problematisch gehalten, daß Verdächtige, Anzeigende und Geschädigte sowie andere von polizeilichen Maßnahmen Betroffene unter gleichem Datensatzaufbau in der gleichen Datei des ISVB gespeichert werden. Zwar lassen sich die Datensätze durch zusätzliche Merkmale unterscheiden, jedoch kann die Vermengung der Daten dieser unterschiedlichen Personenkreise im Einsatzfall zu Fehleinschätzungen führen.

Neue Verfahren

Der Einsatz moderner ADV-Verfahren im Rahmen der Verbrechensbekämpfung machte weitere Fortschritte, die allerdings auch im Hinblick auf die bevorstehende Novellierung des Polizeirechts nicht unkritisch betrachtet werden dürfen.

Im Vordergrund steht hier eine Neukonzeption des **Rechnernetzes**.

Neben dem Aufbau eines neuen Netzes mit reiner Transportfunktion sollen die verschiedenen polizeilichen Systeme so vereinheitlicht werden, daß künftig von jedem Datenendgerät eines Teilnetzes auf jedes an das Netz angeschlossene DV-System mit gleicher Technik zugegriffen werden kann und gleichartige Auskünfte zur Verfügung gestellt werden. Bisher waren neben den Terminals des ISVB andere Terminals ständig und ausschließlich direkt mit dem Rechner des BKA in Wiesbaden verbunden. Für die Datenbestände des Einwohner- oder Kfz-Zulassungswesens konnten nur Terminals dieser Verfahren benutzt werden. Deshalb wurde das vorhandene Terminalnetz des ISVB durch ein von einzelnen Verarbeitungsrechnern unabhängiges Netz mit moderner Technologie ersetzt. Das neue Netz soll so gestaltet sein, daß vom Netz aus Verbindungen zu den ADV-Anlagen des ISVB, des INPOL, des Berliner Einwohner- und des Kfz-Zulassungswesens aufgebaut werden können. Unbeschadet der Zugriffsbefugnisse für jedes zum Netz gehörende Endgerät soll prinzipiell die technische Zugriffsmöglichkeit auf alle an das Netz anzubindenden DV-Systeme bestehen. Die jetzt in Betrieb genommenen 140 Bildschirmarbeitsplätze sollen zudem durch die entsprechende „Intelligenz“ des Datenerfassungsplatzes eine Datenvorverarbeitung (feldweise Bedienerführung, Plausibilitätsprüfungen, Feldunabhängigkeitsprüfungen usw.) ermöglichen.

Ich habe darauf hingewiesen, daß der On-line-Zugriff der Polizei auf Datenbestände anderer Behörden einer eindeutigen Rechtsgrundlage bedarf.

Seit einiger Zeit nutzt der Polizeipräsident die vom Bundeskriminalamt angebotene Möglichkeit, sogenannte **Spurendokumentations-Systeme (SPUDOK)** zu betreiben. Im Gegensatz zu dem ISVB, bei dem die neben der Vorgangsverwaltung nur relativ wenige, den Tathergang sowie die Tatverdächtigen beschreibende Merkmale verarbeitet werden, dienen SPUDOK dazu, die verschiedensten, bei umfangreichen Ermittlungen anfallenden Hinweise und Erkenntnisse (Spuren) zu registrieren und nach bestimmten Merkmalen auszuwerten.

Ein derartiges SPUDOK wird vom Polizeipräsidenten dazu genutzt, Erkenntnisse über Personen, Sachen und der Sachaufklärung dienende Umstände zur Bekämpfung der organisierten Kriminalität insbesondere im Baubereich zu sammeln (SPUDOK Lietze). Ein Petent hatte sich bei mir darüber beschwert, daß in dieser Datei Daten eingespeichert seien, die bei Durchsuchungen ermittelt worden waren. Der Petent behauptete, mit dem Ermittlungskomplex nichts zu tun zu haben. Bei der Überprüfung bestätigte sich, daß Daten über die steuerlichen und finanziellen Verhältnisse des Petenten in den Ermittlungsakten enthalten sind. Ein Teil dieser Daten wurde in das SPUDOK übernommen.

Ich habe den Petenten darauf hingewiesen, daß die Behörden der Polizei bzw. der Staatsanwaltschaft nach den Vorschriften der Strafprozeßordnung verpflichtet seien, strafbare Sachverhalte umfassend aufzuklären. Da bei Einleitung solcher Ermittlungen naturgemäß nicht absehbar ist, welche Angaben im Ergebnis für

ein eventuelles Strafverfahren wichtig sein werden, fallen auch häufig Daten von Personen an, die nur indirekt am Sachverhalt beteiligt sind. Gerade im Bereich der organisierten Kriminalität kann es zur Sachaufklärung erforderlich sein, neue technische Hilfsmittel zur Auswertung einzusetzen; grundsätzliche Einwendungen gegen die Errichtung derartiger Dateien sind deshalb nicht zu erheben. Gleichwohl ist die Speicherung personenbezogener Daten von „anderen Personen“ (also nicht Tatverdächtige oder Opfer) ein Sachverhalt, der in den künftigen Polizeigesetzen sachgerecht geregelt werden muß. Mehrfach habe ich darauf hingewiesen, daß der Umfang der Automatisierung ebenfalls durch Gesetz beschrieben werden muß.

Neben dem Einsatz zentraler Datenverarbeitungsanlagen stehen erste Versuche, **Personalcomputer** bei der Aufklärung von Straftaten einzusetzen. Auch hier tauchen die angesprochenen Probleme auf: So setzt der Polizeipräsident seit einigen Monaten einen Personalcomputer bei der Aufklärung von Hehlereitbeständen ein. Das Gerät ermöglicht die Registrierung und Zusammenführung verschiedenster Merkmale, die Indizien für Hehlerei darstellen (z. B. bestimmte Zeitschriftenanzeigen, Örtlichkeiten, die für derartige Straftaten bekannt sind). Auch bei dieser Anwendung fallen eine Vielzahl von Daten an, die in keinem Zusammenhang mit Straftaten stehen und bei denen sich der Anfangsverdacht nicht erhärtet. Derartige Anwendungen sind nicht von vornherein unzulässig, ich halte aber auch hier Anlaß und Umfang des Einsatzes derartiger Verfahren für regelungsbedürftig. Im Rahmen der mir zugewiesenen Aufgaben (§21 Abs. 2 Satz 3 Berliner Datenschutzgesetz) werde ich diese Entwicklung intensiv beobachten.

Einzelfälle

Die folgende Beschwerde zeigt exemplarisch, wie angesichts des Umfangs der polizeilichen Datenverarbeitung und ihrer Verknüpfung mit anderen Verwaltungsbereichen vage Beschuldigungen einen scheinbar objektiven Charakter annehmen und ein falsches Bild des Betroffenen erzeugen. Es soll daher ausführlich dargestellt werden, wie beim Einsatz moderner Informationstechnik **Risiken für Bürger** entstehen können.

Der Polizeipräsident erhielt ein anonymes Schreiben, in dem ohne weitere Ausführungen behauptet wurde, die Petentin hole ständig **Rauschgift** aus dem Ausland. Dieses Schreiben wurde zum Anlaß genommen, Observations- und Fahndungsmaßnahmen einzuleiten. Der Umstand, daß die Petentin, die im Ausland studiert, mehrfach beim Grenzübertritt eingehenden Kontrollen unterzogen wurde, war Anlaß für die Beschwerde der Petentin. Da die polizeilichen Maßnahmen keinerlei Erkenntnisse erbrachten, wurden die Ermittlungen durch die Staatsanwaltschaft eingestellt. Die Einstellung wurde dem Polizeipräsidenten, dem Senator für Gesundheit und Soziales, dem Bundeskriminalamt, dem Bundesgesundheitsamt - Bundesopiumstelle -, dem Hauptzollamt Berlin Süd sowie dem Zollfahndungsamt Berlin mitgeteilt. Soweit es sich bei den Adressaten um Berliner Stellen handelte, habe ich selbst eine Überprüfung vorgenommen; bei den anderen Dienststellen habe ich den Bundesbeauftragten für den Datenschutz um entsprechende Nachforschungen gebeten.

Danach ergab sich, daß die in dem anonymen Schreiben enthaltenen Behauptungen, die durch keinerlei sachliche Feststellungen gestützt werden konnten, zur Speicherung folgender personenbezogener Daten geführt haben, ohne daß diese aufgrund des Ermittlungsergebnisses gelöscht oder wenigstens gesperrt worden sind.

Kurz nach Eingang des Schreibens wurden personenbezogene Daten über die Petentin als verdächtige Person im ISVB eingespeichert. Unter anderem wurde als Tatzeitpunkt das Datum des Eingangs des anonymen Schreibens erfaßt, unter statistischen Angaben das Merkmal „Dringender Verdacht“. Daten über die Fahndungsausschreibung konnten nicht mehr rekonstruiert werden.

In den INPOL-Verbunddateien wurden entsprechend den bundesweiten Vereinbarungen ebenfalls Daten gespeichert:

Auf der Leitseite, auf die jeder INPOL-Berechtigte Zugriff hat, wurde registriert, daß folgende Daten vorhanden sind: Recht-mäßige Personalien, Alias-Personalien, Einstellung in den KAN

(zentraler Kriminalaktennachweis), Zentraldatei (alle in INPOL erfaßten Personen) sowie Hinweis, daß eine Eintragung in der Falldatei Rauschgift vorhanden ist. In der Verbunddatei „Falldatei Rauschgift“, in die angeblich nur aufgeklärte und abgeschlossene Fälle eingetragen werden, wurde wiederum als Tatzeitpunkt das Eingangsdatum des Schreibens erfaßt sowie folgender Text: „In einem anonymen Schreiben wird ... beschuldigt, RG aus dem Ausland einzuschmuggeln. Weitere Einzelheiten darüber wurden im Brief nicht mitgeteilt“. In die Datei PIOS-Rauschgift, die als eigenständige Verbunddatei geführt wird, wurde als Freitext eingegeben: „Bezugsperson soll RG ... einschmuggeln. Über die dabei verwendeten Verkehrsmittel sowie die Reiserouten ist nichts bekannt“.

Die Mitteilung der Staatsanwaltschaft über die Einstellung des Verfahrens, die diesmal ausnahmsweise erfolgte, führte weder zu einer Überprüfung der Rechtmäßigkeit der weiteren Speicherung der Daten noch zu einer entsprechenden Ergänzung der Datensätze. Vielmehr wurde die Mitteilung lediglich in einer Kriminalakte abgeheftet. Die Kriminalakte enthielt keinerlei Retenue aus dem hier in Frage stehenden Ermittlungsvorgang, so daß dem Polizeipräsidenten für eine Entscheidung über die weitere Aufbewahrung keinerlei Unterlagen mehr zur Verfügung standen. Insbesondere war der Kriminalakte nicht zu entnehmen, daß die Ermittlungen lediglich aufgrund eines anonymen Hinweises erfolgten und sich laut abschließendem Vermerk des Sachbearbeiters in der Ermittlungsgruppe Rauschgift keinerlei Hinweise ergaben, die den Tatverdacht erhärtet hätten.

Diese Feststellungen gaben zu folgenden Erwägungen Anlaß:

Der Umstand, daß im ISVB zwar das Merkmal „Dringender Verdacht“, nicht aber die Tatsache gespeichert wurde, daß der Verdacht lediglich auf einem anonymen Schreiben beruht, erweckt ein falsches Bild von der Petentin. Die zusätzliche Angabe des Eingangsdatums des anonymen Schreibens als Tatzeitpunkt (sowohl im ISVB als auch in der INPOL-Falldatei Rauschgift) ist unrichtig und verstärkt den falschen Eindruck.

Die Einspeicherung der Daten in die genannten Verbunddateien stellt eine Übermittlung dieser Daten an das Bundeskriminalamt sowie an alle anderen Landeskriminalämter dar. Die Einstellung eines bestimmten Kennzeichens in die Datei der Grundpersonalien stellt darüber hinaus eine Übermittlung des Merkmals „einer Rauschgiftstraftat verdächtig“ auch an alle Benutzer dar, die zum Zugriff auf die entsprechende Falldatei selbst nicht berechtigt sind.

Soweit hier unvollständige oder falsche Daten übermittelt wurden, sind diese Übermittlungen ebenfalls rechtswidrig, da irreführende Daten auch für die Aufgaben der Polizeibehörden außerhalb Berlins nicht erforderlich sein können.

Nach der Einstellung des Verfahrens durch die Staatsanwaltschaft hätten die Eintragungen in allen Dateien daraufhin überprüft werden müssen, ob ihre weitere Speicherung erforderlich ist (Ziff. 5.4.3 KpS-Richtlinien). Die Tatsache, daß die polizeiliche Kriminalakte mangels Nachweisen eine derartige Entscheidung überhaupt nicht ermöglichte, stellt einen schwerwiegenden Mangel hinsichtlich des Gebots der Ordnungsgemäßheit der Datenverarbeitung dar.

Mangels Berichtigung im ISVB konnte auch die Folgeberichtigung der über die Einspeicherung in die Verbunddateien an die anderen Polizeibehörden vorgenommenen Übermittlungen (§ 14 Abs. 4 Berliner Datenschutzgesetz) nicht vorgenommen werden.

Die Überprüfung, ob bei den Adressaten der staatsanwaltlichen Mitteilungen ebenfalls irreführende Daten gespeichert werden, führte zu einem beruhigenderem Ergebnis: Der Senator für Gesundheit und Soziales hat in der Tat aufgrund der Anordnung über Mitteilungen in Strafsachen (MiStra) eine Nachricht über die Einstellung erhalten. Diese Mitteilungen werden dort allerdings nur anonym ausgewertet und anschließend vernichtet. Dies entspricht meinen Empfehlungen aus früheren Jahren.

Die in derartigen Fällen bereits vom Polizeipräsidenten vorgenommene Übermittlung personenbezogener Daten über tatverdächtige Personen, die vom Senator für Gesundheit und Soziales

zur sozialpsychiatrischen Betreuung vertraulich an das zuständige Bezirksamt weitergeleitet wird, fand in diesem Fall nicht statt.

Die durch den Bundesbeauftragten vorgenommene Überprüfung bei Bundesbehörden ergab, daß die Bundesopiumstelle keinerlei Daten zur Person der Petentin gespeichert hat und auch keine Daten weitergeben konnte. Fraglich ist hier, wieso die MiStra eine Übermittlung in Fällen vorsieht, bei denen die Bundesopiumstelle keine Zuständigkeit besitzt. Die Zollbehörden speichern dagegen die Daten nach wie vor. Über die Speicherdauer bestehen noch Meinungsverschiedenheiten.

Daß ein nicht unerheblicher materieller Schaden durch Übermittlungsfehler entstehen kann, zeigt eine andere Eingabe: Eine Berlinerin unternahm eine **Urlaubsreise nach Indien**. Auf dem Flughafen in Neu Delhi erschien - nach Angaben der Petentin - bei der Paßkontrolle auf einem Bildschirm der Name mit einem Zusatz, der auf eine Mitgliedschaft in einer extremistischen Organisation hindeutete. Ihr wurde daraufhin die Einreise verweigert; konsularischer Schutz konnte ihr nicht gewährt werden, da die deutsche Botschaft zu diesem Zeitpunkt nicht besetzt war. Die Urlaubsreise mußte abgebrochen werden. Intensive Nachprüfungen in den Berliner Systemen führten nicht zu einer Aufklärung, auf welche Weise die indischen Behörden derartige Daten erhalten haben konnten: Die Petentin war in keinem der in Berlin zugänglichen Systeme erfaßt. Die intensive Suche nach Personen, mit denen die Petentin (die einen weitverbreiteten Namen trägt) hätte verwechselt werden können, hat zu keinem Ergebnis geführt, ebenso wenig die Prüfung des Bundesbeauftragten unter Einschaltung des Auswärtigen Amtes. Allein die Tatsache, daß ein derartiger Vorgang nicht aufgeklärt werden kann, zeigt deutlich die Gefahren der Datenstreuung, vor allem aber auch die Erforderlichkeit zwischenstaatlicher Vereinbarungen über gegenseitige Datenschutzkontrollmaßnahmen.

Ein weiterer bedenkenswerter Fall ging bundesweit durch die Presse: Ein Hochschullehrer machte von seinem Recht Gebrauch, beim Polizeipräsidenten um **Auskunft** über die über ihn gespeicherten Daten zu erbitten. Diese Auskunft wurde ihm verweigert. Daraufhin strengte er einen Verwaltungsprozeß an, in dessen Verlauf ihm die Gewährung der Auskunft angeboten wurde. Die Auskunft, die ihm daraufhin gegeben wurde, war dann allerdings die, daß zwischenzeitlich alle vorher vorhandenen Daten über ihn gelöscht worden seien. Diese weniger unter datenschutzrechtlichen, wohl aber unter prozeßrechtlichen Gesichtspunkten problematische Praxis, Daten durch vorzeitige Löschung vor der Überprüfung zu schützen, wurde dadurch relativiert, daß die zuvor in elektronischen Dateien vorhandenen Daten in den Akten noch weiter aufbewahrt wurden. Hieraus wurde schließlich Auskunft erteilt. Dabei zeigte sich, daß bei der Mehrzahl der Daten der Bürger mit seinem Zwilingsbruder verwechselt worden war.

Neben diesen, durch die automatische Datenverarbeitung charakterisierten Fällen waren wiederum auch eine Reihe von Problemen aus dem Bereich traditioneller Datenverarbeitung zu erörtern.

Ein bei der derzeitigen Rechtslage ungeklärtes Problem ist, in welchem Umfang die Vollzugspolizei zur Unterstützung ihrer Ermittlungsarbeit traditionelle Karteien parallel zu Kriminalakten und ADV-Systemen führen darf (**Arbeitskarteien**). Ein erster Schritt zur Aufklärung dieser Frage war dadurch unternommen worden, daß die KpS-Richtlinien im Jahr 1983 um einen Erlaß ergänzt wurden, mit dem für jede manuell geführte Kartei ebenfalls eine Errichtungsanordnung eingeführt wurde. Die Neuerrichtung von Karteien ist dem Senator für Inneres anzuzeigen, bereits existierende Karteien sind festzustellen und anzuordnen. Mitte 1986 legte der Senator für Inneres ein Verzeichnis dieser Karteien vor, das eine Ausgangsbasis für die Überprüfung der Rechtmäßigkeit bieten kann.

Ein deutlicher Rückschlag ist bei der von den KpS-Richtlinien vorgesehenen **Aussonderung von Altakten** eingetreten. Diese Aufgabe wird von einer Arbeitsgruppe wahrgenommen, die sowohl die Überprüfungsfristen festsetzt als auch die Vernichtung in die Wege leitet. Ziel war es, bis zum Jahre 1991 zu erreichen, daß nur noch Akten vorhanden sind, deren Aufbewahrung den Fristen der KpS-Richtlinien entspricht. Die hierzu erforderliche An-

zahl von Mitarbeitern konnte dadurch zur Verfügung gestellt werden, daß die mit den grundsätzlichen Entscheidungen betrauten Kriminalbeamten durch eine Anzahl von ABM-Kräften unterstützt wurden. Diese ohnehin nicht sehr glückliche Lösung mußte Ende Januar beendet werden, weil die zuständigen Senatsverwaltungen für Inneres sowie für Wirtschaft und Arbeit die Weiterbeschäftigung der ABM-Kräfte ablehnten. Zum Einsatz eigener Mitarbeiter war der Polizeipräsident nur in sehr geringem Umfang in der Lage. Derzeit ist eine konsequente Bereinigung des Altaktenbestandes nicht mehr möglich. Diese Situation macht die Einhaltung der KpS-Richtlinien und künftig auch des Polizeirechts, das ebenfalls Lösungsfristen enthalten wird, unmöglich, obwohl es einer der elementaren Grundsätze des Datenschutzrechtes ist, daß Stellen die – überdies sehr sensible – personenbezogene Daten sammeln, auch Vorkehrungen zu deren Löschung bzw. Vernichtung treffen müssen.

Öffentlichkeit und Ermittlungsverfahren

Aus aktuellem Anlaß war wie auch in Vorjahren mehrfach die Frage zu erörtern, in welchem Umfang personenbezogene Daten aus Ermittlungsvorgängen von der Polizei oder der Staatsanwaltschaft an die Öffentlichkeit, insbesondere die Presse weitergegeben werden dürfen.

Die Strafprozeßordnung selbst enthält fast keine Bestimmungen zum Schutz der personenbezogenen Daten; die Richtlinien für das Strafverfahren und das Bußgeldverfahren (RStBV) enthalten hierzu ebenfalls nur wenige unbefriedigende Regelungen und können angesichts ihres Charakters als Verwaltungsvorschriften ohnehin eine gesetzliche Regelung nicht ersetzen.

Ausdrücklich in der Strafprozeßordnung ist die Verpflichtung geregelt, den **Beschuldigten** von der Einstellung eines Ermittlungsverfahrens in Kenntnis zu setzen, wenn dieser als solcher vernommen worden ist, ein Haftbefehl gegen ihn erlassen war, er um einen Bescheid gebeten hat oder wenn ein besonderes Interesse (des Beschuldigten) an der Bekanntgabe ersichtlich ist (§ 170 Abs. 2 StPO).

Gegenüber dem **Verdächtigen** besteht keine Informationspflicht, solange nicht Nachteile durch künftige Maßnahmen zu befürchten sind und dem Verdächtigen (in diesem Zeitpunkt Beschuldigten) ohnehin rechtliches Gehör zu gewähren ist (§ 163 a StPO). Die Zusammenschau der Bestimmungen führt dazu, daß bei Ermittlungsverfahren, in denen sich von vornherein keine Nachteile für den Verdächtigen abzeichnen, weder die Eröffnung noch die Einstellung des Ermittlungsverfahrens dem Betroffenen mitgeteilt werden müssen.

Gegenüber der **Presse** (und dem Rundfunk) besteht auch für Staatsanwaltschaften die Verpflichtung, zur Erfüllung ihrer öffentlichen Aufgabe Auskünfte zu erteilen (§ 4 Abs. 1 Pressegesetz). Diese Verpflichtung ist jedoch in mehrfacher Hinsicht eingeschränkt: Sie setzt eine entsprechende Anfrage voraus (§ 4 Abs. 1 Pressegesetz); Geheimhaltungsinteressen, insbesondere schutzwürdige private Interessen dürfen nicht entgegenstehen (§ 4 Abs. 2 Ziff. 1, 2, 4 Pressegesetz), die sachgerechte Durchführung eines schwebenden Verfahrens darf nicht vereitelt, erschwert, verzögert oder gefährdet werden (§ 4 Abs. 2 Ziff. 3 Pressegesetz).

Da es nach der Rechtsprechung des Bundesverfassungsgerichts keine belanglosen personenbezogenen Daten mehr gibt, ist davon auszugehen, daß § 4 Pressegesetz grundsätzlich unter dem Vorbehalt steht, daß Auskünfte mit personenbezogenen Daten nur dann an die Presse gegeben werden dürfen, wenn Datenschutz- und andere Geheimhaltungsvorschriften durch spezialrechtliche Regelungen verdrängt werden.

Das **Berliner Datenschutzgesetz** enthält zwar einzelne Bestimmungen, die Voraussetzungen für eine befugte Übermittlung personenbezogener Daten trotz des grundsätzlich bestehenden Datengeheimnisses (§ 8 Berliner Datenschutzgesetz) enthalten. Bei der Übermittlung personenbezogener Daten an nichtöffentliche Stellen ist diese Befugnis jedoch an die Einwilligung des Betroffenen gebunden (§ 11 Berliner Datenschutzgesetz).

Wegen der unterschiedlichen Intention (Verfahrensregelung), insbesondere aber wegen der mangelnden Rechtsnormqualität

stellt Ziff. 23 **RStBV** ebenfalls keine Befugnisnorm dar; das gleiche gilt für andere untergesetzliche Regelungen (z. B. Richtlinien des Abgeordnetenhauses in Immunitätsangelegenheiten) oder Verhaltenskodizes (z. B. Pressekodex und Richtlinien des Deutschen Presserats).

Angesichts der fehlenden gesetzlichen Vorschriften muß die Problematik auf **verfassungsrechtlicher** Ebene diskutiert werden. Dabei steht in Frage, ob aus der (positiven) Gewährleistung der Pressefreiheit (Art. 5 GG) Befugnisse zum Eingriff in das informationelle Selbstbestimmungsrecht abgeleitet werden können. Dies ist dann der Fall, wenn die verfassungsrechtlich gebotene Abwägung beider Grundrechte zugunsten des öffentlichen Informationsinteresses ausfällt: Diese im Hinblick auf die vom Bundesverfassungsgericht geforderte Normenklarheit unbefriedigende Situation muß bis zu einer gebotenen gesetzlichen Klärung (z. B. im Rahmen der zu novellierenden Strafprozeßordnung bzw. der Pressegesetze) hingenommen werden.

Die Diskussion in Rechtsprechung und Literatur kreist im wesentlichen um die Frage der Zulässigkeit der Offenbarung – und späteren Veröffentlichung – des Namens des Beschuldigten. Diese Frage muß angesichts der allgemeinen Bedeutung des informationellen Selbstbestimmungsrechts des Beschuldigten ausgedehnt werden auf alle Informationen, die mit dem in der Öffentlichkeit vorhandenen Wissen auf eine Person beziehbare sind (vgl. § 4 Abs. 1 BlnDSG). Unter diesem Vorbehalt ist folgender Diskussionsstand in Rechtsprechung und Literatur erkennbar:

Das Bundesverfassungsgericht gibt in der sogenannten Lebach-Entscheidung¹⁾ weder dem öffentlichen Informationsinteresse noch dem Schutz der betroffenen Person grundsätzlich den Vorrang. Vielmehr wird die Intensität des **Eingriffs in den Persönlichkeitsbereich** gegen das **Informationsinteresse der Öffentlichkeit** abgewogen. Der Einbruch in die persönliche Sphäre darf nicht weitergehen, als eine angemessene Befriedigung des Informationsbedürfnisses des Publikums es erfordert. Nachteile für den Täter müssen im Verhältnis zur Bedeutung der Tat für die Öffentlichkeit stehen. Das Bundesverfassungsgericht räumt der aktuellen Berichterstattung einen hohen Rang ein. Derjenige, der eine schwere Straftat begehe, habe – zumindest im direkten zeitlichen Zusammenhang – sein Recht auf Persönlichkeitsschutz verwirkt.

Das Bundesverfassungsgericht stellt jedoch klar, daß auf der anderen Seite bis zur Beendigung des Verfahrens durch Verurteilung die Unschuldsvermutung gilt.

Für schwebende Verfahren – also solche, die nicht durch Verurteilung beendet worden sind –, zeichnet sich in der Rechtsprechung noch keine Tendenz ab, der Presse ähnlich klare Grenzen zu setzen. Von den Gerichten wird bei schweren Straftaten die Aufdeckung der Anonymität des Betroffenen durchweg für zulässig gehalten. Dabei verallgemeinert die Rechtsprechung den Grundsatz des § 23 Kunsturhebergesetz und unterscheidet zwischen „absoluten“ und „relativen“ **Personen der Zeitgeschichte**: Absoluten Personen der Zeitgeschichte, die im Rampenlicht der Öffentlichkeit stehen, werden Eingriffe, die allenfalls einen kleinen Bereich des Privatlebens auslassen, zugemutet. Nach dieser Rechtsprechung steht im übrigen der Veröffentlichung personenbezogener Daten nichts entgegen. Nur bei relativen Personen der Zeitgeschichte beschränkt sich das überwiegende öffentliche Interesse auf den Sachzusammenhang.

Im Rahmen der Abwägung der Interessen bei einem Ermittlungsverfahren kann dies so nicht gelten. Der Verwirkungsgedanke, der für die wegen einer schweren Straftat Verurteilten gilt, spielt im Ermittlungsverfahren keine Rolle. Dem Beschuldigten des Ermittlungsverfahrens bereits die Tat zuzurechnen, deretwegen gegen ihn ermittelt wird, verbietet der Grundsatz der Unschuldsvermutung. Ermittlungsverfahren enden im Regelfall mit der Einstellung, so daß dem Betroffenen nicht zugemutet werden kann, daß für diese Zeiten sein Persönlichkeitsschutz eingeschränkt wird.

Auch der Grundsatz der **„Öffentlichkeit der Verhandlung“** vermag die Abwägung hier nicht zu Gunsten der Publizität zu ver-

¹⁾ BVerfGE 35, 204

schieben. Die Hauptverhandlung findet erst statt, wenn eine Anklage erhoben worden ist, wenn die Staatsanwaltschaft somit genügend Anhaltspunkte dafür hat, das Verfahren weiterzuführen. Im Ermittlungsverfahren ist die Öffentlichkeit ausgeschlossen. Dies dient auch dem Schutz des Beschuldigten.

Diese Abwägung entspricht den Regelungen in der Strafprozeßordnung: Sie unterscheidet bei Zwangsmaßnahmen während eines Ermittlungsverfahrens zwischen Beschuldigten, Verdächtigen und anderen Personen. Diese Differenzierung stellt sicher, daß ein bloß Verdächtiger nicht gleichen Eingriffen wie ein Beschuldigter ausgesetzt ist. Eingriffe gegen den Verdächtigen eines Ermittlungsverfahrens sind somit in viel engerem Rahmen als gegen einen Beschuldigten zulässig (vgl. z.B. § 81 b StPO, dagegen § 102 StPO).

Allerdings kann die identifizierende Berichterstattung durch ein gesteigertes Interesse der Allgemeinheit gerechtfertigt sein. Das kann der Fall sein, wenn gegen Personen ermittelt wird, die aufgrund ihres demokratisch legitimierten Amtes ein besonderes öffentliches Vertrauen genießen. Hier kann bereits durch den Verdacht einer Straftat das Vertrauen der Öffentlichkeit berührt sein. Der Bürger hat hier ein Recht, zu erfahren, daß Zweifel an der Integrität der Person bestehen können.

Angeichts des jeder Person zustehenden informationellen Selbstbestimmungsrechts darf jedoch auch dieser Personenkreis nicht schutzlos einem vermeintlichen öffentlichen Interesse ausgeliefert sein, vielmehr ist hier ebenfalls abzuwägen: Auch wer im Rampenlicht der Öffentlichkeit steht, hat einen Anspruch darauf, daß nicht alles und jedes in der Presse erscheint, sondern vielmehr die Eingriffsintensität in einem ausgeglichenen Verhältnis zum Informationsbedürfnis der Öffentlichkeit steht.

Etwas anderes gilt, wenn die in der Öffentlichkeit vorhandenen Informationen gerade eine Richtigstellung fordern.

Nach der Einstellung des Ermittlungsverfahrens ist eine identifizierende Berichterstattung nicht mehr zulässig. Mit der Verfahrenseinstellung nämlich verliert der Betroffene die Eigenschaft als Beschuldigter; er hat als unschuldig zu gelten.

Im **Ergebnis** müssen die Strafverfolgungsbehörden bei der Frage nach der Befugnis zur Offenbarung personenbezogener Daten die für die Veröffentlichung erforderliche Abwägung vorwegnehmen. Klare Kriterien hierfür sind kaum entwickelt.

Presse und Rundfunk selbst werden in den Datenschutzgesetzen hinsichtlich der publizistischen Daten privilegiert (Presse: § 1 Abs. 3 Bundesdatenschutzgesetz; Rundfunk: § 3 Abs. 4 Berliner Datenschutzgesetz). Sie unterliegen keinen materiellen Beschränkungen durch die Datenschutzgesetze.

Vielmehr wird unmittelbar auf die Persönlichkeitsrechte der Betroffenen abzustellen sein. Zu berücksichtigen ist vor allem, daß die Presse zwar bei der Offenbarung personenbezogener Daten durch die Justizbehörden auf die Zulässigkeit auch der Publikation vertrauen kann, aber auch zu einer ausgewogenen fairen Berichterstattung verpflichtet ist¹⁾.

Einen ersten Schritt zur Regelung des Verfahrens hat der Saarländische Minister der Justiz in einer allgemeinen Verfügung zur Informationserteilung an Presse und Rundfunk unternommen²⁾.

4.3 Personalwesen

Nachdem ich in meinem letzten Jahresbericht auf die Schwierigkeiten verwiesen hatte, die der Umgang mit Personaldaten öffentlicher Bediensteter für den Datenschutz, insbesondere aber auch für die Überprüfung der Einhaltung datenschutzrechtlicher Vorschriften aufwirft, nahm sich der Unterausschuß „Berichte des Berliner Datenschutzbeauftragten“ des Ausschusses für Inneres, Sicherheit und Ordnung im Abgeordnetenhaus der Problematik an. Gegenüber der Stellungnahme des Senats zu meinem Jahresbericht, in der dieser eine noch restriktivere Haltung angekündigt hatte, forderte der Unterausschuß, daß künftig die Zusammenarbeit zwischen der Verwaltung und dem Datenschutzbeauftragten ohne Restriktionen verläuft. Insbesondere er-

wartet der Ausschuß, daß der Senat so schnell wie möglich die notwendige Verwaltungsvorschrift über die Führung von Personalakten erlasse. Seither ist eine spürbar bessere Unterstützung meiner Tätigkeit in diesem Bereich zu beobachten.

Personalaktenführung

Als ersten Schritt zu einer Verbesserung der Rechtslage hat der Senator für Inneres erneut einen Vorstoß zum Erlaß von Verwaltungsvorschriften über die Führung von Personalakten der Dienstkräfte des Landes Berlin unternommen. Zwar sollen die Arbeitsergebnisse einer interministeriellen Arbeitsgruppe auf Bundesebene abgewartet werden, die ihre Ergebnisse in diesen Tagen bekanntgeben will. Der Senator für Inneres hat jedoch angekündigt, daß er die im Entwurf enthaltenen Bestimmungen über Inhalt und Gliederung der Personalakte vorab in Kraft setzen will.

Die Vorwegnahme dieser Bestimmungen würde eine Verbesserung des Datenschutzes mit sich bringen: Die Festlegung bestimmter Unterlagen, die nicht Bestandteil der Personalakte sind (z.B. Vorgänge zu Stellenbesetzungen oder Beschwerden), als Sachakten sowie die gesonderte Führung von materiell zur Personalakte gehörigen, aber getrennt zu führenden Beilagen (z.B. zu Beihilfen, Nebentätigkeiten, finanziellen Forderungen gegen den Bediensteten) verhindern, daß die darin enthaltenen Daten bei der Einsicht in Personalakten durch Dritte (z.B. bei Bewerbungen) mitübermittelt werden. Daß dies bisher nicht gewährleistet ist, war häufig Gegenstand von Beschwerden.

Der Entwurf von Verwaltungsvorschriften darf allerdings nicht darüber hinwegtäuschen, daß – wie von mir früher mehrfach gefordert – die Grundlagen für die Verarbeitung von Personaldaten im Recht des öffentlichen Dienstes (Beamten- und Tarifrecht) angemessen geregelt werden müssen. Ich gehe davon aus, daß die Datenschutzbeauftragten bei der Entwicklung der entsprechenden Vorschriften hinreichend beteiligt werden.

Personalinformationssysteme

Gerade bei der Personaldatenverarbeitung ist ein starker Trend zum Einsatz automatisierter Systeme zu beobachten. Im Mittelpunkt der öffentlichen Diskussion steht der Begriff der „Personalinformationssysteme“.

Dabei ist festzustellen, daß dieser Begriff häufig dafür mißbraucht wird, jegliche Verarbeitung von Personaldaten als prinzipiell gefährlich darzustellen. Andererseits wird dem der verharmlosende Begriff des „Personaldateisystems“ entgegengehalten.

Nach meiner Auffassung kann von einem Personalinformationssystem nur die Rede sein, wenn nicht nur Daten zur Personalabrechnung und Personalverwaltung (z.B. Stellenplan, Geschäftsverteilung, Daten, die zum Vollzug gesetzlicher Bestimmungen erforderlich sind) – **administrative Daten** –, sondern zusätzlich Daten verarbeitet werden, die im Sinne eines Soll/Ist-Vergleichs Wertungen über Mitarbeiter enthalten – **dispositive Daten** –. Darüber hinaus ist mit dem Begriff Personalinformationssystem impliziert, daß es sich um ein Informationssystem handelt, bei dem weitgehende Verknüpfungs- und Auswertungsmöglichkeiten bestehen, die über die reine Dateiabfrage oder sequentielle Auswertung hinausgehen. So definiert, entspricht der Begriff in etwa dem Spektrum von Systemen zur automatisierten Verarbeitung von Personaldaten, deren Einführung das Bundesarbeitsgericht unter dem Aspekt der Überwachung des Verhaltens oder der Leistung der Dienstkräfte für mitbestimmungsbedürftig erklärt hat. Die Rechtsprechung des Bundesarbeitsgerichts kann angesichts der übereinstimmenden Formulierungen im Betriebsverfassungsgesetz und in Personalvertretungsgesetzen in den Bereich der öffentlichen Verwaltung übernommen werden.

Das Berliner Datenschutzgesetz verweist bei der Frage, welche datenschutzrechtlichen Kriterien der Speicherung von **Daten über Dienst- und Arbeitsverhältnisse** zugrunde zu legen sind, auf die §§ 23 ff. Bundesdatenschutzgesetz. Abgesehen von ausdrücklichen gesetzlichen Bestimmungen zur Speicherung von Personaldaten und der sicherlich seltenen Einwilligung der Bediensteten ist danach die Speicherung von Personaldaten zulässig entweder im Rahmen der Zweckbestimmung eines Vertragsverhält-

¹⁾ Vgl. Ziff. 13 Pressekodex des Deutschen Presserats

²⁾ AV des Ministers der Justiz Nr. 12/1986 vom 18. Juli 1986

nisses oder vertragsähnlichen Vertrauensverhältnisses bzw. Dienstverhältnisses, oder aber soweit sie zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden (§ 23 Bundesdatenschutzgesetz).

Die zweite Alternative wird im Dienst- und Arbeitsverhältnis im allgemeinen auszuschließen sein, da Personal- und Arbeitsrecht die Speichergrenzen klar umreißen. Im Zuge der Diskussion über das Volkszählungsurteil wurde darüber hinaus von den Datenschutzbeauftragten festgestellt, daß die Sicherung des informationellen Selbstbestimmungsrechts wegen der Abhängigkeit des Arbeitnehmers von Arbeit und Einkommen zur Sicherung seiner Existenz vom Arbeitgeber unter anderem eine Beschränkung auf das zur Zweckerreichung erforderliche Datenminimum verlangt. Im Bereich der Personalinformationssysteme ist festzuhalten, daß jede Speicherung dispositiver Daten ohnehin schutzwürdige Belange verletzen kann und deshalb diese Alternative kaum zum Zuge kommt.

Damit ist die Zulässigkeit der Verarbeitung von Personaldaten ausschließlich danach zu beurteilen, ob die Daten im Rahmen der Zweckbestimmung des Dienst- bzw. Arbeitsverhältnisses erforderlich sind.

Problemlos dürften die Daten sein, mit denen die Dienstbehörde bzw. der Arbeitgeber ihre gesetzlichen und vertraglichen Verpflichtungen gegenüber den Mitarbeitern erfüllen (Personalabrechnungs- und Zahlungsverfahren, Abführung von Steuern und Sozialversicherungsbeiträgen usw.) sowie von Daten, die für die innerbetriebliche Organisation der Arbeitsabläufe erforderlich sind (z. B. Geschäftsverteilung, Schichtpläne, Telefonverzeichnisse, Stellenpläne).

Problematisch sind dagegen die Fälle, bei denen im Falle der Automatisierung die Grenze zum Personalinformationssystem überschritten wird. Auch dies kann im Rahmen der Zweckbestimmung des Dienst- bzw. Arbeitsverhältnisses erforderlich sein, nämlich zur Überprüfung, ob der Mitarbeiter seinen aus dem Arbeitsvertrag folgenden Pflichten genügt. Allerdings muß die Dienstbehörde im Falle einer Abwägung, ob bestimmte Verarbeitungen der Zweckbestimmung noch dienen, vorrangig die Persönlichkeitsrechte des Arbeitnehmers im Auge haben.

Bei der Einführung von Personalinformationssystemen stehen dem Personalrat wie erwähnt **Mitbestimmungsrechte** zu, die über die datenschutzrechtliche Bewertung hinausgehen und das Verfahren unmittelbar beeinflussen können. Da der Personalrat allerdings auch für die Berücksichtigung datenschutzrechtlicher Vorschriften zu sorgen hat (§ 72 Abs. 1 Ziff. 2 Personalvertretungsgesetz), stellt die Zustimmung ein Zulässigkeitskriterium im Rahmen der Verfahrenseinführung dar. Dies bedeutet, daß die Mißachtung der Rechte von Personalvertretungen bei der Einführung derartiger Systeme Speicherung und Verarbeitung von Personaldaten auch datenschutzrechtlich unzulässig macht. Andererseits ist natürlich die Zustimmung des Personalrats alleine nicht ausschlaggebend für die datenschutzrechtliche Bewertung. Läßt der Personalrat die Speicherung und Verarbeitung von Daten zu, die datenschutzrechtlich unzulässig, weil nicht erforderlich sind, so bleiben diese unzulässig. Wiederum war eine Reihe von Einzelproblemen zu klären:

Erhebung von Daten beim Bediensteten

Zur Berechnung des **Ortszuschlags** muß überprüft werden, ob der Ehepartner ebenfalls im öffentlichen Dienst tätig ist. Bislang mußten die Bediensteten stets eine vollständige Auskunft über Beschäftigungsverhältnisse der Ehepartner geben.

Dies halte ich für unzulässig, da personenbezogene Daten nur im erforderlichen Umfang erhoben werden dürfen und bei privaten Arbeitsverhältnissen eine Erforderlichkeit nicht vorliegt. Nach meinem Hinweis hat der Senator für Inneres den Vordruck „Erklärung zum Ortszuschlag, Sozialzuschlag, Anwärterverheiratenzuschlag“ geändert. Die Dienstkräfte müssen danach den Arbeitgeber des Ehegatten nur noch dann nennen, wenn eine Zuordnung zum öffentlichen Dienst nicht von vornherein ausgeschlossen werden kann. Die Zuordnung wird durch Hinweise auf Arbeitsbereiche, die regelmäßig im öffentlichen Dienst angesie-

delt sind, erleichtert. Konkrete Angaben wie Personalien des Ehegatten, Beschäftigungsverhältnis, Name und Anschrift der Beschäftigungsdienststelle werden jetzt nur noch erfragt, wenn der Bedienstete die genannten Voraussetzungen bejaht oder sie trotz der Erläuterungen nicht beurteilen kann.

Dennoch befürchteten einige Personalstellen, daß Betroffene unbewußt oder wider besseres Wissen falsche Angaben machen könnten, und forderten auch ohne konkrete Hinweise darauf die Betroffenen schriftlich auf, in jedem Fall Angaben zum Arbeitgeber des Ehegatten zu machen. Wenngleich ich hierin einen Verstoß gegen das informationelle Selbstbestimmungsrecht sehe, habe ich den Betroffenen zur Vermeidung von Nachteilen empfohlen, eine Zusatzklärung des Ehegatten mit dem Inhalt beizulegen, daß dessen Arbeitgeber keine dem öffentlichen Dienst vergleichbaren Verheirateten- oder Kinderzuschläge gewährt.

Aufgrund von Neuregelungen in den Beihilfevorschriften müssen Bedienstete nunmehr bei Anträgen auf **Beihilfe** Leistungen aus einer Krankenversicherung angeben.

Mehrere Personalräte und Bedienstete baten mich um Überprüfung, ob dieses Verfahren datenschutzrechtlichen Grundsätzen entspricht.

Gesetzliche Vorschriften enthalten eine solche Nachweispflicht nicht unmittelbar. Allerdings ergibt sich die Erforderlichkeit der Angaben daraus, daß nach den Beihilfevorschriften nur solche Leistungen zu gewähren sind, die zusammen mit den Leistungen einer Krankenversicherung die tatsächlich entstandenen Krankheitsaufwendungen nicht übersteigen. Zwar ist zweifelhaft, ob das dieser Regelung zugrundeliegende Bereicherungsverbot im Wege einer Verwaltungsvorschrift geregelt werden kann. Wenn dies allerdings der Fall ist, müssen auch die zum Vollzug der Vorschrift erforderlichen Daten erhoben werden dürfen. Ich habe die zuständige Verwaltung auf die Erforderlichkeit einer hinreichend klaren Regelung hingewiesen.

Offenbarung von Personaldaten innerhalb der Behörde

Einem Amtsleiter, der kurz zuvor in sein Amt eingeführt worden war und sich über den Leistungsstand seiner Mitarbeiter informieren wollte, waren hierzu vom Personalamt die **Personalakten** der Mitarbeiter zur Verfügung gestellt worden. Nachdem sich die Betroffenen an den örtlichen Personalrat wandten, bat dieser mich um eine datenschutzrechtliche Beurteilung.

Wegen der besonderen Zweckbindung der Personalakten sind zugriffsberechtigt nur die Stellen, die selbständig dienst- oder arbeitsrechtliche Verhältnisse begründen, verändern und auflösen dürfen (Dienstvorsetzte). Der Kreis der Berechtigten wird erweitert durch die mit dienstrechtlichen Aufgaben betrauten Mitarbeiter wie Personalsachbearbeiter und Büroleiter¹⁾. Für einen Fachvorgesetzten ergibt sich dagegen ein unmittelbares Recht auf Einsicht in Personalakten nicht, da dieser regelmäßig nicht mit dienstrechtlichen Aufgaben betraut ist.

Daher bringen Fachvorgesetzte bei Einsichtnahme in die gesamte Personalakte personenbezogene Daten in Erfahrung, die sie für ihre Zwecke nicht benötigen. Vielmehr muß die Weitergabe von Daten an den Fachvorgesetzten im Rahmen seiner Mitwirkung bei Stellenanhebungen, Beförderungen u. ä. auf die erforderlichen Unterlagen beschränkt werden. Zwar obliegt dem Fachvorgesetzten auch, seine Mitarbeiter zu beurteilen. Dies berechtigt ihn jedoch nicht zu einer Auswertung aller zu dienst- oder arbeitsrechtlichen Zwecken gesammelten Vorgänge.

Ein ähnliches Problem ergab sich, als der Präsident der Technischen Universität Berlin in einem Rundschreiben Beschäftigte aller Bereiche der Universität aufforderte, **Arbeitsunfähigkeitsbescheinigungen** nicht unmittelbar der Personalstelle, sondern zunächst der jeweiligen Beschäftigungsstelle vorzulegen.

Auch hierin liegt ein datenschutzrechtlicher Mangel, da nach den einschlägigen Vorschriften (z. B. §§ 18 Abs. 3, 36 Abs. 1 Landesbeamtengesetz) die Bescheinigung dem Dienstherrn bzw. Arbeitgeber vorgelegt werden muß, dessen dienst- bzw.

¹⁾ Als Dienstvorsetzter für den örtlichen Zuständigkeitsbereich - vgl. Jahresbericht 1984, Ziff. 4.3

arbeitsrechtliche Aufgaben grundsätzlich nicht vom Fachvorgesetzten wahrgenommen werden.

Zu Recht hatte der örtliche Personalrat befürchtet, daß bei dem angeordneten Verfahren etwa wegen der Angabe der Fachrichtung des behandelnden Arztes einem zu großen Personenkreis Rückschlüsse auf die Art der Erkrankung ermöglicht würden. Andererseits muß sichergestellt werden, daß Fachvorgesetzte bzw. Beschäftigungsdienststellen unverzüglich Informationen über Tatsache und voraussichtliche Dauer von Erkrankungen erhalten.

Ich habe daher empfohlen, die Anordnung dahingehend abzuändern, daß Mitarbeiter die Bescheinigungen nicht über die Beschäftigungsstellen bzw. den Fachvorgesetzten einreichen, sie aber der Beschäftigungsstelle zumindest die Tatsache und voraussichtliche Erkrankungsdauer mitteilen müssen.

Aufgrund eines Beschlusses des Abgeordnetenhauses, nach dem im öffentlichen Dienst ein auftragsbezogenes und auswertbares **Belegwesen** in den handwerklichen Bereichen eingeführt werden soll, hatte die Freie Universität ein neues Verfahren für die Abwicklung von universitätsinternen Reparaturaufträgen erarbeitet. Die Notwendigkeit einer solchen Maßnahme wurde auch damit begründet, daß der Rechnungshof beanstandet hatte, daß keine ausreichenden Aufzeichnungen über die Arbeiten der Betriebshandwerker vorgelegt werden konnten. Weiterhin sollte einer alten Forderung des Kuratoriums – einen wirtschaftlichen Vergleich zwischen eigen- und fremdgewarteten Gebäuden vorzulegen – Rechnung getragen werden.

Die technische Abteilung der Freien Universität hielt es daher für unumgänglich, daß die Betriebshandwerker neben dem Namen und dem Datum folgende Ergänzungen beim Ausfüllen von Arbeitszetteln vornehmen: Angaben über die Arbeitsdauer, Wegezeiten (Hin- und Rückweg), Ausfallstunden, Erschwerniszuschläge, Benutzung des Werkstattwagens, Materialverbrauch und Hinweise auf erkennbare notwendige Folgearbeiten.

Der örtliche Personalrat wandte sich dagegen, daß diese Zettel von den Arbeitern namentlich gezeichnet werden und zudem indirekt noch Angaben über Dritte enthalten sollten, so z. B. zu welchem Zeitpunkt bestimmte Sekretärinnen in welchem Institut nicht anzutreffen waren, bestimmte Reparaturen also nicht durchgeführt werden konnten.

Trotz dieser Bedenken ist das Verfahren zulässig. Die Verwaltung hat die Verpflichtung, gleichermaßen eine sowohl vom Personalaufwand als auch vom Sachaufwand günstige Verwendung öffentlicher Haushalts- bzw. Wirtschaftsmittel zu garantieren. Im Interesse einer solchen ordnungsgemäßen Haushalts- bzw. Wirtschaftsführung halte ich sowohl Art als auch Umfang der vorgesehenen Datenerhebung nach § 23 Bundesdatenschutzgesetz für zulässig. Mit den ausgefüllten Auftragszetteln kommt die Freie Universität im übrigen ihrer spezialgesetzlich geregelten Pflicht nach, dem Rechnungshof eine ordnungsgemäße Prüfung zu ermöglichen. Diese Maßnahme liegt somit im Rahmen der Zweckbestimmung des Dienstverhältnisses.

Das Verfahren muß allerdings sicherstellen, daß nur die Mitarbeiter der Stellen Kenntnis von den ausgefüllten Auftragszetteln nehmen können, die im Rahmen ordnungsgemäßer Aufgabenerfüllung im Arbeitsablauf beteiligt sind (Einsatzstelle, Beschäftigungsstelle vor Ort, Wirtschaftsstelle).

Auch Lobes- und Dankesreden anlässlich von **Jubiläen** bergen datenschutzrechtliche Probleme: Vorgesetzte greifen zur Vorbereitung gern auf Details aus den Personalakten zurück, um einen möglichst lückenlosen Überblick über den beruflichen und persönlichen Werdegang des Jubilars geben zu können.

Zwar kann man meist davon ausgehen, daß Betroffene eine Offenbarung bestimmter Daten zu diesem Anlaß eher begrüßen, jedoch darf diese Vermutung nicht verallgemeinert werden. Vielmehr muß die Dienststelle individuell prüfen, ob schutzwürdige Belange beeinträchtigt sein könnten. Letzte Sicherheit bringt hier nur die Zustimmung der Betroffenen. Daher sollten Jubilare zuvor rechtzeitig gefragt werden, ob sie die zu verwendenden Daten selbst vorgeben wollen oder ob sie sich mit der Verwendung der Personalakte einverstanden erklären.

4.4 Datenschutz im Bildungswesen

Hochschule

Im Oktober wurde eine Neufassung des **Berliner Hochschulgesetzes** verabschiedet.

Der Senator für Wissenschaft und Forschung hatte mir den Gesetzesentwurf nicht zur Stellungnahme zugeleitet, weil er die Auffassung vertrat, eine Datenschutzregelung im Hochschulbereich könne erst nach der Novellierung des Bundesdatenschutzgesetzes erfolgen. Ich hatte demgegenüber darauf hingewiesen, daß sowohl die Personaldatenverarbeitung im Hochschulbereich als auch die Erhebung und Verarbeitung von Studentendaten für Zwecke der Hochschulverwaltung einer bereichsspezifischen Regelung bedürfen, die von der gegenwärtig ohnehin nicht absehbaren Neufassung des Bundesdatenschutzgesetzes unabhängig ist.

Für den Bereich der **Personaldatenverarbeitung in den Hochschulen** hatte ich eine gesetzliche Klarstellung empfohlen, daß personenbezogene Daten von Hochschulmitarbeitern nur in dem für ihre Dienstverhältnisse erforderlichen Umfang und nur von denjenigen Stellen erhoben und verarbeitet werden dürfen, denen das Gesetz eine entsprechende Zuständigkeit für Einzelpersonalentscheidungen zugewiesen hat. Auch sollte das neugefaßte Hochschulgesetz nach meiner Auffassung der Forderung des Bundesverfassungsgerichts nach strikter Zweckbindung personenbezogener Dateien (z. B. Studentendateien einerseits und Beschäftigtendateien andererseits) Rechnung tragen. Die für die Immatrikulation von Studenten zuständige Stelle darf ebenso wenig auf Personaldateien zugreifen, wie die zentrale Personalverwaltung auf Studentendateien.

Eine gesetzliche Regelung der **Verarbeitung von Studentendaten** insbesondere bei der Immatrikulation ist aus meiner Sicht nicht deshalb entbehrlich, weil der Studienbewerber diese Daten der Hochschulverwaltung „freiwillig“ offenbart, um sein Studium durchzuführen. Vielmehr unterliegt er einem faktischen Zwang zur Offenbarung, da er angesichts des Monopols der Hochschulen keine Alternative zur Verwirklichung seines grundrechtlichen Anspruchs auf Zugang zum Studium (Art. 12 GG) hat. Insofern ähnelt die Stellung des Studienbewerbers der des Sozialleistungsempfängers, der ebenfalls nicht freiwillig Daten offenbart, sondern dessen Mitwirkungs- und Offenbarungspflichten im Sozialgesetzbuch detailliert geregelt sind.

Die Notwendigkeit einer bereichsspezifischen Regelung der Verarbeitung von Studentendaten ergibt sich zudem aus der Abhängigkeit der Hochschulstatistik von den durch die Hochschulen erhobenen Verwaltungsdaten. Hierauf hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits 1984 in einem entsprechenden Beschluß hingewiesen.

Das Gesetz sieht in seiner beschlossenen Fassung vor, daß der Senator für Wissenschaft und Forschung die Erhebung personenbezogener Daten für Zwecke der **Planung und Statistik** anordnen kann; die Mitglieder der Hochschule sind verpflichtet, die ihnen vorgelegten Fragen wahrheitsgemäß, vollständig und fristgerecht zu beantworten. Wie bereits im Zusammenhang mit dem Landesstatistikgesetz ausgeführt, halte ich eine derartige Regelung angesichts der Forderung des Bundesverfassungsgerichts, daß Zwangserhebungen einer normenklaaren gesetzlichen Grundlage bedürfen, für verfassungsrechtlich äußerst bedenklich. Ich hatte daher noch unmittelbar vor der Verabschiedung empfohlen, die Bestimmung zu streichen und stattdessen die Regelung des anstehenden Landesstatistikgesetzes abzuwarten. Nach der Verabschiedung habe ich den Senator für Wissenschaft und Forschung gebeten, die Bestimmung bis zum Inkrafttreten des Landesstatistikgesetzes nicht anzuwenden.

Schule

Zahlreiche Beschwerden haben mich in diesem Jahr wiederum zur **Lehrerindividualdatei** beim Senator für Schulwesen, Berufsausbildung und Sport erreicht. Seit 1984 wird die Lehrerindividualdatei aufgrund meiner Empfehlungen in der Weise geführt, daß die Senatsschulverwaltung nur auf anonymisierte Lehrerdaten für statistische Zwecke zugreifen darf. Drei namentlich benannte Mitarbeiter führen außerdem im Auftrag der Bezirke

Lehrerverzeichnisse, die lehrerbezogene Daten enthalten und die jährliche Fortschreibung der anonymisierten Lehrerindividualdatei ermöglichen. Nur zum Zwecke dieser Fortschreibung dürfen die bezirklichen Lehrerverzeichnisse mit der Lehrerindividualdatei zusammengespielt werden, um die Versendung der Erhebungsbögen an die Schulleiter durchzuführen und ihren Rücklauf zu überwachen. Die betreffenden Mitarbeiter sind durch Dienstanweisung auch hausintern zur Verschwiegenheit über den Inhalt der Lehrerverzeichnisse verpflichtet. Zu den rechtlichen Problemen der Lehrerindividualdatei habe ich in der Vergangenheit bereits Stellung genommen¹⁾.

Im Frühjahr dieses Jahres habe ich die organisatorischen und technischen Abläufe bei der jährlichen Aktualisierung der Lehrerverzeichnisse und der Lehrerindividualdatei sowie bei der Anwendung der Lehrerindividualdatei überprüft. Dabei habe ich den Eindruck gewonnen, daß die Dienstanweisung eingehalten wird, und daß das zuständige Referat die datenschutzrechtlich gebotene Trennung mit der erforderlichen Sorgfalt sichert. Die Dienstanweisung schließt jedoch nicht aus, daß es der Senatsschulverwaltung technisch und organisatorisch möglich ist, auf die personenbezogenen Lehrerverzeichnisse ohne Zustimmung der Bezirke zuzugreifen und Datensätze aus der Lehrerindividualdatei bestimmten Lehrern zuzuordnen. Nach meiner Erfahrung gibt eine derartige Selbstbindung durch Verwaltungsvorschriften immer wieder zu die öffentliche Verwaltung belastenden Spekulationen Anlaß, daß diese nicht eingehalten würden. Insbesondere wird darauf hingewiesen, daß die Dienstanweisung jederzeit geändert werden könne. Nach meinem Eindruck ist bei dem derzeit praktizierten Verfahren, das unter meiner Beteiligung entwickelt wurde, bei kritischen Dritten schwer das Vertrauen in die Ordnungsmäßigkeit der Datenverarbeitung herzustellen.

Ich habe deshalb empfohlen, das Verfahren so zu gestalten, daß es zu den beschriebenen Befürchtungen keinen Anlaß mehr gibt.

Das im Herbst 1985 bei der Fortschreibung der Lehrerindividualdatei angewandte Verfahren habe ich in einem Punkt bemängelt:

Das Begleitschreiben an die Schulleiter legte den Schluß nahe, die Schulleiter könnten bestimmte Informationen über Lehrer bei den bezirklichen Lehrpersonalstellen abfragen. Demgegenüber habe ich darauf hingewiesen, daß der Schulleiter zwar die Möglichkeit hat, entweder den Lehrern die Ausfüllung der Erhebungsbögen insgesamt zu überlassen oder die Erhebungsbögen selbst insoweit auszufüllen, als er die Fragen aus eigenem Wissen beantworten kann, und dann den Erhebungsbogen über die Lehrpersonalstelle des zuständigen Bezirksamtes mit der Bitte um Vervollständigung der Angaben aus der Personalakte an die Senatsschulverwaltung zurückzusenden. Ein Zugriff des Schulleiters auf die Personalakte des einzelnen Lehrers - sei es auch nur durch telefonische Rückfrage bei der Lehrpersonalstelle - wäre dagegen unzulässig. Bei der Fortschreibungsaktion im Herbst 1986 wurde die mißverständliche Formulierung nicht mehr verwendet.

Während der Fortschreibung der Lehrerindividualdatei im Herbst 1985 untersagten zahlreiche betroffene Lehrer ihren Schulleitern schriftlich die Weitergabe personenbezogener Daten. Ein Petent wies mich darauf hin, daß zumindest in einem Bezirk diese Schreiben mit entsprechenden Vermerken zu den Personalakten der betroffenen Lehrer genommen werden sollten. Ich habe Zweifel an der Rechtmäßigkeit eines solchen Vorgehens. Zum einen betreffen die genannten Schreiben nicht die Dienstverhältnisse der betroffenen Lehrer, was sich schon daraus ergibt, daß sie nicht an den jeweiligen Dienstvorgesetzten, d. h. das Bezirksamt, gerichtet waren. Zum anderen ist ihre Speicherung in der Personalakte nicht für das betreffende Dienstverhältnis erforderlich, so daß in unverhältnismäßiger Weise in das Recht der Betroffenen auf informationelle Selbstbestimmung eingegriffen wird. Die Senatsschulverwaltung hat bisher nur angeregt, keine entsprechenden Vermerke in die Personalakten aufzunehmen; anders als ich hält sie jedoch die Aufnahme der Schreiben an die Schulleiter für rechtlich zulässig. Ich begrüße es, daß das zuständige Bezirksamt bis zur Klärung dieser Angelegen-

heit die Schreiben der Lehrer getrennt von den Personalakten aufbewahrt.

Der Anmeldung der bezirklichen Lehrerverzeichnisse zum Dateienregister entnahm ich, daß die Lehrerverzeichnisse u. a. zur Feststellung der Dienstbehörde eines Lehrers bei der Weiterleitung von disziplinarrechtlich relevanten Einzelvorgängen benutzt werden. Die **Mitteilungen in Strafsachen gegen Lehrer und Schulaufsichtsbeamte** sind ausschließlich an den unmittelbaren Dienstvorgesetzten, d. h. das Bezirksamt, zu richten. Der Generalstaatsanwalt bei dem Landgericht hat angeordnet, daß in Zukunft bei einem unbekannten Beschäftigungsort des Beschuldigten die Mitteilung in einem verschlossenen Umschlag der Senatsschulverwaltung mit der Bitte übersandt wird, diesen Umschlag ungeöffnet an das jeweils zuständige Bezirksamt weiterzuleiten. Der datenschutzrechtliche Mangel wurde damit behoben.

Bei der Überprüfung der Lehrpersonalstelle eines Bezirksamtes stellte ich fest, daß bei der Ernennung von Lehramtskandidaten zu Referendaren sogenannte **Sammelverfügungen** in die Referendarpersonalakten aufgenommen wurden, die nicht nur den Namen des jeweils Betroffenen, sondern die Namen aller zu einem bestimmten Termin ernannten Studienreferendare enthielten. Auf diese Weise wird das Risiko der unbefugten Weitergabe von Namens- und Adressenlisten an Private (z. B. Versicherungsvertreter) erhöht, obwohl sich dies unter den Bedingungen der modernen Textverarbeitung ohne zusätzlichen Aufwand abschließen ließe. Künftig wird in die Personalakten der Lehramtsanwärter lediglich ein Hinweis auf die mit der Sammelverfügung angeordnete Ernennung ohne Fremddaten aufgenommen.

Diese datenschutzgerechte Lösung des Problems begrüße ich umso mehr, als der Senator für Schulwesen, Berufsausbildung und Sport mir in anderem Zusammenhang grundsätzlich die Kompetenz abspricht, zum Inhalt von **Personalakten** Stellung zu nehmen. Ich war deshalb auch nicht in der Lage, eine Eingabe abschließend zu bearbeiten, mit der mich ein Petent auf den Entwurf zur Änderung der Ausführungsvorschriften über die dienstliche Beurteilung der Beamten des Schul- und Schulaufsichtsdienstes (**AV-Lehrerbeurteilung**) hingewiesen hatte. Dieser Entwurf sieht vor, daß alle dienstlichen Beurteilungen nach der Beteiligung des Personalrates automatisch der Senatsschulverwaltung zuzuleiten und anschließend zu den Personalakten zu nehmen sind. Ich habe darauf hingewiesen, daß die Schulaufsicht die Vorlage von Lehrpersonalakten, die nur das jeweilige Bezirksamt, Abt. Volksbildung, zu führen hat, einschließlich dienstlicher Beurteilungen nur im Einzelfall rechtfertigt, wenn Anhaltspunkte dafür vorliegen, daß schulaufsichtliche Maßnahmen erforderlich werden können. Der Senator für Schulwesen, Berufsausbildung und Sport hat mir mitgeteilt, die beabsichtigte Vorlage aller dienstlichen Beurteilungen diene der Wahrung seiner Aufgaben als oberster Dienstbehörde; welches diese Aufgaben im einzelnen seien, habe er mir nicht darzulegen, da ich zum Inhalt von Personalakten nicht Stellung zu nehmen hätte. Ich habe daraufhin dem Petenten meine gegenteilige Rechtsauffassung mitgeteilt.

Vom Beginn meiner Tätigkeit an habe ich der Verarbeitung von Schülerdaten besondere Aufmerksamkeit gewidmet. Ich begrüße es deshalb, daß der Senator für Schulwesen, Berufsausbildung und Sport nach langjährigen Vorarbeiten am 1. August 1986 **neue Ausführungsvorschriften über die Führung schriftlicher Unterlagen über Schüler (AV-Schülerunterlagen)** in Kraft setzte, die aus meiner Sicht Verbesserungen gegenüber der bisherigen Praxis bringen können.

Allerdings habe ich stets betont, daß derartige Verwaltungsvorschriften eine bereichsspezifische Regelung im Schulgesetz nicht überflüssig machen, wie sie seit dem Volkszählungsurteil des Bundesverfassungsgerichts geboten ist. Auch berücksichtigen die neuen Ausführungsvorschriften meine Empfehlungen nur zum Teil. So wird zwar erstmals auch Schülern ab dem vollendeten 14. Lebensjahr mit Zustimmung ihrer Erziehungsberechtigten ein Einsichtsrecht in Schülerunterlagen eingeräumt. Ich hatte demgegenüber unter Hinweis auf die Grundrechtsmündigkeit heranwachsender Schüler die Auffassung vertreten, daß die Einsichtnahme in bestimmten Fällen auch ohne Zustimmung der Eltern möglich sein müsse. Zu Recht erstreckt sich das neu geregelte Einsichtsrecht auch auf den sonderpädagogischen Beobach-

¹⁾ Jahresbericht 1983, Ziff. 3.4

tungsbogen. Zu begrüßen ist auch, daß gegenüber früheren Entwürfen die Aufnahme von Angaben dritter Personen in den Schülerbogen und deren vertrauliche Behandlung sowie die Übermittlung des Ergebnisses schulärztlicher Untersuchungen zum Alter des Schülers an das Landeseinwohneramt (Ausländerbehörde) nicht mehr vorgesehen ist.

Von zentraler Bedeutung ist die **Regelung der automatisierten Sammlungen personenbezogener Daten in der Schule**, die auch den Einsatz privater Datenverarbeitungsgeräte zur Verarbeitung von Schüler- oder Elterndaten umfaßt. Ich bedauere es allerdings, daß die Ausführungsvorschriften in einem wesentlichen Punkt hinter früheren Entwürfen zurückbleiben, die meine Empfehlungen stärker berücksichtigt.

Der Umfang der personenbezogenen Daten, die automatisiert verarbeitet werden dürfen, ist zu groß. Er umfaßt alle personenbezogenen Daten, die auch manuell in der Schule verarbeitet werden dürfen. Demgegenüber werde ich auch in Zukunft an die automatisierte Verarbeitung von Leistungsdaten (insbesondere Zensuren, Bemerkungen auf Zeugnissen, Erziehungsmaßnahmen) erheblich strengere Anforderungen stellen als an die Verarbeitung von sonstigen personenbezogenen Daten für die Zwecke der Schulverwaltung. Gegen den automatisierten Ausdruck von Zeugnissen und Zeugnislisten habe ich dann keine Einwände, wenn hierbei Leistungsdaten nur vorübergehend für die Zwecke der Textverarbeitung gespeichert und nach deren Abschluß gelöscht werden.

Zu begrüßen ist schließlich die abschließende und differenzierte Aufzählung von Datensammlungen, die in der Schule geführt werden dürfen. Die Automatisierung dieser Datensammlungen darf dementsprechend nicht zu einer generellen Verknüpfung aller Dateien in einem Datenbanksystem führen, vielmehr müssen personenbezogene Unterlagen auch in automatisierter Form voneinander getrennt bleiben und nur den Personen zugänglich sein, die auch in manueller Form auf sie zugreifen dürfen. Der Aufbau eines umfassenden Schulinformationssystems, in dem alle personenbezogenen Unterlagen miteinander verknüpft werden können, ist für die Erfüllung des schulischen Auftrags nicht erforderlich.

Erneut erhielt ich in diesem Jahr Beschwerden zu der bereits früher¹⁾ behandelten Frage, inwieweit Lehrer bei der **Unterrichtsgestaltung** datenschutzrechtliche Belange der Schüler und ihrer Erziehungsberechtigten zu berücksichtigen haben. Ich habe dem Senator für Schulwesen, Berufsausbildung und Sport hierzu detaillierte Empfehlungen gegeben, die in ein entsprechendes Rundschreiben an die Berliner Schulen eingehen sollen. Dabei habe ich auch angeregt, dem **Datenschutz als Unterrichtsthema** stärkere Bedeutung als bisher zu geben. Dabei bin ich mir bewußt, daß es ein legitimes pädagogisches Ziel ist, Kinder zur spontanen Offenbarung eigener Erfahrungen und Daten über sich selbst und Dritte, z. B. die Eltern, zu bewegen. Dieses Ziel ist jedoch nach meiner Auffassung nicht unvereinbar mit einer behutsamen, mit zunehmendem Alter der Schüler differenzierteren Bewußtmachung der Probleme des Persönlichkeitsschutzes. Den Schülern sollte außerdem eine gewisse Wahlfreiheit bei der Bearbeitung von Aufsatzthemen eingeräumt werden. Für unvertretbar halte ich das Vorgehen eines Lehrers, der nach Angaben eines Petenten den Schülern die Aufgabe gestellt hatte, einen eigenen Lebenslauf für Stellensbewerbungen zu verfassen und der vor der gesamten Klasse bemängelte, daß ein Schüler die Scheidung seiner Eltern unerwähnt gelassen hatte.

Bibliothekswesen

Zahlreiche Benutzer und Mitarbeiter haben sich über das neue automatisierte **Ausleihverbuchungsverfahren** der Amerika-Gedenkbibliothek beschwert, das auch Gegenstand öffentlicher Diskussion war. Ich habe daher geprüft, ob meinen Empfehlungen bei der Entwicklung des Systems Rechnung getragen wurde²⁾. Zunächst konnte ich aus der vorhandenen Dokumentation des Verfahrens zweifelsfrei feststellen, daß die von mir geforderte Anonymisierung der Ausleihdaten nach vollständiger Abwick-

lung des Ausleihvorgangs in irreversibler Weise geleistet wird. Damit wird die Möglichkeit einer personenbezogenen Analyse von Leserverhaltensweisen, die erhebliche Rückschlüsse auf ein Persönlichkeitsprofil zulassen würden, ausgeschlossen.

Mit den Anmeldeformularen wurde ein Fragebogen zur **Statistik des Leseverhaltens** ausgegeben. Dieses Formular enthielt keine personenbezogenen Daten. Obwohl dadurch der Anschein der Anonymität erweckt wurde, wurden die auf diesem Formular angegebenen Daten mit Personenbezug in den Computer eingegeben. Einen Hinweis auf diese Verfahrensweise enthielt das Formular nicht. Vielmehr wurde durch die Gestaltung der Eindruck erweckt, es sei nicht beabsichtigt, diese Daten personenbezogen abzuspeichern. Diesen Mangel habe ich beanstandet, weil der Eindruck entstand, daß sich die Amerika-Gedenkbibliothek Daten der Benutzer ohne deren Wissen beschaffen wollte. Aufgrund meiner ausdrücklichen Empfehlungen und des öffentlichen Protests wurde die Benutzung des Fragebogens eingestellt. Dieser Vorfall führte zu einer breiteren öffentlichen Diskussion über die Zulässigkeit der Datenverarbeitung in den städtischen Bibliotheken. Ich wurde erneut in meiner Auffassung bestärkt, daß eine gesetzliche Regelung des Datenschutzes dringend notwendig ist.

Darüber hinaus wurde bei der technisch-organisatorischen Überprüfung der Amerika-Gedenkbibliothek eine Reihe von Mängeln festgestellt:

- Die Ordnungsmäßigkeit und Prüfbarkeit eines Verfahrens dieser Größenordnung erfordert schriftliche **Unterlagen und Dokumentationen**. Diese konnten nicht in der von mir gewünschten Form vorgelegt werden. So fehlten u. a. schriftliche Festlegungen der Funktionsbereiche und der Arbeitsabläufe, Programmier- und Testrichtlinien sowie Teile der Verfahrens- und Programmdokumentation.

Die vorhandenen Unterlagen erlaubten zwar eine hinreichende Rekonstruktion des Verfahrens im allgemeinen, eine Beurteilung der einzelnen Funktionen war dagegen nicht immer möglich.

Die Amerika-Gedenkbibliothek machte geltend, daß die Dokumentation zu den Aufgaben des Lieferanten der automatisierten Datenverarbeitung gehört habe, von diesem aber nicht in zufriedenstellender Weise geliefert worden sei. Man beabsichtige daher, eine umfassende Dokumentation selbst zu erstellen. Die schnelle Umsetzung dieser Absicht scheiterte jedoch an den erheblichen personellen Engpässen.

- Die **Zu- und Abgangskontrolle** zum Rechenzentrum der Amerika-Gedenkbibliothek war sowohl in baulicher als auch technischer und organisatorischer Hinsicht unzureichend.
- Die formalen Pflichten zur Herstellung gesetzlich gebotener interner und externer **Transparenz der Datenverarbeitung** in der Amerika-Gedenkbibliothek (interne Dateienübersicht, Meldungen zum Dateienregister, Veröffentlichung im Amtsblatt) waren nicht erfüllt.

Die meisten festgestellten datenschutzrechtlichen Mängel sind von der Amerika-Gedenkbibliothek mittlerweile behoben worden.

4.5 Organisation und Geschäftsordnung

Datenweitergabe innerhalb des Bezirksamtes

Die Behandlung der Datenweitergabe in großen Verwaltungsorganisationen, die Aufgaben der verschiedensten Art wahrnehmen, warf von Anfang an erhebliche Probleme auf. Für die Bezirksamter hatte ich in meinem Jahresbericht 1985 darauf hingewiesen, daß spätestens das Volkszählungsurteil mit seiner Forderung nach informationeller Gewaltenteilung hier eine Klärung gebracht hat: Jede Zweckänderung eines Datums stellt einen Eingriff in das informationelle Selbstbestimmungsrecht dar und muß daher datenschutzrechtlich überprüft werden. Demgegenüber hatte der Senat weiterhin daran festgehalten, daß das Bezirksamt als Ganzes als speichernde Stelle zu betrachten sei.

In Gesprächen mit dem Senator für Inneres ist es gelungen, eine gemeinsame Auffassung zu entwickeln, die einerseits daten-

¹⁾ Jahresbericht 1983, Ziff. 3.4

²⁾ Jahresbericht 1982, Ziff. 3.2

schutzrechtlichen Anforderungen genügt, andererseits aber nicht unüberwindbare organisatorische Probleme aufwirft. Ich habe das Ergebnis der Beratungen den Bezirksämtern mitgeteilt¹⁾.

Im Ergebnis müssen bei einer Datenweitergabe innerhalb des Bezirksamtes die datenschutzrechtlichen Vorschriften über Übermittlungen bzw. Offenbarungen entsprechend angewandt werden.

Offenbarungen im Rahmen der Aufsicht

Ein Bezirksbürgermeister bat um Beratung zu der Frage, inwieweit bei der **Behandlung von Dienstaufsichtsbeschwerden und Petitionen** das für die Abteilung Personal und Verwaltung zuständige Mitglied des Bezirksamtes befugt ist, Einsicht in die zugrundeliegende Sachakte (z. B. der Abteilungen Sozialwesen oder Gesundheitswesen) zu nehmen.

Bei Dienstaufsichtsbeschwerden gegen das persönliche Fehlverhalten eines Bediensteten oder ein eventuelles Organisationsverschulden des Bezirksamtes ist der Bezirksbürgermeister als Dezernent für die Abteilung Personal und Verwaltung an der Entscheidung über diese Beschwerde zu beteiligen, da er die Funktion des Dienstvorgesetzten wahrnimmt. Nur in der Abteilung Volksbildung ist der zuständige Bezirksstadtrat Dienstvorgesetzter der Mitarbeiter dieser Abteilung.

Handelt es sich dagegen um eine Sachbeschwerde (Gegenvorstellung), so kann neben den die Entscheidung vorbereitenden Bediensteten nur der zuständige Bezirksstadtrat Einsicht in den Vorgang nehmen. Entsprechendes gilt für die Stellungnahme zu Petitionen gegenüber dem Abgeordnetenhaus.

Auch die Offenbarung von Sozialdaten ist insoweit zulässig, da die Ausübung der Dienstaufsicht zur Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch gehört. Würde die Aktenvorlage an den Bezirksbürgermeister oder den zuständigen Bezirksstadtrat zur Offenbarung personenbezogener Daten führen, die dem Berufsgeheimnis des Arztes, Berufspsychologen, Beraters in einer anerkannten Beratungsstelle, Sozialarbeiters oder Sozialpädagogen unterliegen, so wäre die Einwilligung des Betroffenen erforderlich. Falls der Umgang mit diesen Daten gerade Gegenstand der Dienstaufsichtsbeschwerde ist, kann von der Einwilligung ausgegangen werden. In anderen Fällen sollte der Beschwerdeführer darauf hingewiesen werden, daß über seine Beschwerde nur dann entschieden werden kann, wenn er den betreffenden Geheimnisträger von seiner Schweigepflicht entbindet.

Aktenführung

In der Diskussion zum Sozialdatenschutz erhalten die Probleme der Aktenführung einen immer höheren Stellenwert.

In der **Sozial- und Jugendverwaltung** wird die Aktenführung in der Regel von folgendem Prinzip bestimmt: Akten werden nach dem Prinzip der Bedarfsgemeinschaft geführt und ausschließlich chronologisch aufgebaut. Die in Akten befindlichen Unterlagen sind de facto untrennbar verbunden: Nur mit größtem zeitlichen Aufwand ist es möglich, sie nachträglich in Einzelteile so zu zerlegen, daß eine differenzierende Datenübermittlung oder eine differenzierende Einsichtnahme erfolgen kann. Das informationelle Selbstbestimmungsrecht gebietet aber eine derartige Differenzierung.

Personenbezogene Daten dürfen bei der Beratungs- und Betreuungsarbeit nur dann erhoben und gespeichert werden, wenn dies zur Aufgabenerfüllung konkret erforderlich ist. Die Fülle der dem Sozialarbeiter bekannt werdenden Informationen ist von diesem zu sondieren und fachspezifisch auszuwerten. Das bloße Sammeln von Informationen kann die soziale Betreuung nicht ersetzen. Da soziale Leistungsverhältnisse in der Regel auf Freiwilligkeit basieren, muß der Sozialarbeiter den Willen des Leistungsempfängers in besonderem Maße berücksichtigen. Er hat gewissermaßen eine Maklerfunktion zwischen den Aufgaben der Behörde und den Bedürfnissen des Leistungsempfängers.

In Zusammenarbeit mit den betroffenen Verwaltungen beabsichtige ich, eine Bestandsaufnahme unter Berücksichtigung der rechtlichen Rahmenbedingungen insbesondere des informationellen Selbstbestimmungsrechts sowie den hierzu geltenden gesetzlichen Bestimmungen vorzunehmen und Verbesserungen vorzuschlagen. Auch der Senator für Inneres, der derzeit mit einer Organisationsuntersuchung zu Fragen der Aktenführung befaßt ist, ist an den Beratungen beteiligt.

Für den Bereich des Schulpsychologischen Dienstes wurden Verwaltungsvorschriften vorbereitet, die es den betroffenen Stellen zur Auflage machen, bei der Aktenführung dafür Sorge zu tragen, daß das Einsichtsrecht der Betroffenen nicht unzulässigerweise geschmälert wird und bei der Aktengliederung differenzierend auf die jeweilige Verwaltungsaufgabe abgestellt wird. Maßnahmen, die aufgrund gesetzlicher Anordnung erfolgen, sind demnach getrennt von denjenigen Unterlagen abzuheften, die aufgrund eines freiwilligen Leistungsverhältnisses entstehen.

Vordrucke

Personenbezogene Daten werden in der Regel vom Betroffenen mit Hilfe von Vordrucken erhoben. Dabei ist dieser nach § 9 Abs. 2 Berliner Datenschutzgesetz auf die Rechtsgrundlage, aufgrund derer die Daten erhoben werden, ansonsten auf die Freiwilligkeit seiner Angaben hinzuweisen. Dabei spielt es keine Rolle, ob der Vordruck von dem Betroffenen selbst ausgefüllt wird oder aber der Verwaltungsmitarbeiter die Angaben durch Befragen des Betroffenen erhebt und in den Vordruck einträgt.

Formulärmäßig werden - vom Bürger oftmals unbemerkt - auch personenbezogene Daten von anderen Behörden oder öffentlichen Stellen zur rechtmäßigen Erfüllung der in der eigenen Zuständigkeit liegenden Aufgaben abgefragt (§ 10 Abs. 1 Berliner Datenschutzgesetz).

Eine Durchsicht von Vordrucken, die der Senator für Inneres entwickelt hat, hat ergeben, daß bei vielen Vordrucken eine Verbesserung in datenschutzrechtlicher Hinsicht geboten ist.

Ich gehe von folgenden Grundsätzen aus:

- Bei Vordrucken, die vom **Betroffenen** ausgefüllt werden, ist bei jeder Frage entweder der Hinweis auf die Freiwilligkeit der Angaben anzubringen oder die Rechtsgrundlage zu benennen. Dabei genügen pauschale Hinweise auf einschlägige Rechtsvorschriften (Personenstandsrecht, Bürgerliches Recht) nicht.
- In Ausnahmefällen, insbesondere dann, wenn durch diese Hinweise die Vordruckgestaltung unübersichtlich würde, könnten Fußnoten angebracht werden oder die Erläuterungen in einem gesonderten Merkblatt, das der Betroffene mitausgehändig bekommt, erfolgen.
- Wenn der Verwaltungsmitarbeiter den Vordruck nach **Befragen** des Betroffenen ausfüllt, sollte ein Merkposten den Mitarbeiter daran erinnern, den Bürger auf die Rechtslage hinzuweisen.
- Bei Formularen, mit denen **bei anderen Stellen** im Rahmen der ordnungsgemäßen Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben Informationen **abgefragt** werden, habe ich angeregt, im Hinblick auf § 10 Abs. 3 Berliner Datenschutzgesetz ebenfalls auf die Rechtsgrundlage hinzuweisen, damit die übermittelnde Stelle über die Zulässigkeit der Datenübermittlung entscheiden kann.

Der Senator für Inneres hat zugesagt, meinen Empfehlungen und Anregungen bei jeder Neuauflage der durchgesehenen Vordrucke weitestgehend Rechnung zu tragen. Es wäre wünschenswert, wenn auch andere Verwaltungen - losgelöst von Einzelfallüberprüfungen - bei der Neuauflage die Vordrucke überprüfen würden.

Postverkehr

Die Offenbarung teils sensibler personenbezogener Daten bei der Versendung von Schriftstücken durch die Bundespost ist häufig

¹⁾ Anlage 6

fig Anlaß von Bürgereingaben. Das Spektrum der betroffenen Behörden reicht von Gerichten über die Bezirksverwaltungen hin bis zu Behörden der Hauptverwaltung. Aufnahme in das Adreßfeld von Briefen fanden neben dem Namen und der Anschrift des Adressaten unterschiedliche Angaben wie z. B. das Geburtsdatum, Geburtsort, Geburtsname oder Beruf. In anderen Fällen waren Hinweise auf gegen den Betroffenen laufende Verfahren oder Namen und Anschrift des behandelnden Arztes aus dem Adreßfeld ersichtlich.

Auf Postkarten wurden Bürgern u. a. Zahlungsrückstände, Einladungen zur Vorsorgeuntersuchung der Geschwulstberatungsstelle oder Einzeldaten in Sozialhilfeangelegenheiten mitgeteilt.

Diese Praxis verstößt sowohl gegen Rechts- als auch Verwaltungsvorschriften.

Nach § 30 Verwaltungsverfahrensgesetz dürfen die zum persönlichen Lebensbereich gehörenden Geheimnisse sowie die Betriebs- und Geschäftsgeheimnisse von der Behörde nicht unbefugt offenbart werden (vgl. für den Sozialleistungsbereich auch § 35 SGB I). Weiterhin verstößt eine Aufnahme von für die ordnungsgemäße Zustellung durch die Bundespost nicht erforderlichen Zusatzdaten auch gegen das Datengeheimnis nach den §§ 8 und 11 Berliner Datenschutzgesetz.

Diese Datenschutzbestimmungen finden auch in der Gemeinsamen Geschäftsordnung für die Berliner Verwaltung (GGO I) Berücksichtigung. Nach § 62 Abs. 1 GGO I darf die Anschrift nicht mit Zusätzen versehen werden, die auf persönliche oder sachliche Verhältnisse schließen lassen. Nach § 58 Abs. 1 GGO I dürfen Postkarten keine geheimzuhaltenden Angaben und keine Hinweise enthalten, aus denen auf Geheimzuhaltendes geschlossen werden kann.

Ebenso problematisch ist die Form der Absendergestaltung durch Behörden, die jedoch nicht eindeutig geregelt ist.

Zweifellos greifen Postsendungen mit einem Absender, der einen Zusatz wie „Geschwulstberatungsstelle“, „Sozialpsychiatrischer Dienst“, „Haftentlassenenhilfe“, o. ä. enthält, in die Persönlichkeitsrechte des Empfängers ein. Hier muß darauf hingewirkt werden, daß derartige Zusätze entweder völlig entfallen oder aber die Bezeichnungen von sensiblen Verwaltungseinheiten so abgekürzt oder verschlüsselt werden, daß Rückschlüsse auf persönliche oder sachliche Beziehungen des Adressaten nicht möglich sind. Aufgrund meiner Empfehlung verzichtet das Landes-einwohneramt seither auf die Angabe des Referates als Absender. Damit ein nicht zustellbares Schriftstück den absendenden Sachbearbeiter wieder verschlossen erreichen kann, habe ich zusätzlich empfohlen, das Stellenzeichen des Bearbeiters anzugeben.

4.6 Umweltschutz auf Kosten des Datenschutzes?

In dem Maße, wie sich die Verwaltung im Interesse eines effektiven Umweltschutzes der elektronischen Datenverarbeitung bedient, stellen sich auch in diesem Bereich zunehmend datenschutzrechtliche Fragen.

Der Senator für Stadtentwicklung und Umweltschutz erstellte aufgrund des Bundesimmissionsschutzgesetzes ein **Emissionskataster**, das Angaben über Art, Menge, räumliche und zeitliche Verteilung und die Austrittsbedingungen von Luftverunreinigungen bestimmter Anlagen und Fahrzeuge enthält. Für das Emissionskataster „Hausbrand“ sollten die Adressendateien von BEWAG und GASAG ausgewertet werden. Ich habe darauf hingewiesen, daß die Adressendateien jedenfalls insoweit personenbezogene Daten enthalten, als es sich um Einfamilienhäuser handelt. Ihre Auswertung bedarf, wenn sie zur Erstellung des Katasters erforderlich ist, einer bereichsspezifischen Rechtsgrundlage, die bisher fehlt. Solange diese nicht vorhanden ist, kann die Datenerhebung nur beim Betroffenen und unter ausdrücklichem Hinweis auf die Freiwilligkeit erfolgen. Der Umweltschutzsenator hat daraufhin das Emissionskataster ohne Auswertung personenbezogener Daten in anonymisierter Form aufgestellt.

Zur möglichst wirksamen Abwehr von Gefahren für das Grundwasser durch wassergefährdende Stoffe hat die Senatsverwaltung für Stadtentwicklung und Umweltschutz - Wasserbehörde - eine Leitstelle eingerichtet, die eine **Datei aller Lagerbehälter für wassergefährdende Stoffe** führt. Diese Datei erfüllt zwei

unterschiedliche Funktionen. Zum einen verarbeitet die Senatsverwaltung im Auftrag der Bezirke personenbezogene Daten zum Vollzug der Lagerverordnung, insbesondere zur Überwachung der Überprüfung von Lagerbehältern durch die beauftragten Sachverständigen. Zum anderen nutzt die Senatsverwaltung als Wasserbehörde die Lagerbehälterdatei zu Zwecken der Gewässeraufsicht, insbesondere der Gefahrenabwehr bei Ölunfällen.

Soweit der Umweltschutzsenator als Auftragnehmer der Bezirke den Vollzug der Lagerverordnung überwacht, ist hiergegen nichts einzuwenden, wenn die gebotenen Datensicherungsmaßnahmen getroffen werden. Zu Zwecken der Gefahrenabwehr kann der Umweltschutzsenator aus der Lagerbehälterdatei nur bestimmte, hierfür erforderliche Daten (Name und Anschrift des Polizeipflichtigen, Größe und Art des Lagerbehälters einschließlich seiner technischen Sicherheitsvorkehrungen, Lagermedium) abrufen. Dagegen ist der Umweltschutzsenator nicht befugt, auf alle übrigen von den Bezirksämtern im Vollzug der Lagerverordnung gespeicherten Daten (z. B. Genehmigung des Behälters, Genehmigungsdatum, Zeitpunkt der letzten Prüfung) zuzugreifen. Dies ist nach der Durchführungsverordnung zum Allgemeinen Sicherheits- und Ordnungsgesetz ausschließlich Sache der Bezirke. Ich habe empfohlen, die rechtlichen Probleme bei der Führung der Lagerbehälterdatei durch die Aufnahme einer klarstellenden Vorschrift in die Lagerverordnung zu lösen, die der Senatsverwaltung die zentrale Speicherung von Lagerbehälterdaten für Zwecke der Gewässeraufsicht erlaubt.

Bis 1984 hatten die Berliner Stadtreinigungs-Betriebe dem Senator für Stadtentwicklung und Umweltschutz eine Liste mit den **Abfallanlieferern** übersandt, aus denen dieser entnehmen konnte, welcher der Anlieferer die nach dem Abfallbeseitigungsgesetz erforderliche Transportgenehmigung nicht besaß. Darüber hinaus hatte der Umweltschutzsenator die Kraftfahrzeug-Handwerksinnung um Übermittlung von Anschriften und Unterlagen über solche Betriebe gebeten, die sich im weitesten Sinne mit Kfz-Reparaturen befaßten.

Demgegenüber habe ich empfohlen, daß die Stadtreinigung zukünftig die entsprechenden Daten bei den Abfallanlieferern zugleich im Auftrag des Senators für Stadtentwicklung und Umweltschutz erhebt und die anliefernden Unternehmen auf dieses Auftragsverhältnis und auf ihr Auskunftsverweigerungsrecht gegenüber der Überwachungsbehörde hinweist. Da der Abfallanlieferer in jedem Fall verpflichtet ist, Angaben zur Person zu machen, kann der Senator für Stadtentwicklung und Umweltschutz in den Fällen der Auskunftsverweigerung selbständig ermitteln, ob die erforderliche Transportgenehmigung vorgelegen hat.

Eine Übermittlung von Daten über Kfz-Handwerksbetriebe durch die betreffende Innung ist dagegen in keinem Fall zulässig. Weder die Handwerksordnung noch die entsprechende Innensatzung enthalten Auskunftspflichten gegenüber der abfallrechtlichen Überwachungsbehörde. Eine Datenübermittlung ist zudem nicht erforderlich, da der Senator für Stadtentwicklung und Umweltschutz auf diese Daten durch Einsichtnahme in die Handwerksrolle zugreifen kann. Zudem würde die Senatsverwaltung über die Handwerksinnung nicht Informationen über alle Handwerksbetriebe erhalten, da die Innung nur ein freiwilliger Zusammenschluß ist.

Gegen die im Auftrag des Senators für Stadtentwicklung und Umweltschutz von einer privaten Firma durchgeführte Befragung aller Industriebetriebe zur **Erstellung eines Abfallkatasters** des Landes Berlin habe ich keine Einwände erhoben. Ich habe jedoch darauf hingewiesen, daß die Industriebetriebe zur Auskunft über Abfalltransporteure und -beseitiger nicht verpflichtet sind.

Zu dem Vorhaben des Senats, aufgrund eines „**Altlasten-Suchkonzepts**“ aus dem Jahre 1982 belastete Flurstücke im Liegenschaftskataster mit Kennzeichen zu versehen, stimme ich mit dem Senator für Bau- und Wohnungswesen und dem Senator für Stadtentwicklung und Umweltschutz darin überein, daß die grundstücksbezogene Veröffentlichung von Altlasten im Liegenschaftskataster einer Rechtsgrundlage bedarf, die gegenwärtig fehlt. Ich habe empfohlen, diese Frage im Vermessungsgesetz bereichsspezifisch zu regeln.

4.7 Datenschutz im Kreditwesen

Schufa

Starke Beachtung in der Öffentlichkeit fand das Urteil des Bundesgerichtshofes¹⁾, das die von der Kreditwirtschaft bisher verwendete Klausel für unwirksam erklärt. Der Bundesgerichtshof führte folgende Gründe an:

Eine pauschale Übermittlung von Konto- bzw. Kreditdaten sei mit § 24 Bundesdatenschutzgesetz, der eine Interessenabwägung im Einzelfall fordere, nicht vereinbar. Zudem könne vom Kunden auch nicht ohne weiteres der Verzicht auf die Wahrung des Bankgeheimnisses verlangt werden. Die Schufa-Klausel benachteilige damit den Kunden unangemessen und verstoße gegen das Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen.

Daraus folgt nicht, daß jede Weitergabe an die Schufa und jede Auskunft von der Schufa zu untersagen war. Jedoch war die Datenweitergabe neu zu regeln. Die Vertreter der Datenschutzaufsichtsbehörden, der Kreditinstitute und der Schufa erzielten Einvernehmen über eine neue Schufa-Klausel. Die wichtigsten Regelungen:

- Grundlage der Übermittlung an die Schufa ist eine ausführliche Vertragsbestimmung, in die der Kunde schriftlich einwilligt;
- der Kunde wird umfassend über das Verfahren aufgeklärt, zusätzlich kann er sich durch Merkblätter weiter informieren;
- Daten über die Aufnahme und ordnungsgemäße Abwicklung einer Geschäftsverbindung (Konto, Kredit, Bürgschaft) dürfen nur mit schriftlicher Einwilligung des Kunden übermittelt werden (sogenannte Positivmerkmale);
- anders ist es bei Angaben über vertragswidriges Verhalten eines Kunden, z. B. beim Scheckkartenmißbrauch und bei der Durchführung von Vollstreckungsmaßnahmen. Hier hat eine Interessenabwägung im Einzelfall stattzufinden, bei der die Belange des Kunden mit denen der Kreditwirtschaft zu vergleichen sind. Eine Übermittlung an die Schufa kommt in Betracht, wenn nach dem Ergebnis der Abwägung die Interessen der Allgemeinheit bzw. der Kreditwirtschaft gegenüber den Belangen des Kunden überwiegen;
- der Kreis der Anschlußfirmen der Schufa ist auf solche Unternehmen beschränkt worden, die Geld- oder Warenkredite gewähren. Die Zahl der Anschlußfirmen ist damit erheblich reduziert worden.

Angesichts der großen Zahl von Kunden war es aus praktischen Gründen nicht möglich, nachträgliche Einwilligungen einzuholen. Die Kunden sind aber auf die neue Situation hingewiesen worden und haben die Möglichkeit, dem Übermittlungsverfahren zu widersprechen.

Allerdings ist abzusehen, daß Kunden, die dem Schufa-Verfahren widersprechen, Schwierigkeiten haben werden, ein Konto zu eröffnen oder einen Kredit zu erhalten, da die Kreditinstitute sich über die Bonität der Kunden informieren wollen.

Ich vertrete nach wie vor die Auffassung, daß dem Kunden ein „schufaloses Konto“ angeboten werden sollte, wie dies vereinzelt bereits bei anderen Instituten geschieht.

Geldautomaten

Aus vielen Eingaben ist mir bekannt, daß Zweifel an der Benutzungssicherheit der Geldautomaten bestehen. Die Presse berichtete mehrfach, daß Manipulationen möglich seien. Klare Beweise liegen jedoch nicht vor. Viele Bürger befürchten auch, daß bei Verlust oder Diebstahl der Scheckkarte das Konto leergeräumt werden könnte.

Viele Kunden der Kreditinstitute legen auch gar keinen Wert darauf, den Service des Geldautomaten zu nutzen. Die Auffassung dieser Personen sollte künftig mehr berücksichtigt werden. Die Kreditinstitute sollten ein Risiko - des Verlustes, der Mani-

pulation - nicht auf den Kunden übertragen, der die Service-Leistungen der Scheckkarte gar nicht in Anspruch nehmen will.

Ich empfehle daher, dem Kunden die Möglichkeit einzuräumen, eine magnetstreifenlose Karte zu erhalten.

Diskretion

Seit langem setze ich mich gegenüber der Sparkasse der Stadt Berlin West dafür ein, Verbesserungen des Datenschutzes bei der persönlichen Abwicklung von Bankgeschäften zu erreichen. Die Sparkasse hat zusätzliche Maßnahmen ergriffen. So wird Kunden der Berliner Sparkasse aufgefallen sein, daß an den Bankschaltern seit einiger Zeit Hinweisschilder mit der Aufschrift „Diskretion - Bitte Abstand halten“ angebracht sind.

Im Juni informierte die Sparkasse ihre Kunden zusätzlich über ihre Maßnahmen zur Sicherstellung und Verbesserung der Vertraulichkeit beim Umgang mit finanziellen Angelegenheiten und verwies darauf, daß dazu auch die Unterstützung der Kunden notwendig sei. Zudem werden zu diesem Thema Schulungsmaßnahmen für die Mitarbeiter durchgeführt.

Neues Rechenzentrum

Die Sparkasse errichtet in der Nähe der Zentrale ein Technisches Zentrum, das das Rechenzentrum und auch Teile der Verwaltung beherbergen soll. Bei einem Informationsgespräch zeigte es sich, daß die Konzeption des Rechenzentrums einwandfrei gelöst ist. Datenschutzrechtliche und sicherheitstechnische Probleme traten nicht zutage.

5. Nachtrag zu Feststellungen aus den Vorjahren

Soweit Nachträge zu Feststellungen aus den Vorjahren nicht bereits im Zusammenhang mit den einzelnen Punkten dieses Berichts erfolgten, werden sie im folgenden Abschnitt zusammengefaßt.

Übersendung von ISVB-Ausdrucken an die Staatsanwaltschaft (Jahresbericht 1984, Ziff. 2.4)

Bereits in seiner Stellungnahme zu meinem Jahresbericht 1984 hat der Senat festgestellt, daß die Praxis des Polizeipräsidenten, den an die Staatsanwaltschaft zu übersendenden Ermittlungsakten jeweils einen kompletten Ausdruck aus dem Informationssystem Verbrechensbekämpfung beizufügen, nicht erforderlich ist. Insbesondere Daten zur Gefahrenabwehr dürfen den Strafverfolgungsbehörden nur übermittelt werden, soweit es für deren Tätigkeit nötig ist. Das Verfahren wurde nunmehr geändert. Künftig werden nur noch folgende Daten von der Polizei an die Staatsanwaltschaft weitergegeben:

- Bestrafungen - unter Berücksichtigung der Straftilgungsfristen -;
- Erkenntnisse über abgeschlossene Ermittlungsverfahren gegen den Beschuldigten;
- im Einzelfall erforderliche personengebundene Hinweise.

Diese Daten werden zur Ermittlungsakte genommen, so daß sie dem Einsichtsrecht des Verteidigers unterliegen, wodurch die Waffengleichheit der Prozeßbeteiligten gewährleistet ist.

Datei der Taxifahreranmeldungen (Jahresbericht 1981, Ziff. 2.8; Jahresbericht 1984, Ziff. 5)

Aufgrund der Klage eines Taxi-Unternehmers gegen die Regelung der Taxenordnung, wonach eine Verpflichtung zur namentlichen Benennung aller Fahrzeugführer besteht, hatte das Verwaltungsgericht Berlin über die Rechtmäßigkeit dieser Vorschrift zu entscheiden. Das Gericht kam zu dem Ergebnis, daß die in der Taxenordnung vorgesehene Meldepflicht nicht von den in der Verordnung benannten Ermächtigungsgrundlagen im Personenbeförderungsgesetz gedeckt ist. Der Ordnungsgeber sei gehalten, Regelungen zur Betriebspflicht, d. h. zum ordnungsgemäßen, den örtlichen Verhältnissen anzupassenden Taxenverkehr, zu schaffen. Die betriebsinterne Organisation bleibe dagegen den Unternehmern überlassen.

Über die vom Polizeipräsidenten gegen dieses Urteil eingelegte Berufung ist noch nicht entschieden.

¹⁾ BGH III ZR 213/83, NJW 1986, S. 46 ff.

Rückverteilung von Lohnsteuerkarten (Jahresbericht 1980, Ziff. 2.6; Jahresbericht 1981, Ziff. 2.3)

In Zusammenarbeit mit dem Senator für Inneres wurde erreicht, daß künftig zumindest das Landesverwaltungsamt Berlin alle Lohnsteuerkarten in der Gehalts- und Lohnstelle einzeln - in Fensterbriefumschlägen - kuvertieren und an die jeweiligen Büroleitungen übersenden wird, die dann wiederum entsprechend ihrem Verteilungssystem diese an die Beschäftigten weiterleiten. Dieses neue Verfahren soll bereits bei der Rückverteilung der Lohnsteuerkarten 1986 im Bereich der Abrechnungsstelle Landesverwaltungsamt Berlin Anwendung finden.

Ebenso wird das Landesverwaltungsamt auch bei der Rückverteilung der Entgeltbescheinigungen der VBL das obengenannte Verfahren anwenden.

Wählerverzeichnisse (Jahresbericht 1985, Ziff. 4.3)

Noch rechtzeitig vor den allgemeinen Wahlen zu den Personalräten der Behörden Berlins 1986 hat der Senator für Inneres durch Rundschreiben vom 10. September 1986 die Empfehlung herausgegeben, in die auszulegenden Wählerverzeichnisse über Namensangaben hinaus grundsätzlich nur noch Hinweise auf den jeweiligen Dienst- oder Arbeitsbereich aufzunehmen.

Damit hat er sich meiner Auffassung angeschlossen, daß auf Angaben der Geburtsdaten und Wohnanschriften schon deshalb regelmäßig verzichtet werden muß, weil weder das Personalvertretungsgesetz noch die Wahlordnung Hinweise über den Inhalt der Wählerverzeichnisse geben und insoweit nach datenschutzrechtlichen Grundsätzen der Datenumfang auf das erforderliche Maß reduziert bleiben muß.

Sozialhilfestatistik (Jahresbericht 1981, Ziff. 2.5)

Die Datenerhebung im Rahmen der Sozialhilfestatistik wurde gegenüber den Vorjahren dadurch datenschutzgerechter gestaltet, daß das Statistische Landesamt nicht mehr das Aktenzeichen des jeweiligen Sozialhilfefalles mit dem Geburtsdatum des Hilfeempfängers erhält. Im Zählblatt wird lediglich die Telefonnummer des Sachbearbeiters vermerkt, bei dem aufgrund der Plausibilitätskontrolle in ca. 10% der Fälle Rückfragen erforderlich sind.

Personaldaten (Jahresbericht 1985, Ziff. 4.3)

Bei einer Einrichtung einer Universität hatte ich beanstandet, daß ein für Einzelpersonalangelegenheiten unzuständiges Organ regelmäßig eine personenbezogene monatliche Gesamtübersicht über das Personal der Einrichtung erhielt. Dieser Mangel wurde durch Anonymisierung der monatlichen Gesamtübersicht abgestellt.

6. Zusammenarbeit mit anderen Stellen

Datenschutzbeauftragte des Bundes und der Länder

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in fünf Sitzungen unter Vorsitz des Niedersächsischen Datenschutzbeauftragten beraten. Die wichtigsten Ergebnisse lassen sich wie folgt zusammenfassen:

25. Konferenz am 27. Januar 1986:

- Entschließung zu den „Sicherheits- und Datenschutzgesetzen“

26. Konferenz am 14. März 1986:

- Entschließung zur Änderung des Bundesdatenschutzgesetzes
- Entschließung zum Datenschutz im Krankenhaus

27. Konferenz am 18. April 1986:

- Entschließung zur Änderung des Bundesverfassungsschutzgesetzes

- Entschließung zum Entwurf einer Telekommunikationsordnung

28. Konferenz am 24./25. November 1986:

- Entschließung zu Datenschutzvorschriften in der Strafprozeßordnung

Der Konferenzvorsitz wird mit dem Jahreswechsel turnusgemäß auf den Landesbeauftragten für den Datenschutz des Landes Nordrhein-Westfalen übergehen.

Abgeordnetenhaus

Die gute Zusammenarbeit mit dem Abgeordnetenhaus konnte weiter fortgesetzt werden. Einen Schwerpunkt bildete die Beratung im **Unterausschuß Berichte des Berliner Datenschutzbeauftragten** des Ausschusses für Inneres, Sicherheit und Ordnung. Dieser hat sich in mehreren Sitzungen mit den Jahresberichten beschäftigt, die verbleibenden offenen Fragen behandelt und die anstehenden datenschutzrelevanten Gesetzesvorhaben erörtert. Hervorzuheben ist das Projekt eines Bibliotheks- und Archivgesetzes sowie die Fragen des Melderechts wie z. B. die Hotel- und Krankenhausmeldepflicht und der Umfang von Übermittlungen aus dem Melderegister. Eingehend erörtert wurde auch die Frage des Umgangs mit Personaldaten.

Eine immer wieder auftretende Fragestellung bei der parlamentarischen Ausschubarbeit ist **das Recht, Akten einzusehen** und die Bedeutung des Datenschutzes für diese Frage. Unbestritten ist, daß der Petitionsausschuß und die Untersuchungsausschüsse Aktenvorlagerechte besitzen, da dies rechtlich besonders geregelt ist. Die Frage, ob auch die übrigen Ausschüsse ein Aktenvorlagerecht haben, ist primär keine Datenschutzfrage, sondern betrifft die Regelung des Verhältnisses von Legislative und Exekutive. Dabei wird bisher davon ausgegangen, daß die Ausschüsse üblicherweise nur den Senator zitieren und zu bestimmten Sachen befragen können. Datenschutzfragen tauchen erst auf, soweit ein Einsichtsrecht bejaht wird. Dann muß nämlich geprüft werden, ob und inwieweit der Einsichtnahme in Akten besondere Persönlichkeitsrechte der Betroffenen oder Dritter entgegenstehen, insbesondere ob und inwieweit das Einverständnis dieser Personen eingeholt werden müßte.

Eine weitere Frage von allgemeiner Bedeutung war, ob und inwieweit personenbezogene Daten bei Antworten auf Kleine Anfragen verwendet werden dürfen.

So bat mich der Senator für Wissenschaft und Forschung um Stellungnahme zu der Frage, in welchem Umfang bei der **Beantwortung Kleiner Anfragen** detaillierte Auskünfte zu personalrechtlichen Einzelangelegenheiten von öffentlichen Bediensteten gegeben werden dürfen. In meiner Stellungnahme habe ich hervorgehoben, daß diese Frage bisher weder gesetzlich noch durch die Geschäftsordnung des Abgeordnetenhauses oder die Gemeinsame Geschäftsordnung für die Berliner Verwaltung geregelt ist. Das Persönlichkeitsrecht des Betroffenen ist deshalb mit dem Recht des einzelnen Abgeordneten auf Auskunftserteilung in der Weise abzuwägen, daß beide Rechtspositionen ihre Geltungskraft möglichst weitgehend behalten. Das Recht des öffentlichen Bediensteten auf informationelle Selbstbestimmung gebietet es nach meiner Auffassung jedenfalls, daß die Antwort auf eine ihn betreffende Kleine Anfrage nicht ohne seine Einwilligung in personenbezogener Form veröffentlicht wird. Eine dem § 50 Abs. 2 der Geschäftsordnung des Abgeordnetenhauses entsprechende Verfahrensweise, bei der die Antwort auf eine solche Kleine Anfrage mündlich in dem zuständigen Ausschuß des Abgeordnetenhauses in nichtöffentlicher Sitzung gegeben wird, hielt ich datenschutzrechtlich während einer Übergangszeit für hinnehmbar. Letztlich ist jedoch der Gesetzgeber auch in diesem Bereich gehalten, die Offenbarung personenbezogener Daten bereichsspezifisch und normenklar gesetzlich zu regeln.

Im Einzelfall kann ausnahmsweise das Persönlichkeitsrecht des Betroffenen aufgrund besonderer Umstände hinter dem Recht des einzelnen Abgeordneten auf öffentliche Beantwortung seiner Anfrage zurücktreten. Ein solcher Fall wäre z. B. gegeben, wenn

die Offenbarung der personenbezogenen Daten dazu dient, unwahre Tatsachenbehauptungen richtigzustellen, die der Betroffene selbst veröffentlicht hat (vgl. § 69 Abs. 1 Nr. 3 SGB X).

Wie in den vergangenen Jahren arbeitete ich in Einzelfällen auch mit dem **Petitionsausschuß** zusammen. Schließlich habe ich mich bei einem informatorischen Besuch in der Geschäftsstelle und im Geheimschutzraum des **I. Untersuchungsausschusses der 10. Wahlperiode** zur Aufklärung der Hintergründe von öffentlichen Entscheidungen im Berliner Bau- und Grundstücksbereich davon überzeugt, daß die erforderlichen Datensicherungsmaßnahmen in vollem Umfang getroffen wurden.

Aufsichtsbehörde für nichtöffentliche Stellen

Im Rahmen der guten Zusammenarbeit mit der Aufsichtsbehörde für den Datenschutz beim Senator für Inneres wurden Fragen des Datenschutzes im Krankenhaus, des Schufa-Verfahrens und der Koordination bei der Anbieterkontrolle im Bildschirmtext behandelt.

7. Aufgaben des Berliner Datenschutzbeauftragten

7.1 Im Berichtsjahr 1986

Die Zahl der schriftlichen **Eingaben** entspricht denen des Vorjahres. Sie entfallen nach der Häufigkeit geordnet insbesondere auf folgende Gebiete:

1. Öffentliche Ordnung
2. Bezirke
3. Öffentliche Sicherheit
4. Körperschaften/Anstalten/Stiftungen
5. Gesundheit und Soziales
6. Justiz

Ähnlich wie im Vorjahr haben sich bei mehr als 50 % der Eingaben Mängel herausgestellt. Den Bund, die Kirchen, den SFB und den Bereich der Privatwirtschaft betreffende Eingaben habe ich an die zuständigen Stellen abgegeben.

Eine steigende Zahl von Vorgängen wurden wiederum als **Beratungsersuchen** (§ 21 Abs. 1 Satz 2 Berliner Datenschutzgesetz)

an mich herangetragen. Im technischen Bereich haben sich die Beratungsersuchen sogar mehr als verdoppelt.

Das von mir zu führende **Dateienregister** enthält nunmehr 1 454 (Stand: 15. Oktober 1986) Dateien (Vorjahr: 1 234) von 303 (269) speichernden Stellen. Damit konnte der Überblick über die automatisierten Dateien des öffentlichen Bereichs in Berlin noch weiter verbessert werden. Man kann feststellen, daß die mit der gesetzlichen Verpflichtung zur Führung des Dateienregisters verfolgten Zwecke nunmehr annähernd erreicht sind. Die befriedigende Durchsetzung der gesetzlichen Regelung hat allerdings sieben Jahre gedauert. Die Behörden haben in der Regel einen Überblick über ihre eigene Datenverarbeitung; Art und Umfang der automatisierten Datenverarbeitung sind darüber hinaus gegenüber dem Bürger und vor allem auch gegenüber den Kontrollbehörden transparenter geworden. Das 1985 von mir erstellte Verzeichnis zum Dateienregister ist wegen der zahlreichen Änderungen neu herausgegeben worden.

7.2 Voraussichtliche Schwerpunkte

Aufgrund der bisherigen Erfahrung ergeben sich folgende Schwerpunkte für das Jahr 1987:

- a) Erledigung der Anliegen, die die Bürger mit ihren Eingaben verfolgen,
- b) Überprüfung von Amts wegen und Beratung bei
 - der Vorbereitung und Durchführung der Volkszählung in den Bezirksämtern und dem Statistischen Landesamt
 - der Anwendung der Datenfernverarbeitung, insbesondere bei der Planung zum Aufbau eines Verwaltungsnetzes in Berlin
 - weiteren öffentlichen Stellen, wie den Bezirksämtern,
- c) Werbung für die zügige Verwirklichung der auf Landesebene erforderlichen bereichsspezifischen Regelungen.

Berlin, den 16. Dezember 1986

Der Berliner Datenschutzbeauftragte
Dr. Kerkau

Anlage 1

**Entschließung der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 27. Januar 1986
zu den „Sicherheitsgesetzen“**

Die Datenschutzbeauftragten erinnern an ihre Entschließungen zu den Auswirkungen des Volkszählungsurteils des Bundesverfassungsgerichts, zur Einführung eines maschinenlesbaren Personalausweises und zur Datenverarbeitung bei Polizei und Verfassungsschutz. Sie stellen fest, daß die angekündigten Datenschutz- und Sicherheitsgesetze den von ihnen erhobenen Forderungen nur sehr unzureichend Rechnung tragen und den Vorgaben des Bundesverfassungsgerichts nur teilweise entsprechen. Die geplanten Regelungen haben erhebliche Konsequenzen für die Datenverarbeitung in den Ländern und präjudizieren die Landesgesetzgeber in vielerlei Hinsicht.

Die Datenschutzbeauftragten des Bundes und der Länder sehen sich zu folgender erster Bewertung veranlaßt:

1. Zum Bundesdatenschutzgesetz

- Das Recht auf informationelle Selbstbestimmung gilt für jeglichen Umgang mit personenbezogenen Daten. Daher ist es nicht gerechtfertigt, die Beschränkung des Bundesdatenschutzgesetzes auf Dateien festzuschreiben und die Datenerhebung auszugrenzen. Die vorgeschlagenen Regelungen im Verwaltungsverfahrensgesetz sind kein ausreichender Ersatz, weil wichtige Verwaltungsbereiche, wie z. B. die Finanzbehörden, ausgenommen sind und die Datenverarbeitung in Akten und anderen Unterlagen der Datenschutzkontrolle weitgehend entzogen wird.
- Das Auskunftsrecht des Bürgers bleibt stark eingeschränkt.
- Unbefriedigend ist auch, daß der Datenschutz im nicht-öffentlichen Bereich insgesamt nicht verbessert wird.

2. Zum Personalausweisgesetz und Paßgesetz

- Die Einführung des maschinenlesbaren Ausweises verändert entscheidend die Bedingungen, unter denen Informationen über die Bürger im Sicherheitsbereich erhoben und verarbeitet werden.
Mit seiner Hilfe soll die Polizei vorhandene Dateien automatisiert abrufen und abgleichen sowie neue Datensammlungen anlegen können.
Der behauptete Sicherheitsgewinn ist bis heute nicht dargestellt.
- Darüber hinaus fehlt es an bereichsspezifischen Gesetzen, die den Umgang der Sicherheitsbehörden mit dem Ausweis regeln, wie sie auch der Deutsche Bundestag in seiner Entschließung vom 17. Januar 1980 gefordert hat. Die jetzt diskutierten Begleitgesetze einschließlich der

Ergänzung der Strafprozeßordnung genügen den Anforderungen nicht. Dies gilt umso mehr, als auch unverdächtige Bürger betroffen sind.

- Die Gefahren wachsen, wenn die gleichzeitig beabsichtigte automatisierte Nutzung des Verkehrszentralregisters in der vorgesehenen Form verwirklicht und der Datenverbund der Sicherheitsbehörden untereinander weiter ausgebaut wird.

3. Zum Bundesverfassungsschutzgesetz

Auch für den Verfassungsschutz gilt, daß seine Aufgaben im Gesetz klar in eine für den Bürger nachvollziehbare Weise zu beschreiben sind. Gerade weil seine Tätigkeit weitgehend im Geheimen stattfindet, müssen die Bürger die Gewißheit haben, daß der Verfassungsschutz an eindeutige, eng umrissene und abschließend geregelte Aufgaben und Befugnisse gebunden ist. Der vorliegende Entwurf verfehlt dieses Ziel. Weitere schwerwiegende Mängel kommen hinzu:

- Dem Bürger kann nach wie vor jegliche Auskunft verweigert werden.
- Es fehlen gesetzliche Fristen für die Löschung gespeicherter Daten.
- Dem Verfassungsschutz darf nicht das Recht zugestanden werden, in jedes amtliche Datenregister Einblick zu nehmen und jede Art von Daten anzufordern. Im Gesetzesentwurf sind davon nicht einmal Gesundheits- und Steuerdaten ausgenommen.
- Während sich das Nachrichtendienstliche Informationssystem (NADIS) bisher nur auf die Speicherung von Aktennachweisen beschränkte, sollen nach dem Gesetzesentwurf auch Textzusätze über den Bürger automatisiert den Nachrichtendiensten bundesweit zur Verfügung stehen. Damit werden zu Lasten des Bürgers Akteninhalte verkürzt und aus ihrem Entstehungszusammenhang herausgenommen.

4. Zur Zusammenarbeit von Nachrichtendiensten und Polizei

- Die rechtsstaatlichen Gremien der Zusammenarbeit von Nachrichtendiensten und Polizei werden für das Trennungsgebot bestimmt. Das Trennungsgebot erschöpft sich nicht in einer bloßen organisatorischen Trennung zwischen Nachrichtendiensten und Polizei. Gerade wegen der amtlichen Datenverarbeitung kommt es mindestens ebenso auf eine strikte Trennung der Informationsbestände an. Das Trennungsgebot darf nicht durch einen umfassenden Informationsaustausch unterlaufen werden.
- Im übrigen darf eine Zusammenarbeit zwischen Polizei, MAD, Verfassungsschutz und BND erst erfolgen, wenn für die einzelnen Dienste eindeutige auch den Datenschutz sichernde Rechtsgrundlagen geschaffen sind.

Anlage 2

**Entschließung der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder vom 18. April 1986
zur Änderung des Bundesverfassungsschutzgesetzes**

Die Datenschutzbeauftragten beurteilen den Entwurf zur Novellierung des Bundesverfassungsschutzgesetzes (Drs. 10/4737) nach den Grundsätzen des Volkszählungsurteils des Bundesverfassungsgerichts, den Notwendigkeiten, die sich aus der technischen Entwicklung der Informationsverarbeitung ergeben und den Forderungen, die sie bereits in früheren Entschließungen formuliert haben. Sie messen ihn auch an der Erklärung der Bundesregierung, den Datenschutz im Interesse der Bürger zu verbessern und die Datenverarbeitung transparenter zu gestalten.

Der Entwurf wird den sich aus dem Urteil des Bundesverfassungsgerichts zum Volkszählungsurteil ergebenden Anforderungen nicht gerecht. Seine Vorschriften müssen schon deshalb wesentlich präziser gefaßt werden, weil die Arbeit des Verfassungsschutzes vorwiegend unter Ausschluß der Öffentlichkeit und der Kontrolle der betroffenen Bürger stattfindet.

Hauptkritikpunkte sind:

1. Da sich der zulässige Umfang der Informationsverarbeitung maßgeblich nach den Aufgaben der datenverarbeitenden Stelle bemißt, bedarf es einer möglichst genauen gesetzlichen Beschreibung dieser Aufgaben. Die in § 3 Abs. 1 verwendeten Begriffe wie etwa „Bestrebungen gegen die frei-

heitlich-demokratische Grundordnung" oder „Gefährdung auswärtiger Belange" sind unpräzise.

Unklar bleibt weiterhin, unter welchen Voraussetzungen „beeinflusste" Organisationen beobachtet werden dürfen und wie weit hierbei die Beobachtung auf Einzelpersonen ausgedehnt werden darf. Für den einzelnen muß feststellbar sein, wann er die Schwelle von der Ausübung der Grundrechte zur verfassungsfeindlichen Bestrebung überschreitet.

Auf jeden Fall ist es notwendig, die Voraussetzungen für die Erhebung, Speicherung und sonstige Verwendung personenbezogener Daten im Rahmen der Erfüllung dieser Aufgaben präziser und für den Bürger transparent zu regeln. Begriffe wie „Aufgaben des Verfassungsschutzes" und „Zwecke des Verfassungsschutzes" sind nicht hinreichend bestimmt.

Die Mitwirkung der Verfassungsschutzbehörden an der Überprüfung von Personen durch andere Stellen muß im Verfassungsschutzgesetz abschließend geregelt werden. Sofern über die Sicherheitsüberprüfung (§ 3 Abs. 2) hinaus eine Mitwirkung an anderen Verfahren wie etwa bei Einbürgerungen, Asylverfahren, Ordensverleihungen oder der Überprüfung von Bewerbern für den öffentlichen Dienst für unabdingbar gehalten wird, sind diese im Gesetz ausdrücklich zu nennen. Auch die damit im Zusammenhang stehende Datenverarbeitung ist im Verfassungsschutzgesetz präzise zu regeln. Unabhängig davon ist für die Sicherheitsüberprüfungen und jedes andere Verfahren zur Überprüfung von Personen eine bereichsspezifische Regelung erforderlich.

2. Der im Entwurf vorgesehene Informationsaustausch der Verfassungsschutzbehörden untereinander (§ 4 Abs. 1) ist zu umfassend und bedarf einer aufgabenbezogenen Einschränkung. Er ist nur zulässig, soweit Informationen für die jeweilige Aufgabenerfüllung der einzelnen Verfassungsschutzbehörden erforderlich sind. So dürfen beispielsweise die aus einer Telefonüberwachung gewonnenen Daten auch zwischen Verfassungsschutzbehörden nur unter den engen Voraussetzungen des § 7 Abs. 3 G 10 ausgetauscht werden.

Besondere datenschutzrechtliche Risiken birgt die Aufnahme von Textzusätzen aus Akten der Verfassungsschutzbehörden in automatisierte Dateien. Damit werden zu Lasten des Bürgers Akteninhalte verkürzt und aus ihrem Entstehungszusammenhang herausgenommen. Sollten trotz dieser Bedenken Textzusätze in eingeschränktem Umfang zugelassen werden, ist es über die bereits im Entwurf getroffenen Beschränkungen und Schutzvorkehrungen hinaus unerlässlich, in der Datei die für die Bewertung und Überprüfung solcher Textzusätze maßgeblichen Unterlagen anzugeben. Entscheidungen dürfen auf diese Textzusätze allein nicht gestützt werden. Die im Gesetz gewollte Begrenzung auf Spionageabwehr und Terrorismusbekämpfung wird nicht erreicht, weil der Gewaltbegriff nicht einschränkend definiert ist.

3. Die in § 5 und § 6 Abs. 2 vorgesehene Befugnis, nachrichtendienstliche Mittel einzusetzen, entspricht nicht dem Grundsatz der Normenklarheit. Zumindest sind die wichtigsten Mittel im Gesetz aufzuzählen. Auch zum Zwecke der Datenschutzkontrolle sollte daneben die interne Festlegung der zulässigen Mittel und die Dokumentation ihres Einsatzes im einzelnen vorgeschrieben werden. Angesichts der Schwere des mit der Anwendung nachrichtendienstlicher Mittel verbundenen Eingriffs in das Persönlichkeitsrecht darf sich ihr Einsatz grundsätzlich nur gegen konkret verdächtige Personen richten. Entsprechend den Regelungen über die Post- und Telefonüberwachung sind Verwertungsbeschränkungen und eine Verpflichtung zur nachträglichen Unterrichtung des Betroffenen vorzusehen.
4. Die in § 6 Abs. 1 geregelte Befugnis zur Datenerhebung entspricht wegen der Bezugnahme auf die zu weitreichende Klausel „zur Erfüllung der Aufgaben der Verfassungsschutzbehörden erforderlich" nicht dem Grundsatz der Verhältnismäßigkeit. Die verfassungsrechtlich gebotene Güterabwägung im Einzelfall kann ergeben, daß vorrangige

Individualrechte einer personenbezogenen Erhebung entgegenstehen, so beispielsweise bei der Ausübung des Demonstrationsrechts (vgl. Brokdorf-Beschluß des Bundesverfassungsgerichts). Dies gilt gleichermaßen hinsichtlich solcher Personen, die selbst keinerlei verfassungswidriger Bestrebungen verdächtig sind.

5. Die in § 7 getroffene Regelung über die Speicherung, Veränderung und sonstige Nutzung personenbezogener Daten darf nicht – wie jetzt vorgesehen – auf Dateien beschränkt bleiben, zumal bei Verfassungsschutzbehörden ein Großteil der das Persönlichkeitsrecht der Bürger berührenden Daten in Akten geführt wird und komplexe Aktensammlungen bereits heute gezielt und mit Hilfe automatisierter Verfahren erschlossen werden können.

Im Bereich der Beobachtung verfassungswidriger Bestrebungen ohne Gewaltbezug sollte die personenbezogene Speicherungsbefugnis davon abhängig gemacht werden, daß der Extremismusbezug in der Person des zu Speichernden vorliegt.

Überdies muß die Vorschrift um die Festlegung von Überprüfungs- und Lösungsfristen, differenziert nach den einzelnen Aufgabenbereichen, erweitert werden.

6. Der Entwurf will in § 8 die Verpflichtung anderer Behörden, den Verfassungsschutz über eigene Wahrnehmungen von sich aus zu unterrichten, auf Erkenntnisse aus den Bereichen Spionage und Terrorismus beschränken, ohne jedoch – wegen des zu weiten Gewaltbegriffs – dieses Ziel voll zu erreichen. Die darüber hinaus allen Behörden eingeräumte Befugnis, dem Verfassungsschutz auch Informationen über gewaltfreie extremistische Bestrebungen zuzuleiten, birgt in dieser uneingeschränkten Form die Gefahr in sich, daß ein Klima allgemeiner Verdächtigungen entsteht. Auch vermag der Bürger, der in Kontakt mit einer Verwaltungsbehörde tritt, nicht zu erkennen, was diese wann und bei welcher Gelegenheit an die Verfassungsschutzbehörde übermittelt.

Schließlich fehlt in der Vorschrift eine Regelung, unter welchen Voraussetzungen Veränderungen des Sachverhalts der Verfassungsschutzbehörde nachzuberichten sind.

7. Die in §§ 9 und 16 des Entwurfs festgelegte Verpflichtung für alle übrigen öffentlichen Stellen, den Verfassungsschutzbehörden auf Ersuchen die zur Erfüllung ihrer Aufgaben erforderlichen Auskünfte zu erteilen, geht zu weit, da sie im Einzelfall z. B. der Zweckbindung widersprechen kann. Noch weniger hinnehmbar ist die vorgesehene pauschale Ermächtigung der Verfassungsschutzbehörde, in alle amtlich geführten Register Einsicht zu nehmen. Schließlich fehlt es auch an einer Regelung für die Übermittlung von Informationen durch andere Stellen, die diese aufgrund besonderer Eingriffsbefugnisse erlangt haben. Die in § 9 Abs. 2 vorgesehene Befreiung der Verfassungsschutzbehörde von der Verpflichtung, ihre Auskunftersuchen zu begründen, kann nur für die Fälle hingenommen werden, in denen Sicherheitsinteressen oder schutzwürdige Belange des Betroffenen einer Begründung entgegenstehen.
8. Angesichts des weitreichenden Auftrages der Verfassungsschutzbehörden zur Sammlung von Informationen bedürfen die dabei angefallenen personenbezogenen Erkenntnisse einer besonders strengen Abschottung nach außen. Dem trägt § 10 Abs. 1 des Entwurfs nicht hinreichend Rechnung, der es für eine Weiterleitung verfassungsschutzbehördlicher Erkenntnisse an andere öffentliche Stellen genügen läßt, daß die Daten dort im Rahmen der Aufgabenerfüllung für Zwecke der öffentlichen Sicherheit benötigt werden.

Die in § 10 Abs. 2 zugelassene Übermittlung von Daten der Verfassungsschutzbehörde an Dienststellen der Stationierungstreitkräfte muß angesichts der unübersehbaren Folgewirkungen und wegen der fehlenden Geltung deutschen Datenschutzrechts an besonders enge Voraussetzungen geknüpft werden. Zumindest ist in jedem Fall eine Abwägung mit den schutzwürdigen Belangen der Betroffenen vorzuschreiben.

Die Weitergabe von Erkenntnissen an private Stellen (§ 10 Abs. 3) muß auf die Fälle der Sicherheitsüberprüfung und der Spionage- bzw. Terrorismusabwehr beschränkt werden.

9. Die Übermittlung personenbezogener Daten durch das Bundesamt für Verfassungsschutz an die politische Führung (§ 11 Abs. 1) darf nur zugelassen werden, soweit dies für Zwecke der Aufsicht oder im Rahmen der politischen Berichtspflicht erforderlich ist. Darüber hinaus ist eine strenge Zweckbindung für die übermittelten Daten vorzusehen.

Die nach § 11 Abs. 2 zugelassene Unterrichtung der Öffentlichkeit über personenbezogene Daten muß die Ausnahme bleiben.

10. Die in § 14 auf automatisierte Dateien beschränkte Verpflichtung, Errichtungsanordnungen zu erstellen, muß auf alle Datensammlungen ausgedehnt werden. Die Unterrichtung des Datenschutzbeauftragten vor Aufnahme des Dateibetriebes ist vorzusehen. Schließlich ist gesetzlich sicherzustellen, daß die Frage der Notwendigkeit zur Weiterführung oder Änderung einer Datei in bestimmten Zeitabständen aufgabenbezogen überprüft wird.

Anlage 3

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. April 1986 zum Entwurf einer Telekommunikationsordnung (TKO) vom November 1985

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Absicht des Bundesministers für das Post- und Fernmeldewesen, die Bedingungen für die Benutzung der Einrichtungen für das Fernmeldewesen in einer einheitlichen Telekommunikationsordnung (TKO) neu zu regeln und an einer Stelle zusammenzufassen. Damit soll auch der technischen Entwicklung Rechnung getragen werden: Die Digitalisierung der Telekommunikation führt zu einer bisher nicht gekannten Speicherung von Verbindungs-, Abrechnungs- und Benutzungsdaten. Auch der Inhalt der Kommunikation wird zunehmend elektronisch gespeichert.

Das Bundesverfassungsgericht hat gerade vor dem Hintergrund der zunehmenden elektronischen Datenverarbeitung in seinem Urteil zum Volkszählungsgesetz 1983 die Bedeutung des Rechts auf informationelle Selbstbestimmung unterstrichen und daraus Grundsätze abgeleitet. Diese sind auch für die TKO von Bedeutung, da die Bürger auf die Inanspruchnahme der einzelnen Dienste in zunehmendem Maße angewiesen sind. Der Entwurf trägt diesen Anforderungen nicht hinreichend Rechnung:

1. Jeder der Telekommunikationsdienste birgt technisch bedingte Risiken in sich, die vom Teilnehmer nicht ohne weiteres erkennbar sind, bei der Nutzung aber berücksichtigt werden müssen. Deshalb sollte in die TKO eine Vorschrift aufgenommen werden, die die Deutsche Bundespost verpflichtet, die Teilnehmer des jeweiligen Dienstes über dessen wesentliche technische Bedingungen und Risiken bei der Benutzung des Telekommunikationsnetzes zu informieren und sie auf sicherheitsförderndes bzw. sicherheitsgefährdendes Nutzungsverhalten hinzuweisen.
2. Die in § 4 TKO genannten öffentlichen Telekommunikationsdienste werden nicht hinreichend präzise umschrieben. Diese Dienste dürfen nur zugelassen werden, soweit sich aus den ihren Einsatz regelnden gesetzlichen Bestimmungen die Voraussetzungen und der Umfang der Einschränkung des Rechts auf informationelle Selbstbestimmung klar und für den Bürger erkennbar ergeben.
3. Durch Veränderung der technischen und betrieblichen Funktionsbedingungen ist eine inhaltliche Umgestaltung einzelner Dienste ohne Änderung der entsprechenden Be-

stimmungen in der TKO möglich (§ 5 TKO). Eine derartige Ermächtigung der Deutschen Bundespost ist mit den Forderungen des Bundesverfassungsgerichts nach Transparenz der Datenverarbeitung und nach Schaffung einer normenklaaren gesetzlichen Grundlage für eine Einschränkung des Rechts auf informationelle Selbstbestimmung nicht vereinbar. Gleiches gilt für die Regelung des § 3 Abs. 1 Satz 3 der TKO, nach der das öffentliche Telekommunikationsnetz für sonstige, in der TKO nicht geregelte Telekommunikationszwecke freigegeben werden kann.

4. Die im Zusammenhang mit den öffentlichen Telekommunikationsdiensten maßgeblichen datenschutzrelevanten Begriffe wie „Teilnehmer“, „Anbieter“, „Abrechnungsdaten“, „Verbindungsdaten“, „Benutzungsdaten“ etc. sollten bei den nach § 2 TKO in einem Anhang zu dieser Verordnung festgelegten Begriffsbestimmungen aufgeführt werden. In einem Anhang sollten ferner die bei der Nutzung der einzelnen Dienste anfallenden personenbezogenen Daten erläutert werden. Nur so kann der Bürger als Nutzer der Öffentlichen Kommunikationsdienste entsprechend einer Forderung des Bundesverfassungsgerichts wissen, welche personenbezogenen Daten die Deutsche Bundespost wann und bei welcher Gelegenheit über ihn verarbeitet.
5. Wiederholt wird die Zulässigkeit der Verarbeitung personenbezogener Daten damit begründet, daß sie aus „betriebsbedingten Gründen“ erforderlich sei. Dieser Rechtsbegriff bedarf einer Definition in der TKO, aus der hervorgeht, welcher Art diese Gründe sein können, wobei die Eigenart der verschiedenen Dienste zu berücksichtigen ist.
6. Die Allgemeinen Vorschriften zum Datenschutz in Teil VI Abschnitt 2 TKO bedürfen der Ergänzung und Präzisierung:
 - Wann Bestandsdaten, Verbindungsdaten und Gebühren-daten zu löschen sind, ist teils überhaupt nicht, teils nur unbestimmt geregelt. So dürfen Verbindungsdaten aus „betriebsbedingten Gründen“ auf unbestimmte Zeit gespeichert werden. Gleiches gilt, wenn der Teilnehmer „eine andere Art der Verarbeitung“ beantragt hat; die Voraussetzungen hierfür werden nämlich nicht festgelegt.
 - Auch die Bestimmungen über die Verarbeitung der Gebühren-daten müssen so formuliert werden, daß keine unzulässigen Schlüsse auf ein Teilnehmerverhalten gezogen werden können.
 - Die Regelungen umfassen nicht alle bei der Post anfallenden Daten. Beispielsweise fehlen Regelungen zu den

Inhalten der Informationen und den beim Betrieb der Dienste anfallenden Daten.

- Die Vorschriften erlauben der Post, alle Daten zu beliebigen „Telekommunikationszwecken“ zu verwenden. Unerlässlich ist eine Nutzungsbeschränkung auf die Zwecke der jeweils in Anspruch genommenen Dienste.
- Die Regelung der Befugnis, Daten weiterzugeben, ist zu umfassend und unklar. Insbesondere sollten Verbindungsdaten von jeder Übermittlung ausgeschlossen bleiben.
- Trotz der Fülle und der besonderen Sensitivität der bei der Post vorhandenen personenbezogenen Daten fehlen spezielle Vorschriften über die Datensicherung.

Insgesamt dürfen die allgemeinen Datenschutzregelungen nicht hinter dem Standard der neuen Mediengesetzgebung zurückbleiben.

7. Auch die Regelungen zu den einzelnen Diensten berücksichtigen die Interessen der Bürger unzureichend:

- Beim Telefondienst ist der „Zwangseintrag“ der Teilnehmer im Telefonbuch vorgesehen. Insbesondere nach dem Volkszählungsurteil bestehen Zweifel, ob dies mit dem informationellen Selbstbestimmungsrecht noch vereinbar ist.
- Unter welchen Voraussetzungen die Post Daten über einzelne Telefonverbindungen, insbesondere die gewählte Rufnummer, registriert und an wen sie Auskunft darüber gibt, ist nicht geregelt. Das gleiche gilt für die sogenannte Fangschaltung. Beim Funktelefon speichert die Post ohne Rechtsgrundlage detaillierte Verbindungsdaten.
- Trotz seiner Annäherung an die Struktur der Datenschutzbestimmungen des Bildschirmtext-Staatsvertrages (Btx-StV) bleibt der Regelungsgehalt des § 387 TKO hinter Art. 9 Btx-StV zurück. Dies betrifft insbesondere die Regelung zu den Verbindungsdaten sowie Definition und Umfang der Vergütungsdaten. Ein klares Verbot der

Übermittlung von Vergütungsdaten an Dritte fehlt. Ferner fehlt ein Verbot der Übermittlung von Daten, die im Zusammenhang mit der Übermittlung von Mitteilungs- und Antwortseiten anfallen. Unzureichend ist auch der Umfang der technischen und organisatorischen Maßnahmen zur Datensicherung geregelt.

8. Abgesehen von Kritik an Einzelbestimmungen des Entwurfs der TKO bleiben wesentliche Fragen offen:

- Eine auf den Netzbereich beschränkte Regelung, für die allein der Bund zuständig ist, muß wesentliche Aspekte der Medienordnung ungeregt lassen. Auch die in die Länderkompetenz fallenden Nutzungs- und Anwendungsbereiche werfen Datenschutzprobleme auf, die von der jeweiligen Netzstruktur abhängig sind und die bereits bei der Konzeption der Dienste berücksichtigt werden müssen.
- Auch bei der in Aussicht genommenen Regelung weiterer Dienste (z.B. Breitbandkommunikationsdienste, Fernwirkdienste) sind entsprechende spezielle Datenschutzregelungen in die TKO aufzunehmen.
- Zur Fortentwicklung der datenschutzrechtlichen Möglichkeiten der TKO wird die Post aufgefordert, bei der Neu- und Umgestaltung einzelner Telekommunikationsdienste datenschutzfreundliche Lösungen zu realisieren. So sollten Überlegungen angestellt werden, ob nicht z. B. ein Dienst zur Verschlüsselung der Nachrichten sowie Verfahren der Gebührenzahlung bzw. -abrechnung beim Teilnehmer eingeführt werden können.
- In Anbetracht der Bedeutung einer künftigen Telekommunikationsstruktur und im Hinblick auf künftige Diensteneinführungsentscheidungen sind nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder verfassungsrechtliche Zweifel angebracht, ob die Verordnungsmächtigung aus § 14 PostVwG für die Regelung solcher wesentlichen Bereiche des öffentlichen Lebens bestimmender Sachverhalte noch als ausreichend anzusehen ist oder ob nicht vielmehr der Gesetzgeber die wesentlichen Entscheidungen treffen muß.

Anlage 4

**Entwurf einer Telekommunikationsordnung (E-TKO)
Ergänzungen zur Entschliebung der DSB-Konferenz
vom 18. April 1986 aufgrund der Neufassung des Entwurfs
vom April 1986**

Vorbemerkung

Die Neufassung des Entwurfs enthält eine Vielzahl von Änderungen, die im wesentlichen systematischer und terminologischer Art sind. Allerdings befinden sich hierunter einige Änderungen, die Gesichtspunkte der Entschliebung der DSB-Konferenz berücksichtigen. Grundsätzlich anzumerken ist, daß die Begründung zu den Änderungen, insbesondere zum Teil VII („Erläuterungen zu den im TKO-Entwurf vorgesehenen Änderungen“) kaum eine inhaltliche Argumentation enthält.

**1. Öffentliches Telekommunikationsnetz und technische und betriebliche Funktionsbedingungen
(§§ 3, 5 E-TKO; Ziff. 3, 8 der Entschliebung)**

Die Landesdatenschutzbeauftragten vertreten die Auffassung, daß bei der Einführung insbesondere neuer Mehrwertdienste (z. B. Bildschirmtext, Fernwirkdienste) den Ländern eine Gesetzgebungskompetenz zur Regelung der Nutzung zusteht. In Ziff. 8 der Entschliebung war hierauf hingewiesen worden.

§ 3 Abs. 1 Satz 2 der ursprünglichen Fassung des E-TKO sah vor, daß über die Benutzung des Netzes für öffentliche TKO-Dienste hinaus die Deutsche Bundespost auch Benutzungen für sonstige TKO-Zwecke zulassen kann. Die Neufassung beseitigt selbst dieses Zulassungserfordernis. Damit kann die Bundespost nicht mehr nur über die Ausweitung der Dienste entscheiden, sondern ihre Einführung wird in das Belieben Dritter gestellt. Dies wird bekräftigt durch die Möglichkeit, private Endstelleneinrichtungen mit entsprechenden Funktionen an das Netz anzuschalten (vgl. § 3 Abs. 2).

Demgegenüber wird in der Neufassung des § 5 Abs. 1 Satz 1 die Befürchtung entkräftet, die Bundespost könne durch eine Veränderung der technischen und betrieblichen Funktionsbedingungen eine inhaltliche Umgestaltung einzelner Dienste vornehmen: Nunmehr ist die Definitionsgewalt (die auch die Verarbeitung personenbezogener Daten umfassen kann) auf die Festlegung der jeweils erforderlichen Güte beschränkt.

**2. Definitionen
(§ 2 E-TKO Ziff. 4 der Entschliebung)**

Die Datenschutzbeauftragten hatten das Fehlen der Definitionen der für den Datenschutz wesentlichen Grundbegriffe zur Verordnung beanstandet. Nun wird neben den Definitionen im Anhang auch auf die Legaldefinitionen im Text verwiesen (§ 2). So sind die Begriffe „Teilnehmer“ in § 312, „Informationsanbieter“

ter" in § 355, „Verbindungsdaten" in § 383, „Gebührendaten" in § 383 bestimmt. Nach Mitteilung des Bundesbeauftragten für den Datenschutz ist die zusätzliche Herausgabe eines Sachweisers geplant.

Die notwendige Transparenz wird durch die Zersplitterung nicht erreicht, vielmehr sollten die wesentlichen Begriffe an einer Stelle leicht auffindbar definiert werden.

3. Verarbeitung personenbezogener Daten aus betriebsbedingten Gründen (§§ 383, 384 a E-TKO Ziff. 5 der Entschließung)

Die Datenschutzbeauftragten hatten kritisiert, daß eine präzise Zweckbestimmung aus diesem Begriff nicht entnommen werden kann. Nunmehr wird der Begriff nicht mehr verwendet, vielmehr wird er durch den Terminus „betrieblicher Grund" ersetzt. In dem neugeschaffenen § 384 a werden als Regelfälle für betriebliche Gründe, Störungseingrenzung und -beseitigung, die Verhinderung von Mißbrauch sowie die Netzoptimierung genannt. Obwohl damit die betrieblichen Gründe nicht abschließend definiert sind, stellt die Definition einen tragbaren Kompromiß zwischen dem Schutz vor unzulässiger Datenverarbeitung und der Notwendigkeit für die Post dar, auch bei einem unvorhergesehenen betrieblichen Erfordernis entscheidungsfähig zu sein. Maßgeblich bleiben die in § 384 a angeführten Gründe.

4. Speicherung und Löschung von Verbindungs- und Gebühren- daten (§§ 383, 384 E-TKO; Ziff. 6 Strich 1 der Entschließung)

§ 383 E-TKO eröffnet der Bundespost die rechtliche Möglichkeit, die technischen Voraussetzungen für die Speicherung von Verbindungsdaten zu schaffen. Dies steht in einem prinzipiellen Widerspruch zu der Forderung der Datenschutzbeauftragten nach nutzungsneutraler Abwicklung aller Dienste.

Dessenungeachtet hatten die Datenschutzbeauftragten mangelnde Präzision bei den Löschungsvorschriften kritisiert. Unter anderem waren **Verbindungsdaten** nur „so bald als möglich" zu löschen.

Der neueingefügte § 383 Abs. 2 E-TKO ordnet jetzt die Löschung von Verbindungsdaten grundsätzlich an. Als Ausnahme bleiben nur noch die Anonymisierung, Gebührenabrechnung (unter Umständen mit Einwilligung des Teilnehmers als Einzelgebühreennachweis, § 383 Abs. 2) und die in § 389 a definierten betrieblichen Gründe.

Im Gegenzug hat sich allerdings die Unklarheit, welche Voraussetzungen an die vom Teilnehmer beantragbare „andere Art der Verarbeitung" zu stellen sind, auf § 383 Abs. 1 verlagert. In diesem Punkt bleibt der E-TKO kritikwürdig.

Nach wie vor unklar bleibt darüber hinaus, ob auch außerhalb von „Netzknoten" Verbindungsdaten anfallen können bzw. wann diese Daten zu löschen sind.

Das Problem der Gebührendaten hat sich durch die Neufassung des § 384 Abs. 2 E-TKO verlagert. Durch Einfügung der Worte „der Fernmelderechnung" macht der zweite Absatz Rückschlüsse aus dem Abrechnungsformular über ein Nutzungsverhalten des Teilnehmers unmöglich. Er trifft jedoch im Gegensatz zur ursprünglichen Fassung keine Aussage mehr zum Schutz bei Entstehung der Daten. Diese dürfen nunmehr nach Absatz 1 der

Vorschrift ungehindert nach Art, Anzahl, Dauer usw. gespeichert werden. Der in der Ursprungsversion enthaltene Widerspruch zwischen Abs. 1 und Abs. 2 hat sich so zum Nachteil des Datenschutzes aufgelöst.

Für die Löschung der Gebührendaten wurde eine ausnahmslose Frist von 80 Tagen nach Absendung der Fernmeldeabrechnung festgelegt.

5. Nutzung und Weitergabe personenbezogener Daten (§ 385 E-TKO; Ziff. 6 Strich 4-5 der Entschließung)

Der Forderung der Datenschutzbeauftragten, die Nutzung der anfallenden personenbezogenen Daten (z. B. Weitergabe innerhalb der Post) auf die Zwecke der jeweils in Anspruch genommenen Dienste zu beschränken, wurde nicht nachgekommen.

Die Forderung der Datenschutzbeauftragten, die Verbindungsdaten von jeder Übermittlung auszuschließen, hat nach wie vor ihre Berechtigung. Auch in der neuen Fassung sieht § 383 Abs. 1 eine Übermittlung von Verbindungsdaten vor. Durch § 384 a ist die Übermittlung sonstiger Betriebsdaten zwar nunmehr geregelt, doch bleibt die Befugnis zur Weitergabe von Gebührendaten weiterhin unklar.

6. Inhalts- und Betriebsdaten (§ 385 E-TKO; Ziff. 6 Strich 3 der Entschließung)

Der Verdacht, die Regelungen umfaßten nicht alle bei der Post anfallenden Daten, wird beim neugefaßten § 385 Abs. 1 bestätigt. Die Verallgemeinerung des Datenbegriffs in der Neufassung bewirkt wegen der Formulierung „erhobene" Daten nunmehr eine Begrenzung der Zweckbindung auf erhobene Daten. Es ist jedoch erforderlich, die zweckgebundene Verwendung auf alle „anfallenden" Daten auszudehnen. So bedürfen z. B. die im Mitteilungsdienst anfallenden persönlichen Steuerinhalte eines Teilnehmers des gleichen Schutzes wie die „erhobenen Daten".

7. Datensicherung (§ 387 Abs. 5 E-TKO; Ziff. 6 Strich 6 der Entschließung)

In der Neufassung von § 387 Abs. 5 werden für Bildschirmtext Datensicherungsvorschriften in Anlehnung an Art. 9 Abs. 8 Btx-Staatsvertrag (allerdings ohne die Verpflichtung zur technischen Gewährleistung der Löschung von Verbindungsdaten) geschaffen. Eine entsprechende Regelung für andere Dienste fehlt nach wie vor.

Dies ist ein Indiz dafür, daß die Post nach wie vor Vorbehalte gegen eine grundsätzliche Verbesserung des Datensicherungsstandards hat.

8. Zwangseintrag im amtlichen Teilnehmerverzeichnis (§ 217 E-TKO; Ziff. 7 Strich 1 der Entschließung)

Der neue Absatz 6 a des § 217 beseitigt den Zwangseintrag bei Telefax, Btx, Daten- und Bildübermittlungsdienst. Die Forderung der Datenschutzbeauftragten, auf den Zwangseintrag beim Telefondienst zu verzichten, bleibt daher bestehen.

Auffällig ist, daß der Zwangseintrag nur bei den in erster Linie geschäftlich genutzten Diensten entfallen soll, nicht aber bei dem im privaten Bereich vorherrschenden Telefondienst.

Anlage 5

**Ausführungsvorschriften
über die Führung schriftlicher Unterlagen über Schüler
(AV - Schülerunterlagen)**

Vom 9. Juli 1986

SchuBSport II - C A 1

Tel.: 30 32 - 2 50 oder 30 32 - 1, intern 9 87 - 2 50

Auf Grund des § 59 Satz 1 des Schulgesetzes für Berlin (SchuLG) in der Fassung vom 20. August 1980 (GVBl. S. 2103), zuletzt geändert durch Gesetz vom 11. April 1984 (GVBl. S. 542), wird bestimmt:

1 - Geltungsbereich, Begriffsbestimmungen

- (1) Diese Ausführungsvorschriften gelten für die Berliner Schule, das Abendgymnasium, das Berlin-Kolleg, die Volkshochschullehrgänge zum nachträglichen Erwerb schulischer Abschlüsse und die Fachschulen. Diese Ausführungsvorschriften gelten nicht für Unterlagen des Schulärztlichen Dienstes und des Schulpsychologischen Dienstes, für Prüfungsunterlagen sowie für Zeugnisse.
- (2) Schule im Sinne der nachfolgenden Bestimmungen ist jede der in Absatz 1 erfaßten Einrichtungen; zu den Sonderschulen gehören auch die Sonderschuleinrichtungen. Schüler im Sinne der nachfolgenden Bestimmungen sind auch Hörer, Kollegiaten und Studierende.

2 - Grundsatz

- (1) Informationen über Schüler und den Unterricht, die in der Schule über einen längeren Zeitraum für die Unterrichts- und Erziehungsarbeit sowie für die notwendigen Verwaltungsarbeiten benötigt werden, sind schriftlich festzuhalten. In den nachfolgenden Bestimmungen ist geregelt, in welchen Fällen und in welchem Umfang dies zu geschehen hat.
- (2) Eintragungen, die unrichtig sind oder deren Aufnahme rechtswidrig war, sind zu berichtigen. Werden Eintragungen vom Schüler oder seinen Erziehungsberechtigten beanstandet, so sind diese zu überprüfen.
- (3) Folgende Unterlagen mit schriftlichen Angaben über Schüler und gegebenenfalls Unterricht werden geführt:
- a) in der Grundschule Schülerbogen, Klassenbuch, Klassenliste, Unterrichtsbuch für Fördermaßnahmen, Schülerkartei,
 - b) in der Hauptschule, der Realschule und im Gymnasium (Klassenstufen 7 bis 10) Schülerbogen, Klassenbuch, Klassenliste, Kurs- und Anwesenheitsnachweise bzw. Kursbücher, Schülerkartei,
 - c) in der Gesamtschule Schülerbogen, Kerngruppenbuch, Kerngruppenliste, Kursbücher, Schülerkartei,
 - d) in der gymnasialen Oberstufe Schülerbogen, Klassenbuch, Klassenliste, Kurs- und Anwesenheitsnachweise, Akten des pädagogischen Koordinators, Schülerkartei,
 - e) in den berufsbildenden Oberschulen einschließlich der Fachschulen, Schülerpersonalblatt, Klassenbuch, Klassenliste, Schülerkartei,
 - f) in den Sonderschulen Schülerbogen, sonderpädagogischer Beobachtungsbogen, Klassenbuch, Klassenliste, Schülerkartei,
 - g) in den Abendlehrgängen zum nachträglichen Erwerb des Haupt-, des erweiterten Haupt- und des Realschulabschlusses sowie in den entsprechenden Volkshochschullehrgängen Schülerakte, Klassenbuch, Klassenliste, Schülerkartei,
 - h) im Abendgymnasium im Berlin-Kolleg sowie in den Volkshochschulkollegs Schülerakte, Kurs- und Anwesenheitsnachweise, Akten des pädagogischen Koordinators, Schülerkartei.

In Gesamtschulen mit Ganztagsbetrieb werden von den Sozialpädagogen besondere Akten mit Angaben über Schüler geführt.

3 - Schülerbogen

- (1) Der Schülerbogen soll zum besseren Verständnis der Persönlichkeit des Schülers beitragen und dient zugleich als Unterlage für die Zusammenarbeit zwischen Schule und Elternhaus. Angaben über die persönlichen und häuslichen Verhältnisse des Schülers dürfen nur dann aufgenommen werden, wenn sie in Zusammenhang mit seiner schulischen Entwicklung stehen.
- (2) Der Schülerbogen (Vordruck) enthält die in der Anlage 1 aufgeführten Angaben. Die über den Schüler in der Schule entstandenen Unterlagen werden bei dem Schülerbogen aufbewahrt,

insbesondere Zeugnisabschriften, Empfehlung zum Schulanfang, Oberschulempfehlung, Unterlagen über das Verhalten des Schülers in der Schule einschließlich über etwaige Ordnungsmaßnahmen. Darüber hinaus wird dort der den Schüler betreffende Schriftverkehr gesammelt.

(3) Schülerbogen werden vom Klassenlehrer, Kerngruppenleiter oder Oberstufentutor geführt. Er hat alle Eintragungen selbst vorzunehmen; das Recht des Schulleiters, Eintragungen vorzunehmen, bleibt unberührt. Der Schulleiter überwacht die Führung der Schülerbogen. Er hat dafür Sorge zu tragen, daß die Schülerbogen nach einheitlichen Maßstäben insbesondere im Hinblick auf die Übersichtlichkeit der Anlagen geführt werden; Zeugnisabschriften sind getrennt von den übrigen Anlagen abzulegen. Ferner entscheidet er, wenn Zweifel bestehen, ob eine Eintragung vorgenommen oder Unterlagen zum Schülerbogen genommen werden sollen.

4 - Schülerpersonalblatt

- (1) In den berufsbildenden Schulen einschließlich der Fachschulen tritt an die Stelle des Schülerbogens das Schülerpersonalblatt. Nummer 3 gilt entsprechend, soweit in Absatz 2 nichts anderes bestimmt ist.
- (2) Das Schülerpersonalblatt besteht aus einem für alle berufsbildenden Oberschulen einschließlich Fachschulen gleichen Vorblatt und einer auf die Bedürfnisse des jeweiligen Bildungsganges zugeschnittenen Anlage. Vorblatt und Anlage können in einem Vordruck zusammengefaßt werden. Es enthält die in der Anlage 2 aufgeführten Angaben.

5 - Schülerakten

- (1) Schülerakten treten in den Einrichtungen des zweiten Bildungsweges an die Stelle der Schülerbogen. Sie enthalten Angaben wie die Schülerkartei (Nummer 9). Darüber hinaus wird der im Zusammenhang mit dem Schüler entstandene Schriftwechsel zu den Schülerakten genommen.
- (2) Nummer 3 Abs. 3 gilt entsprechend.

6 - Sonderpädagogischer Beobachtungsbogen

- (1) Der sonderpädagogische Beobachtungsbogen ergänzt den Schülerbogen um die Unterlagen, die sich aus der Behinderung des Schülers ergeben. Er ist Grundlage für sonderschulspezifische Entscheidungen, insbesondere über Rückschulungsmaßnahmen, und dient als Orientierungshilfe für das sonderpädagogische Handeln. Der sonderpädagogische Beobachtungsbogen gibt Auskunft über die physischen und psychischen Besonderheiten des Schülers und enthält insbesondere Vermerke über
- a) Entscheidungen der Schulaufsicht über Förder- oder Umschulungsmaßnahmen,
 - b) Beobachtungen zur Persönlichkeit des Schülers,
 - c) die vom Schüler erreichten und zu erwartenden individuellen Lern- und Erziehungsziele.

Ihm sind beizufügen

- a) die Stellungnahme der für den Schüler bisher zuständigen Grund- oder Oberschule zum Übergang des Schülers auf eine Sonderschule,
 - b) schulärztliche und gegebenenfalls fachärztliche Gutachten,
 - c) das sonderpädagogische und gegebenenfalls das schulpsychologische Gutachten.
- (2) Nummer 3 Abs. 3 gilt entsprechend.

7 - Akten der Sozialpädagogen

Informationen über Schüler, die im Zusammenhang mit der außerunterrichtlichen Betreuung durch Sozialpädagogen und Erzieher von Sozialpädagogen an Gesamtschulen mit Ganztagsbetrieb gesammelt werden, sind in besondere Akten getrennt vom Schülerbogen aufzunehmen. Diese Akten werden von dem Sozialpädagogen geführt, der den Schüler betreut.

8 - Akten des pädagogischen Koordinators der gymnasialen Oberstufe

Der pädagogische Koordinator führt über jeden von ihm betreuten Schüler besondere Akten, aus denen Informationen über absolvierte Kurse, Leistungen in den Kursen, Kursplanungen des Schülers, Beratung in Bezug auf die Kursplanung sowie weitere nach den Bestimmungen der Verordnung über die gymnasiale Oberstufe erforderliche Information über die Schullaufbahn in der gymnasialen Oberstufe und das Abitur ersichtlich sind.

9 - Schülerkarteien

(1) In jeder Schule wird eine Schülerkartei geführt. Sie dient der schnellen Ermittlung der für die laufenden Verwaltungsgeschäfte erforderlichen Informationen. In die Schülerkartei dürfen nur die in der Anlage 3 aufgeführten Informationen aufgenommen werden.

(2) Die Schülerkartei ist eine Datei im Sinne des Berliner Datenschutzgesetzes.

10 - Klassenbücher, Klassenlisten, Kursbücher, Kurs- und Anwesenheitsnachweise, Unterrichtsbücher für Fördermaßnahmen

(1) Soweit der Unterricht in Klassen oder Kerngruppen stattfindet, werden Klassen- bzw. Kerngruppenbücher geführt. Bei in Kursen stattfindendem Unterricht wird für jeden Kurs ein Kursbuch, in der Grundschule ein Unterrichtsbuch für Fördermaßnahmen, im Gymnasium sowie im Abendgymnasium und den Kollegs ein Kurs- und Anwesenheitsnachweis geführt. Die Klassen- bzw. Kerngruppenbücher werden ergänzt durch eine Klassen- bzw. Kerngruppenliste, die getrennt vom Klassen- bzw. Kerngruppenbuch aufzubewahren ist. In der Kursphase der gymnasialen Oberstufe sowie im Abendgymnasium und den Kollegs werden vom Oberstufentutor gesonderte Anwesenheitsnachweise geführt.

(2) Das Klassenbuch sowie die Kurs- und entsprechenden Bücher enthalten Angaben über Namen und Geburtsdaten der Schüler, Stundenplan, unterrichtende Lehrer, Klasse, Kern- oder Kursgruppe, erteilten Unterricht (einschließlich Unterrichtsausfälle und besondere Veranstaltungen), Fehlzeiten von Schülern (einschließlich Verspätungen und Beurlaubungen), besondere Vorkommnisse. Als Anlage zum Kerngruppenbuch wird in Gesamtschulen ein Anwesenheitsnachweis geführt, in den Fehlzeiten der Schüler der Kerngruppe auch in den Kursen aufgenommen werden.

(3) Die Klassen- bzw. Kerngruppenliste enthält Namen und Anschriften der Schüler und Erziehungsberechtigten, deren Telefonnummer und Staatsangehörigkeit, Erziehungsmaßnahmen sowie Angaben über Themen und Noten der Klassenarbeiten. Der gesonderte Anwesenheitsnachweis nach Absatz 1 Satz 5 enthält Namen und Anschriften der Schüler und Erziehungsberechtigten, deren Telefonnummer und Staatsangehörigkeit sowie Angaben über den Zeitpunkt des Eintritts in die gymnasiale Oberstufe und den Besuch der Kurse.

11 - Einsicht in die Schülerunterlagen

(1) Die in Nummer 2 Abs. 3 genannten Unterlagen sind so aufzubewahren, daß Unbefugte keine Einsicht erlangen können.

(2) Lehrer und sonstige in der Schule und der Schulverwaltung beschäftigte Personen dürfen in die in Nummer 2 Abs. 3 genannten Unterlagen nur insoweit Einsicht nehmen, als dies zur Erfüllung ihrer Aufgaben erforderlich ist. Ist eine begrenzte Einsicht nicht möglich, weil sich benötigte und nicht benötigte Angaben nicht trennen lassen, so sind von der die jeweilige Unterlage führenden Person die erforderlichen Auskünfte zu erteilen.

(3) Erziehungsberechtigte, volljährige Schüler und mit Zustimmung der Erziehungsberechtigten noch nicht volljährige Schüler ab vollendetem 14. Lebensjahr dürfen in sämtliche in Nummer 2 Abs. 3 genannten Unterlagen Einsicht nehmen, es sei denn, das Wohl des Schülers wird dadurch beeinträchtigt oder schutzwürdige Interessen Dritter, insbesondere anderer Schüler oder Erziehungsberechtigter, werden verletzt. Über die Verweigerung oder Beschränkung der Einsicht entscheidet der Schulleiter. Wird die Einsicht verweigert oder auf Teile beschränkt, ist auf Verlangen in allgemeiner Form Auskunft über die vorenthaltenen Informationen zu erteilen, wenn dies ohne Beeinträchtigung der Interessen, die zur Verweigerung oder Beschränkung der Einsicht führten, möglich ist. Aus der Klassen- bzw. Kerngruppenliste dürfen nur Auskünfte erteilt werden; Einsicht in diese Unterlage ist nicht zulässig.

(4) Das Auskunftsrecht aus der Schülerkartei richtet sich nach den Vorschriften des Berliner Datenschutzgesetzes.

(5) Außerschulischen Stellen darf Einsicht in die in Nummer 2 Abs. 3 genannten Unterlagen nur in den gesetzlich vorgesehenen Fällen (z. B. § 5 Verwaltungsverfahrensgesetz, § 99 Verwaltungsgerichtsordnung, § 96 Strafprozeßordnung) gewährt werden.

(6) Im übrigen ist die Einsicht in Unterlagen über einen Schüler mit Zustimmung des Betroffenen, bei minderjährigen Schülern der Erziehungsberechtigten zulässig.

(7) In Zweifelsfällen entscheidet der Schulleiter, ob und in welchem Umfang Einsicht zu geben ist.

12 - Weitergabe von Schülerunterlagen oder Informationen über Schüler

(1) Die Weitergabe von Schülerunterlagen an andere Schulen ist nur im Rahmen der Bestimmungen der Absätze 2 bis 4 zulässig. Die Weitergabe von Schülerunterlagen oder darin enthaltenen Informationen an außerschulische Stellen ist nur insoweit zulässig, als Einsicht (Nummer 11 Abs. 5 und 6) gewährt werden darf. Die Versendung hat so zu erfolgen, daß Unbefugte keine Einsicht erlangen können.

(2) Verläßt ein Schüler die Schule, so verbleiben die über ihn geführten Schülerunterlagen grundsätzlich bei der bisher besuchten Schule. Hiervon abweichend wird bei einem Schulwechsel innerhalb Berlins nach Eingang der Aufnahmebestätigung der aufnehmenden Schule übersandt

- a) der Schülerbogen, wenn der Wechsel von einer allgemeinbildenden Schule oder entsprechenden Sonderschule in eine andere allgemeinbildende Schule oder entsprechende Sonderschule erfolgt,
- b) der sonderpädagogische Beobachtungsbogen, wenn der Wechsel zwischen Sonderschulen stattfindet,
- c) das Schülerpersonalblatt (ohne Anlage), wenn der Wechsel zwischen berufsbildenden Oberschulen stattfindet; sind Vorblatt und Anlage des Schülerpersonalblattes in einem Vordruck zusammengefaßt, gilt Satz 1.

Satz 2 gilt entsprechend bei einem Wechsel eines Schülers auf eine anerkannte Privatschule. Bei einem Wechsel von einer allgemeinbildenden Schule auf eine berufsbildende Oberschule ist der aufnehmenden Schule nur der Stand der Schullaufbahn mitzuteilen; der Schülerbogen ist der aufnehmenden Schule auf Verlangen zur Einsichtnahme zu übersenden. Bei einem Wechsel eines Schülers von einer Sonderschule auf eine allgemeinbildende Schule ist der aufnehmenden Schule auf Verlangen neben dem Schülerbogen ein pädagogisches Gutachten über die Eignung des Schülers für die aufnehmende Schule zu übersenden. Bei einem Wechsel eines Schülers auf eine andere gymnasiale Oberstufe sind der aufnehmenden Schule auf Verlangen die auf den Schüler bezogenen Angaben aus den Kurs- und Anwesenheitsnachweisen und den Akten des pädagogischen Koordinators zur übermitteln.

(3) Wechselt ein Schüler auf eine öffentliche Schule oder anerkannte private Schule eines anderen Landes der Bundesrepublik Deutschland, gilt Absatz 2 mit der Maßgabe, daß Unterlagen nur auf Antrag übersandt werden.

(4) Wechselt ein Schüler auf eine Schule im Ausland oder auf eine nicht anerkannte Privatschule, bleiben sämtliche Schülerunterlagen bei der zuletzt besuchten Schule. Der aufnehmenden Schule ist auf Antrag ein pädagogisches Gutachten über den Leistungsstand des Schülers zu übersenden.

(5) Die Weitergabe von Namen und Anschriften

- a) der Elternvertreter einer Klasse oder Kerngruppe an die Erziehungsberechtigten der Schüler der Klasse oder Kerngruppe und umgekehrt der Erziehungsberechtigten an die Elternvertreter, wenn die Erziehungsberechtigten nicht widersprechen,
- b) des Vorsitzenden der Gesamtelternvertretung an die Elternvertreter der Schule und umgekehrt der Elternvertreter der Schule an den Vorsitzenden der Gesamtelternvertretung

ist zulässig.

(6) Nummer 11 Abs. 7 gilt entsprechend.

13 - Aufbewahrungsfristen

(1) Die Aufbewahrungsdauer beträgt für

- a) den Schülerbogen, das Schülerpersonalblatt, die Schülerakten, den sonderpädagogischen Beobachtungsbogen und die Akten der Sozialpädagogen zwei Jahre, mindestens jedoch bis zur Beendigung der allgemeinen Schulpflicht,
- b) die Akten des pädagogischen Koordinators zwei Jahre oder, wenn der Schüler vor dem Abitur die Schule verläßt, fünf Jahre,
- c) die Kurs- und Anwesenheitsnachweise (gymnasiale Oberstufe) fünf Jahre,
- d) die übrigen in Nummer 2 Abs. 3 genannten Unterlagen ein Jahr.

Die Aufbewahrungsfristen beginnen für die

- a) in Satz 1 Buchstaben a und b genannten Unterlagen mit Ablauf des Schuljahres, in dem der Schüler die Schule verlassen hat,
- b) in Satz 1 Buchstaben c und d genannten Unterlagen mit Ablauf des Schuljahres, für das die Unterlage angelegt worden ist.

Nach Ablauf der Aufbewahrungsfristen sind die Unterlagen zu vernichten.

(2) Schülerbogen und sonderpädagogische Beobachtungsbogen sind auf den Antrag der Erziehungsberechtigten oder des volljährigen Schülers, bestimmte Eintragungen zu löschen, daraufhin zu überprüfen, ob die dort festgehaltenen Informationen noch benötigt werden. Unterlagen über Ordnungsmaßnahmen werden in der Regel nach Ablauf von drei Schuljahren nicht mehr benötigt, wenn zwischenzeitlich keine weiteren Ordnungsmaßnahmen ergriffen worden sind. Bei Angaben über besondere häusliche Verhältnisse ist davon auszugehen, daß sie in der Regel nach spätestens vier Jahren nicht mehr aussagekräftig sind, es sei denn, der Schule liegen Informationen über das Fortbestehen dieser Verhältnisse vor. Begründungen für Fehlzeiten sind nur bis zum Ablauf des auf das Schuljahr, in dem die Fehlzeiten aufgetreten sind, folgenden Schuljahres aufzubewahren.

(3) Findet der Unterricht in Semestern statt, so tritt an die Stelle des Schuljahres das Semester.

14 - Automatisierte Sammlungen

(1) Die in Nummer 2 Abs. 3 genannten Unterlagen mit Ausnahme des sonderpädagogischen Beobachtungsbogens dürfen auch ganz oder teilweise als automatisierte Sammlungen geführt werden.

(2) Automatisierte Sammlungen dürfen nicht mehr Angaben enthalten als die in diesen Vorschriften vorgesehenen Angaben. Personenbezogene Daten über Schüler sind zu löschen, wenn ihre Kenntnis für die Schule nicht mehr erforderlich ist oder wenn ihre Speicherung ohnehin unzulässig war; Nummer 13 gilt entsprechend. Soweit Teile des Klassen- bzw. Kerngruppenbuches durch das automatisierte Verfahren ersetzt werden, ist vor dem Löschen ein Ausdruck zu fertigen, für den die Bestimmungen über Klassen- bzw. Kerngruppenbücher gelten. Die Einrichtung automatisierter Sammlungen darf nur auf Anordnung des Schulleiters erfolgen. In der Anordnung sind der Zweck der Sammlung sowie Art und Umfang der zu speichernden Informationen festzulegen.

(3) Verantwortlich für die automatisierte Verarbeitung ist der Klassenlehrer, Kerngruppenleiter, Oberstufentutor oder pädagogische Koordinator. Die auftragsgemäße Verarbeitung der Informationen durch andere Lehrer oder schulische Mitarbeiter ist nur im Rahmen der Weisungen des zuständigen Lehrers zulässig.

(4) Die erforderliche Veröffentlichung im Amtsblatt für Berlin sowie die Meldung zum Datenregister beim Berliner Datenschutzbeauftragten (§§ 12, 22 BlnDSG) sind vom Bezirksamt vorzunehmen. Die Schule ist speichernde Stelle im Sinne der datenschutzrechtlichen Bestimmungen; sie stellt die erforderlichen Unterlagen sofort nach der Einrichtungsanordnung zur Verfügung.

(5) Werden in der Schule personenbezogene Informationen über Schüler oder Erziehungsberechtigte automatisiert verarbeitet, hat der Schulleiter zur Gewährleistung des Datenschutzes und der Datensicherung (§ 5 BlnDSG) einen Schuldatenschutzbeauftragten zu benennen. Dieser nimmt in entsprechender Anwendung der §§ 28, 29 Bundesdatenschutzgesetz die dort genannten Aufgaben wahr. Er darf keine Aufträge nach Absatz 3 Satz 2 übernehmen.

(6) Personenbezogene Informationen über Schüler oder Erziehungsberechtigte dürfen nur mit Zustimmung des Schulleiters auf privaten Datenverarbeitungsgeräten verarbeitet werden; die Absätze 1 bis 5 gelten entsprechend. Die Zustimmung darf nur erteilt werden, wenn der Betreiber des Geräts schriftlich zugesichert hat, daß er dem Berliner Datenschutzbeauftragten die Wahrnehmung von dessen Kontrollaufgaben gemäß §§ 21 ff. Berliner Datenschutzgesetz ermöglicht.

15 - Übergangsvorschriften

Unterlagen nach Nummer 2 Abs. 3, die vor Inkrafttreten dieser Ausführungsvorschriften angelegt wurden, werden mit ihrem derzeitigen Inhalt weitergeführt; neue Eintragungen unterliegen diesen Vorschriften; die Regelungen über Berichtungspflichten (Nummer 2 Abs. 2) und Aufbewahrungsfristen (Nummer 13) sind auch auf vorhandene Unterlagen anzuwenden. Vorhandene Vordrucke sind aufzubrechen.

16 - Inkrafttreten

(1) Diese Ausführungsvorschriften treten am 1. August 1986 in Kraft. Sie treten mit Ablauf des 31. Juli 1996 außer Kraft.

(2) Durch sie werden ersetzt

- a) die Ausführungsvorschriften über die Führung von Schülerbogen vom 6. Juli 1970 (DBl. III S. 168), geändert durch Verwaltungsvorschriften vom 9. November 1970 (DBl. III S. 216),
- b) das Rundschreiben II Nr. 35/1976 vom 20. Mai 1976 (Einsicht in Klassenbücher durch Elternvertreter),
- c) Nummer 5 der Ausführungsvorschriften über Werbung, gewerbliche Tätigkeit, Aushänge und Sammlungen in der Berliner Schule, im Berlin-Kolleg und in den Fachschulen des Landes Berlin - AV-Werbung - vom 17. Dezember 1982 (ABl. S. 1677 / DBl. III S. 345), berichtigt am 6. Januar 1983 (ABl. S. 26, 54 / DBl. III S. 3),
- d) das Rundschreiben II Nr. 98/1976 vom 22. November 1976 (Auskünfte über Namen und Anschriften von ausländischen Schülern).

Anlage 1 AV-Schülerunterlagen

Angaben im Schülerbogen

Name
Vornamen
Geschlecht
Geburtsdatum, -ort
Staatsangehörigkeit
Anschrift, Telefonnummer
Name, Vorname, Anschrift, Telefonnummer der/des Erziehungsberechtigten
Beginn der Schulpflicht
Angaben über die Schullaufbahn in der allgemeinbildenden Schule
Vermerke über Kontakte mit den Erziehungsberechtigten und Einrichtungen, die den Schüler betreuen
Übereignete Lernmittel

Anlage 2 AV-Schülerunterlagen

Angaben im Schülerpersonalblatt

1. Vorblatt

Name
Vornamen
Geschlecht
Geburtsdatum, -ort
Anschrift
Telefonnummer
Staatsangehörigkeit
ggf. Name, Vorname des Erziehungsberechtigten
ggf. Anschrift und Telefonnummer des Erziehungsberechtigten, falls sie nicht mit denen des Schülers identisch sind
Angaben zur schulischen Vorbildung
ggf. Angaben zur Schullaufbahn in berufsbildenden Schulen
Tag der erstmaligen Aufnahme in eine berufsbildende Schule
2. Anlage

Name
Vornamen
Geschlecht
Geburtsdatum, -ort
Geliehene Lernmittel
ggf. Name, Anschrift und Telefonnummer des Ausbildungsbetriebes
Angaben über berufliche Vorbildung oder Tätigkeit
Angaben über das Durchlaufen des Bildungsganges
Zeugnisnoten
Bemerkungen auf Zeugnissen
Nachweis über Schulbesuch

Anlage 3 AV - Schülerunterlagen

Angaben in der Schülerkartei

Name
 Vornamen
 Geschlecht
 Geburtsdatum, -ort
 Anschrift
 Telefonnummer
 Staatsangehörigkeit
 ggf. Name, Vorname des Erziehungsberechtigten

ggf. Anschrift des Erziehungsberechtigten, falls sie nicht mit der des Schülers identisch ist
 ggf. Name, Vorname, Anschrift, Telefonnummer von Personen oder Einrichtungen, die bei einem unvorhersehbaren Ereignis verständigt werden sollen
 ggf. Name, Anschrift und Telefonnummer des Ausbildungsbetriebes oder der Praxisstelle
 Schullaufbahn (Aufnahme- und Abgangsdatum, besuchte Klassen bzw. Kurse)
 Teilnahme am Religionsunterricht
 ggf. Teilnahme an freiwilligen Arbeitsgemeinschaften oder Kursen
 Gesundheitliche Rücksichten
 Versand des Schülerbogens bzw. Schülerpersonalblattes

Anlage 6

051.Inn-91/84

Berlin, 9. Januar 1986

An die
 Bezirksämter
 von Berlin

Betr.: Datenschutzrechtliche Bewertung der Datenweitergabe innerhalb des Bezirksamtes

Die datenschutzrechtliche Bewertung der Datenweitergabe innerhalb von Bezirksämtern hat, ebenso wie die Bewertung der Datenweitergabe innerhalb von Kommunen in anderen Bundesländern, in der Vergangenheit verschiedene Probleme aufgeworfen. Der Auffassung, die Bezirksämter (Städte und Gemeinden) seien als solche als speichernde Stelle zu betrachten und die interne Datenweitergabe daher ein in den Datenschutzgesetzen nicht geregelter Vorgang, haben die Datenschutzbeauftragten frühzeitig entgegengehalten, daß die Regelung der Datenübermittlung an die jeweilige gesetzliche Aufgabenzuweisung anknüpfe und der Begriff der speichernden Stelle daher in enger Verbindung mit der Aufgabenzuweisung gesehen werden müsse (funktionaler Behördenbegriff).

Das Urteil des Bundesverfassungsgerichts zur Volkszählung hat nach meiner Auffassung diese Position bestätigt.

Der Senat hält diese Frage weiterhin für strittig.

Um bis zu einer gesetzlichen Neuregelung eine für alle Seiten hinnehmbare Verfahrensweise zu erreichen, empfehle ich nach Abstimmung mit dem Senator für Inneres folgendes Vorgehen:

Ungeachtet der Frage, welche Organisationseinheit formal als speichernde Stelle i. S. des Berliner Datenschutzgesetzes anzusehen ist, ist bei der Weitergabe von Daten innerhalb eines Bezirksamtes die Vorschrift des § 10 Abs. 1 Satz 1 entsprechend anzuwenden. Unterliegen die Daten einem besonderen Berufs- oder Amtsgeheimnis (z. B. Sozialdaten), müssen die spezialgesetzlich vorgegebenen Voraussetzungen (z. B. §§ 67 ff. SGB X) vorliegen; die in § 10 Abs. 1 Satz 2 Berliner Datenschutzgesetz vorgesehenen Beschränkungen sind zu berücksichtigen.

Die Weitergabe personenbezogener Daten durch das als Meldebehörde tätige Bezirkseinschreibeamt richtet sich ausschließlich nach dem Meldegesetz vom 26. Februar 1985, insbesondere nach den §§ 25, 8 Meldegesetz. Danach ist sicherzustellen, daß zwei Jahre lang Auskunft über diejenigen Übermittlungen gegeben werden kann, bei denen mehr als die in § 28 Abs. 1 Meldegesetz genannten Daten weitergegeben wurden.

Dr. Kerkau

Anlage 7

Empfänger regelmäßiger Übermittlungen aus dem Melderegister – Anlage 4 zu § 3 Nr. 1 DVO-MeldeG vom 4. März 1986, GVBl. S. 476

Lfd. Nr.	Datenempfänger	Regelmäßig übermittelte Daten	Anlaß der regelmäßigen Datenübermittlungen	Zweck der regelmäßigen Datenübermittlungen
1	2	3	4	5
1	Bezirksämter von Berlin - zuständige Stellen -	Familiennamen, Vornamen, akademische Grade, Ordensnamen/Künstlernamen, Tag der Geburt, Geschlecht, Staatsangehörigkeit, gegenwärtige Anschriften, Familienstand	Eintritt des jeweiligen Ereignisses nach Spalte 5	Begrüßung der erstmals in einen Bezirk von Berlin zuziehenden Einwohner, Versendung von Informationsmaterial für 18jährige Jungbürger, 60-, 65- und 70jährige Einwohner, Ehrung von Alterjubilaren (Vollendung des 80., 85., 90. und jeweils weiteren Lebensjahres), Ehrung von Ehejubilaren (Vollendung des 50., 60., 65., 70. und 75. Ehejahres)
2	Bezirksämter von Berlin - zuständige Stellen -	Familiennamen, Vornamen, Tag und Ort der Geburt, Geschlecht, gesetzlicher Vertreter (Vor- und Familien- namen, akademische Grade, Anschrift, Tag der Geburt), Staatsangehörigkeit, gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs, Sterbetag und -ort	von minderjährigen Einwohnern: Änderung der Anschrift, des Familiennamens, Tod	Durchführung des Bundes-Seuchengesetzes (Schutzimpfungen) und des Gesundheits- dienst-Gesetzes (Jugendgesundheitsdienst)
3	Bezirksämter von Berlin - zuständige Stellen -	Familiennamen, Vornamen, Tag und Ort der Geburt, Geschlecht, gesetzlicher Vertreter (Vor- und Familien- namen, akademische Grade, Anschrift, Tag der Geburt), Staatsangehörigkeit, gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs	von Einwohnern vom vollendeten 6. Lebens- jahr bis zum vollendeten 18. Lebensjahr: Zuzug nach Berlin	Durchführung des Schulgesetzes für Berlin (Schulpflicht)
4	Bezirksämter von Berlin - zuständige Stellen -	Familiennamen, Vornamen, akademische Grade, Tag und Ort der Geburt, Geschlecht, gesetzlicher Vertreter (Vor- und Familien- namen, akademische Grade, Anschrift, Tag der Geburt), Staatsangehörigkeit, gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs, Familienstand, Sterbetag und -ort	von Einwohnern, für die der Datenempfänger regelmäßige Datenübermittlung beantragt hat: Änderung der Anschrift, des Familiennamens Tod	Durchführung des Gesetzes für Jugendwohl- fahrt (Aufgaben des Jugendamts im Vormund- schaftswesen) und des Bürgerlichen Gesetz- buches (Vormundschaften und Pflegschaften für Volljährige)
5	Entschädigungsamt Berlin	Familiennamen, frühere Namen, Vornamen, akademische Grade, Tag und Ort der Geburt, Geschlecht, Staatsangehörigkeit, gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs, Familienstand, einschließlich der Hinweise, Sterbetag und -ort	von Einwohnern, für die der Datenempfänger regelmäßige Datenübermittlung beantragt hat: Änderung der Anschrift, des Familienstandes, Tod	Durchführung des Bundesentschädigungs- gesetzes und des Gesetzes über die Anerken- nung und Versorgung der politisch, rassisch oder religiös Verfolgten des Nationalsozialis- mus, Gewährung von Ehrenunterstützungen an Ber- liner Bürger, die in der NS-Zeit Verfolgten uneigennützig geholfen haben (Amtsblatt für Berlin 1981 S. 902)
6	Landesamt für Zentrale Soziale Aufgaben - Landesversorgungsamt -	Familiennamen, Vornamen, akademische Grade, Tag und Ort der Geburt, Geschlecht, gesetzlicher Vertreter (Vor- und Familien- namen, akademische Grade, Anschrift, Tag der Geburt), Staatsangehörigkeit, gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs, Sterbetag und -ort	von Einwohnern, für die der Datenempfänger regelmäßige Datenübermittlung beantragt hat: Änderung der Anschrift, Tod	Durchführung des Schwerbehindertengesetzes sowie des Bundesversorgungsgesetzes, des Haftlingshilfegesetzes, des Unterhaltsbeihilfegesetzes, des Bundes-Seuchengesetzes und des Opferentschädigungsgesetzes (Soziales Entschädigungsrecht)
7	Präsident des Landgerichts Berlin Präsident des Amtsgerichts Friedrichshagen	Familiennamen, frühere Namen, Vornamen, akademische Grade, Tag und Ort der Geburt, Geschlecht, Staatsangehörigkeit, gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs, Familienstand, Sterbetag und -ort	von Einwohnern, für die der Datenempfänger regelmäßige Datenübermittlung beantragt hat: Änderung der Anschrift, des Familienstandes, der Staatsangehörigkeit, Tod	Führung der Listen von Schöffen

Anlage 4 (zu § 3 Nr. 1 DVO-MeldeG)

Lfd. Nr. 1	Datenempfänger 2	Regelmäßig übermittelte Daten 3	Anlaß der regelmäßigen Datenübermittlungen 4	Zweck der regelmäßigen Datenübermittlungen 5
8	Polizeipräsident in Berlin - Landespolizeidirektion -	Familiennamen, frühere Namen, Vornamen, Tag und Ort der Geburt, Geschlecht, gesetzlicher Vertreter (Vor- und Familien- namen, akademische Grade, Anschrift, Tag der Geburt), Staatsangehörigkeit, gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs, Familienstand, Ehegatte (Vor- und Familiennamen, akade- mische Grade, Tag der Geburt, Anschrift, Sterbetag), Ausstellungsbehörde, -datum, Gültigkeitsdauer des Personalausweises/Pas- ses, Übermittlungssperren, Sterbetag und -ort, einschließlich der Hin- weise	von Einwohnern, für die der Datenempfänger regelmäßige Datenübermittlung beantragt hat: Änderung des Namens, der Anschrift, des Familienstandes Tod Ausstellung eines Personalausweises/ Passes	Durchführung der Aufgaben der Verfolgung von Straftaten und der Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung
9	Polizeipräsident in Berlin - Landespolizeidirektion -	Familiennamen, Vornamen, Tag und Ort der Geburt, Sterbetag und -ort, einschließlich der Hin- weise	von allen Einwohnern: Zuzug nach Berlin Änderung der Anschrift Tod	zur Berichtigung und Fortschreibung der Fahndungsunterlagen
10	Ausländerbehörde	Familiennamen, frühere Namen, Vornamen, akademische Grade, Ordensnamen/Künstlernamen, Tag und Ort der Geburt, Geschlecht, gesetzlicher Vertreter (Vor- und Familien- namen, akademische Grade, Anschrift, Tag der Geburt), Staatsangehörigkeit, gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs, Familienstand, einschließlich der Hin- weise, Ehegatte (Vor- und Familiennamen, akade- mische Grade, Tag der Geburt, Anschrift, Sterbetag), minderjährige Kinder (Vor- und Familien- namen, Tag der Geburt, Sterbetag), Ausstellungsbehörde, -datum, Gültigkeitsdauer des Personalausweises/Pas- ses, Übermittlungssperren, Sterbetag und -ort	von Ausländern: Zuzug nach Berlin Änderung der Anschrift, der Hauptwohnung, des Familienstandes, des Geburtsdatums, der Staatsangehörigkeit, Geburt eines Kindes Tod	Erfüllung der den Ausländerbehörden durch Rechtsvorschrift übertragenen Aufgaben
11	Fahrerlaubnisbehörde Personenbeförderung	Familiennamen, frühere Namen, Vornamen, Tag und Ort der Geburt, Staatsangehörigkeit, gegenwärtige Anschriften, Hauptwohnung außerhalb Berlins, Übermittlungssperren, Sterbetag und -ort	von Einwohnern, für die der Datenempfänger regelmäßige Datenübermittlung beantragt hat: Tod	Durchführung der Straßenverkehrs- Zulassungs-Ordnung (Fortschreibung der Führerscheinkarte)

Empfänger regelmäßiger Übermittlungen aus dem Melderegister - Anlage 5 zu § 3 Nr. 2 DVO-MeldeG vom 4. März 1986, GVBl. S. 476

Anlage 5
(zu § 3 Nr. 2 DVO-MeldeG)

1. Die **Bezirksämter von Berlin** - jeweils zuständige Stellen - dürfen abrufen bei Einwohnern, bei denen eine Lohnsteuerkarte ausgestellt werden soll, Familiennamen, frühere Namen, Vornamen, akademische Grade, Ordensnamen/Künstlernamen, Tag und Ort der Geburt, Geschlecht, gesetzlicher Vertreter (Vor- und Familiennamen, akademische Grade, Anschrift, Tag der Geburt), Staatsangehörigkeit, rechtliche Zugehörigkeit zu einer Religionsgesellschaft, die durch die Finanzbehörden Berlins Steuern erhebt, gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs, Familienstand, Ehegatte (Vor- und Familiennamen, akademische Grade, Tag der Geburt, Anschrift, Sterbetag), minderjährige Kinder (Vor- und Familiennamen, Tag der Geburt, Sterbetag), Ausstellungsbefähigung, -datum, Gültigkeitsdauer des Personalausweises/Passes, Übermittlungssperren, Sterbetag und -ort.
2. Die **Bezirksämter von Berlin** - jeweils zuständige Stellen - dürfen abrufen bei Einwohnern, bei denen im Einzelfall die Kenntnis der Daten zur Erfüllung der den Bezirksämtern durch Rechtsverordnung obliegenden Aufgaben erforderlich ist, Familiennamen, frühere Namen, Vornamen, akademische Grade, Tag und Ort der Geburt, gesetzlicher Vertreter (Vor- und Familiennamen, akademische Grade, Anschrift, Tag der Geburt), gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs, Familienstand, Ehegatte (Vor- und Familiennamen, akademische Grade, Tag der Geburt, Anschrift, Sterbetag), minderjährige Kinder (Vor- und Familiennamen, Tag der Geburt, Sterbetag), Ausstellungsbefähigung, -datum, Gültigkeitsdauer des Personalausweises/Passes, Übermittlungssperren, Sterbetag und -ort.
3. Die **Berliner Feuerwehr** darf abrufen bei Einwohnern, bei denen im Einzelfall die Kenntnis der Daten zur Einziehung der von der Feuerwehr zu erhebenden Benutzungsgebühren erforderlich ist, Familiennamen, frühere Namen, Vornamen, akademische Grade, Tag und Ort der Geburt, gesetzlicher Vertreter (Vor- und Familiennamen, akademische Grade, Anschrift, Tag der Geburt), gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs, Familienstand, Ehegatte (Vor- und Familiennamen, akademische Grade, Tag der Geburt, Anschrift, Sterbetag), minderjährige Kinder (Vor- und Familiennamen, Tag der Geburt, Sterbetag), Ausstellungsbefähigung, -datum, Gültigkeitsdauer des Personalausweises/Passes, Übermittlungssperren, Sterbetag und -ort.
4. Der **Polizeipräsident in Berlin** - Landespolizeidirektion - darf abrufen bei Einwohnern, bei denen im Einzelfall die Kenntnis der Daten zur Erfüllung polizeilicher Aufgaben erforderlich ist, Familiennamen, frühere Namen, Vornamen, akademische Grade, Ordensnamen/Künstlernamen, Tag und Ort der Geburt, einschließlich der Hinweise, Geschlecht, gesetzlicher Vertreter (Vor- und Familiennamen, akademische Grade, Anschrift, Tag der Geburt), Staatsangehörigkeit, gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs, Familienstand, einschließlich der Hinweise, Ehegatte (Vor- und Familiennamen, akademische Grade, Tag der Geburt, Anschrift, Sterbetag), minderjährige Kinder (Vor- und Familiennamen, Tag der Geburt, Sterbetag), Ausstellungsbefähigung, -datum, Gültigkeitsdauer des Personalausweises/Passes, Übermittlungssperren, Sterbetag und -ort, einschließlich der Hinweise.
5. Die **Personalausweisbehörde** darf abrufen bei deutschen Einwohnern und bei deren Kindern unter 16 Jahren ohne Rücksicht auf deren Staatsangehörigkeit zur Durchführung der Aufgaben der Personalausweisbehörde nach der BK/O (46) 61 folgende Daten einschließlich der Hinweise: Familiennamen, frühere Namen, Vornamen, akademische Grade, Ordensnamen/Künstlernamen, Tag und Ort der Geburt, Geschlecht, gesetzlicher Vertreter (Vor- und Familiennamen, akademische Grade, Anschrift, Tag der Geburt), Staatsangehörigkeit, gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs, Familienstand, Ehegatte (Vor- und Familiennamen, akademische Grade, Tag der Geburt, Anschrift, Sterbetag), minderjährige Kinder (Vor- und Familiennamen, Tag der Geburt, Sterbetag), Ausstellungsbefähigung, -datum, Gültigkeitsdauer des Personalausweises/Passes, Übermittlungssperren, Sterbetag und -ort.
6. Die **Passbehörde** darf abrufen bei deutschen Einwohnern zur Durchführung der Aufgaben der Passbehörde nach dem Paßgesetz folgende Daten einschließlich der Hinweise: Familiennamen, frühere Namen, Vornamen, akademische Grade, Ordensnamen/Künstlernamen, Tag und Ort der Geburt, einschließlich der Hinweise, Geschlecht, gesetzlicher Vertreter (Vor- und Familiennamen, akademische Grade, Anschrift, Tag der Geburt), Staatsangehörigkeit, gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs, Familienstand, Ehegatte (Vor- und Familiennamen, akademische Grade, Tag der Geburt, Anschrift, Sterbetag), minderjährige Kinder (Vor- und Familiennamen, Tag der Geburt, Sterbetag), Ausstellungsbefähigung, -datum, Gültigkeitsdauer des Personalausweises/Passes, Übermittlungssperren, Sterbetag und -ort.
7. Die **Zulassungsstelle für Kraftfahrzeuge** darf abrufen bei Einwohnern, bei denen im Einzelfall die Kenntnis der Daten zur Erfüllung der Aufgaben der Kraftfahrzeugzulassungsbehörde erforderlich ist, Familiennamen, frühere Namen, Vornamen, Ordensnamen/Künstlernamen, Tag und Ort der Geburt, Geschlecht, gesetzlicher Vertreter (Vor- und Familiennamen, akademische Grade, Anschrift, Tag der Geburt), gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs, Familienstand, Ehegatte (Vor- und Familiennamen, akademische Grade, Tag der Geburt, Anschrift, Sterbetag), minderjährige Kinder (Vor- und Familiennamen, Tag der Geburt, Sterbetag), Ausstellungsbefähigung, -datum, Gültigkeitsdauer des Personalausweises/Passes, Übermittlungssperren, Sterbetag und -ort.
8. Die **Verkehrsordnungswidrigkeitenbehörde** darf abrufen bei Einwohnern, bei denen im Einzelfall die Kenntnis der Daten zur Abmilderung und Verfolgung von Ordnungswidrigkeiten im Straßenverkehr erforderlich ist, Familiennamen, frühere Namen, Vornamen, akademische Grade, Ordensnamen/Künstlernamen, Tag und Ort der Geburt, einschließlich der Hinweise, Geschlecht, gesetzlicher Vertreter (Vor- und Familiennamen, akademische Grade, Anschrift, Tag der Geburt), gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, Tag des Ein- und Auszugs, Familienstand, Ehegatte (Vor- und Familiennamen, akademische Grade, Tag der Geburt, Anschrift, Sterbetag), minderjährige Kinder (Vor- und Familiennamen, Tag der Geburt, Sterbetag), Ausstellungsbefähigung, -datum, Gültigkeitsdauer des Personalausweises/Passes, Übermittlungssperren, Sterbetag und -ort.

Anlage 8

**Anforderungen an Datenschutzregelungen
in Strafverfahren**

Das Strafprozeßrecht enthält in wesentlichen Bereichen noch keine den Anforderungen der Rechtsprechung des Bundesverfassungsgerichts genügenden Vorschriften über den Umgang mit personenbezogenen Daten. Das gilt für die Verarbeitung in automatisierten und nicht automatisierten Dateien ebenso wie für die Aktenführung.

In ihrer Entschlieung vom 25. November 1986 hat die Konferenz der Datenschutzbeauftragten u. a. folgende Themenkreise für regelungsbedürftig gehalten:

1. **Befugnisse von Staatsanwaltschaft und Polizei im Ermittlungsverfahren**
 - 1.1 Befugnisnormen für die Informationserhebung
 - 1.2 Örtliche, überörtliche und internationale Fahndungsausschreibung bei Haftbefehl
 - Ermittlung des Aufenthalts von Beschuldigten und Zeugen
 - Öffentlichkeitsfahndung
 - Besondere Fahndungsmethoden
 - Rasterfahndung
 - Spurendokumentationssysteme
 - Polizeiliche Beobachtung
 - Erkennungsdienstliche Behandlung
 - Datenerhebung in Versammlungen
 - Einsatz technischer Mittel, z. B. Video
 - Informanten der Polizei, V-Personen, verdeckte Ermittler
 - 1.3 Befugnisnorm für Speicherung und sonstige Verwendung
 - 1.4 Datenübermittlung zwischen Staatsanwaltschaft und Polizei sowie Staatsanwaltschaften untereinander
2. **Rechte der Beteiligten und Dritter**
 - 2.1 Umfang der Akteneinsicht
 - 2.2 Unterrichtung Dritter über das Verfahren (z. B. Information an den Anzeigenden)
 - 2.3 Öffentlichkeit und Persönlichkeitsschutz
 - 2.4 Medien
 - 2.5 Kontrolle von Gerichtsbesuchern
3. **Aufbewahrungs- und Löschungsbestimmungen**
4. **Aussage- und Zeugnisverweigerungsrechte**
5. **Organisatorische Maßnahmen**

Stichwortverzeichnis

Angegeben sind die Fundstellen aller Jahresberichte seit 1979. Die Ziffern ohne Jahreszahl beziehen sich auf den Zusammen-
druck der Jahresberichte in den von mir herausgegebenen Mate-
rialien zum Datenschutz, Band 2, Datenschutz in Berlin 1979 –
1983

- Abfall 1986/26
Abgangskontrolle 104
Abgeordnetenhaus 14, 121; 1984/28; 1985/17; 1986/28
Abiturienten 118
Ablichtung 42, 55, 87, 113
Abonnentenverwaltung 106
Abruf, unbefugter 76, 107; 1986/16
Adoption 108, 109; 1985/4; 1986/6
Adrema-Platten 115
Adressenmittlung 26
Adreßbuch 1985/6
Adreßlisten 58, 115
ADV-Gesetz 1985/3, 26
ADV-Grundsätze 1984/18
Akten 25, 49, 58
Akten, Aufbewahrung 1986/16
Akten, Vollständigkeitsprinzip 56
Akteneinsicht 25, 28, 50, 59
Akteneinsicht, medizinische Daten 100
Akteneinsicht, Sozialgesetzbuch 59
Aktenführung 110; 1986/25
Aktenvernichtung 63
Allgemeine Geschäftsbedingungen 1984/6
Allgemeine Ortskrankenkasse 1984/16
Allgemeines Sicherheits- und Ordnungsgesetz 107; 1984/3, 10
1985/3, 7, 26, 27; 1986/16
Amerika-Gedenkbibliothek 85; 1984/28; 1986/16
Amtsanwaltschaft, s. Staatsanwaltschaft
Amtsarzt 1984/9; 1985/23
Amtsblatt, Dateiveröffentlichung 57
Amtsgeheimnis 55
Amtsgericht 54
Amtshilfe 25
Anonymisierung 34, 40, 51, 104
Anordnung über Mitteilungen in Strafsachen 40, 41, 44, 108;
1984/12, 24; 1985/3, 23; 1986/5, 23
Anordnung über Mitteilungen in Zivilsachen 54; 1984/25
Anrufungen 9, 25, 32, 50, 89, 121; 1984/29; 1986/29
Anschriften 115
Anzapfen 77
Arbeitsplatzcomputer 1986/3
Archive 46, 88, 106; 1984/3; 1985/11, 26
Archivgesetz 1985/3; 1986/3, 4
ASOG, s. Allgemeines Sicherheits- und Ordnungsgesetz
ASTA, s. Staatsanwaltschaft
Asylverfahren 1986/7
Aufklärung bei der Erhebung 42
Aufsichtsbehörde für den Datenschutz 27, 45, 61, 64, 88, 120;
1984/29; 1985/24; 1986/29
Auftragsdatenverarbeitung 112; 1984/17
Ausbildungsförderung, s. Bundesausbildungsförderungsgesetz
Auskunft 25, 35, 52, 116; 1985/23; 1986/6
Auskunft, Gebührenpflicht 28
Auskunft, Sicherheitsbehörden 35
Auskunftssperre 108, 109
Auskunftsverweigerung 35
Ausländer 33, 53, 82, 117
Ausländerbehörde 58, 111, 119; 1986/7
ärztliche Schweigepflicht, s. medizinische Daten
BAföG, s. Bundesausbildungsförderungsgesetz
Bankauskünfte 1984/6
Banken, Bildschirmtext 60
Basisdokumentation Psychiatrie 1984/9
Bau- und Planungsakten 73
Bau- und Wohnungswesen 116
Beamtenrecht 56; 1984/3, 9, 18; 1985/3, 26; 1986/3
Beamtenversorgungsgesetz 72
Bebauungsplan 74
BEHALA 105
Beihilfe 1984/20
Belegfluß 54
Benutzerkontrolle 86
Beratung 13, 26, 32, 43, 50, 64, 89, 121; 1984/29; 1986/29
bereichsspezifischer Datenschutz 28, 31, 45; 1984/3, 12; 1985/3, 26
Berichtigungsanspruch 35
Berliner Datenschutzgesetz 24, 121; 1985/26
Berliner Entwässerungswerke 105
Berliner Pfandbriefbank 1985/16
Berliner Philharmonisches Orchester 106
Berliner Stadtreinigungsbetriebe 57; 1985/16
Berliner Wasserwerke 105
Beschwerden s. Anrufung
Betriebsdatenbank 85; 1985/24
Betriebskrankenkasse des Landes und der Stadt Berlin 1984/17
BEWAG 36
Bezirksämter 109, 116; 1984/16; 1985/16; 1986/24, 38
Bezirkseinwohneramt 54
Bezirksverordnetenversammlungen 15, 73
Bibliotheken 85, 105; 1985/11, 26; 1986/16, 24
Bibliotheksgesetz 1985/3
Bildschirmtext 33, 37, 45, 59, 67, 75, 87, 101; 1984/12, 28
1985/12; 1986/12
Bildschirmtext, Anbieter 1984/14; 1985/17
Bildschirmtext, Betreiber 1984/14
Bildschirmtext, externe Rechner 101
Bildschirmtext, Staatsvertrag 75, 88, 123
Bildschirmtext, Zustimmungsgesetz 101, 120
Blutspendedienst 1984/8
Breitbandkommunikation 59, 101
Broschüren 27
Bundesausbildungsförderungsgesetz 63
Bundesbaugesetz 119
Bundesdatenschutzgesetz, Novellierung 65, 88, 89, 120, 121; 1986/4
Bundeskindereldgesetz s. Kindergeld
Bundeskriminalamt 44
Bundessozialhilfegesetz 72
Bundesstatistikgesetz 31; 1986/8
Bundesverfassungsgericht 1984/3; 1986/5
Bundeszentralregister, unbeschränkte Auskunft 40, 56, 88, 120;
1984/28
Bußgeldverfahren 1984/22
BVG 104; 1986/9
Chipkarte 1985/14; 1986/4
Codes 34, 60, 77, 101; 1984/6
Computerkriminalität 1984/5; 1986/4
Computermißbrauch 1984/4
Datei 25, 31, 49, 55, 58; 1985/18
Dateienregister 12, 24, 26, 27, 30, 43, 57, 64, 86, 88, 105, 120, 121;
1985/24; 1986/29
Datenangst 99
Datengeheimnis 55
Datenscheckheft 50
Datenschutzbeauftragter, Kontrollrechte 120
Datenschutzbeauftragter, Rolle 99
Datenschutzbeauftragter, Zuständigkeit 25
Datensicherung bei manuellen Datensammlungen 114
Datensicherung 37, 42, 57, 58, 64, 93, 116; 1984/5
Deutsche Klassenlotterie Berlin 85
Deutsche Oper Berlin 105
Deutsches Bibliotheksinstitut 105
Dezentralisierung 1986/3
Dienststelle, Aufbau 16, 24, 33, 50, 121
Dokumentation 1984/6
EG-Arbeitskräftestichprobe 1984/23
Eigenbetriebe 104
Einheitliche Patientendatenverarbeitung 63
Einladungskarteien 105
Einsichtsrecht 25, 41, 59, 66, 100; 1985/20
Einsichtsrecht, medizinische Daten 1986/11
Einsichtsrecht, Schülerbogen 41
Einwilligung 24, 26, 31, 34, 51, 57, 59, 67; 1985/22
Emissionskataster 1986/26
Entmündigung 1986/5
Einwohnerdatenbank, s. Melderegister
Epidemiologie, s. Forschungsprojekte
Erforderlichkeit 25, 41, 58, 61
Erhebung 40, 51, 56, 110,
erkennungsdienstliche Unterlagen 1984/11
EUROCAT 50
Europarat 28, 46; 1985/3, 35
Europäische Gemeinschaften 28, 50
externe Schreibkräfte 1984/9
Fahndung, Kraftfahrzeuge 79
Fahrzeugregister 1984/22
Familienkrankenhilfe 72
Fehlbelegungsabgabe 72, 75
Fehleintragung 54
Fehlspeicherung 107
Fensterbriefumschläge 43
Ferngespräche, Erfassung, s. Telefondatenerfassung
Fernmeldeordnung 1984/12
Fernwartung 63; 1985/34; 1986/15
Fernwirkdienste 101, 102; 1984/16; 1985/14; 1986/13
Feuersozietät 1984/16
Feuerwehr 79
Finanzverwaltung 88

- Flughafen 1985/4
 Formulare 26
 Forschung 33, 51, 59, 61, 82, 112, 117
 Forschung, Sozialgesetzbuch X 82
 Forschungsprojekte 50, 61, 87, 118
 Forsten 1985/5
 Fotos 1986/11
 Fremdfirmen 63, 84, 86
 Friedhöfe 1985/5
 Funk 42
 Führungszeugnis 57
 Funktionentrennung 86, 101, 114; 1984/6
 GASAG 36, 104
 Geburtsdaten 41; 1985/18; 1986/6
 Gebührenpflicht bei Auskünften 28
 Geldautomaten 1986/27
 Gemeinsame Geschäftsordnung für die Berliner Verwaltung 89, 106; 1985/3, 10
 Geschäftsverteilungsplan 115
 Gesetz über Abbau der Fehlsubventionierung s. Fehlbelegungsabgabe
 Gesetz über psychisch Kranke 121; 1986/1985/3
 Gesundheitsdaten, s. medizinische Daten
 Gewerbeordnung 62, 87
 Gewereregister 31, 62, 87, 88
 GGO, s. Gemeinsame Geschäftsordnung
 Glaubwürdigkeit kindlicher Zeugen 36
 Grundrecht auf Datenschutz 28
 Grundrechte 30
 Hacking 1984/4
 Handels- und Gaststättenzählung 1985/11
 Hausbesetzungen 80, 120
 Haushaltbegleitgesetz 100
 Haushaltsstrukturgesetze 72
 Herstellerfirmen 63
 Hochschulen 25, 32, 50, 57, 63; 1986/11
 Hochschulgesetz 1986/22
 Hochschulstatistikgesetz 58; 1984/24
 home-banking 60
 Identitätsfeststellung 1984/11
 illegale Beschäftigung, Bekämpfung 72
 in-camera-Verfahren 90
 Industrie- und Handelskammer 45, 61
 Information des Bürgers 27
 Information des Datenschutzbeauftragten 26, 43, 64, 113
 informationelles Selbstbestimmungsrecht 25; 1984/3
 Informationsgesellschaft 49
 Informationsgleichgewicht 15, 30
 Informationssystem Verbrechensbekämpfung 36, 79, 108; 1984/10; 1985/8; 1986/16
 Informationsverarbeitung, Entwicklung 49
 INPOL-System 44; 1985/8
 Institutionsleihe 44
 intelligente Schnittstelle 1985/6
 interner Datenschutzbeauftragter 105, 112, 116
 internes Dateienregister 105
 Intimbereich 39
 isolierte Rechner 63, 114; 1985/5
 ISDN 1986/3
 ISVB, s. Informationssystem Verbrechensbekämpfung
 Jugendgerichtshilfe 58, 110
 Justizverwaltung 50, 60
 Justizvollzugsanstalten 55, 81, 87; 1985/17
 Kabelkommunikation 33, 37, 39, 46, 67, 102
 Kabelpilotprojekt 101; 1984/15; 1985/3, 15; 1986/13
 Kammergericht 1985/5
 KAN, s. Kriminalaktennachweis
 Kassenarzt 1986/5, 10
 Kaufpreissammlung 119; 1984/27
 Kindergeld 72, 100; 1984/19
 Kirchen 24, 27, 32
 Kirchensteuerstelle 1984/17
 Klassenliste 118
 Kleinrechner 84, 114; s.a. Personalcomputer
 Klinische Nachsorgeregister 50
 Konferenz der Datenschutzbeauftragten 18, 43, 64, 88, 120; 1984/28; 1985/24; 1986/28
 Konsolprotokolle 63
 Kontrollen von Amts wegen 11, 24, 25, 26, 32, 50, 68
 Konverter 102
 Kosten- und Behandlungsplan 110; 1984/9, 34
 Kostenübernahme, Krankenhaus 1986/10
 Kostenübernahmescheine 81
 KPM 105
 KpS-Richtlinien 27, 43, 56, 79, 119; 1984/12, 27
 Kraftfahrzeuge 25, 79
 Krankenakten, s. medizinische Daten
 Krankentbett 1986/11
 Krankengeschichtenverordnung 120; 1984/8
 Krankenhäuser, s. medizinische Daten
 Krankenkassen 1985/21; 1986/10
 Krebsregister 50, 88; 1984/8
 Kriminalaktennachweis 44
 Kriminalpolizeiliche personenbezogene Daten, s. KpS-Richtlinien
 kulturelle Einrichtungen 105
 Landesamt für Elektronische Datenverarbeitung 62, 63
 Landesamt für Verfassungsschutz, s. Verfassungsschutz
 Landesarchiv, s. Archive
 Landeseinwohneramt 1986/5
 Landeskrankenhausesgesetz 1984/3, 7, 30
 Landesmeldegesetz 35, 45, 53, 64, 77, 107, 121; 1984/3, 21
 Landesstatistikgesetz 104; 1984/3
 Landesversicherungsanstalt 1984/16
 Landeswahlordnung, s. Wahlen
 Lastschrifteneinzug 1984/17
 LED, s. Landesamt für Elektronische Datenverarbeitung
 Lehrerindividualdatei 118; 1986/22
 Liegenschaftskataster 75; 1984/17
 Lohnsteuerkarte 43, 54, 57; 1986/28
 Lohnsteuerstellen 119
 Löschungsanspruch 35
 manuelle Datensammlungen 89, 91, 93, 112, 114, 117
 Max-Planck-Gesellschaft 61, 87
 Medienforum Berlin 1985/15;
 Medienprivileg 8, 38, 65, 68
 medizinische Daten 25, 27, 31, 40, 49, 63, 100, 112, 120; 1984/3, 7; 1985/20; 1986/10
 Meldegesetz 35, 45, 53, 64, 77, 107, 121; 1984/3; 1985/3, 6, 26; 1986/3, 5, 39
 Meldepflicht, s. Meldegesetz, Melderechtsrahmengesetz
 Melderechtsrahmengesetz 27, 31, 44, 55, 100; 1985/26
 Melderegister 54, 63, 64, 78, 87, 107; 1984/21; 1985/6, 23; 1986/5
 Menschenrechtskonvention 28
 Mieterlisten 73
 Mietobergrenzen 1984/27
 Mietpreissetzen 73
 Mikrocomputer 1984/18
 Mikroverfilmung 1984/32
 Mikrozensus 1984/23; 1985/11; 1986/8
 Mischverwaltung 44
 MiStra, s. Anordnung über Mitteilungen in Strafsachen
 MiZi, s. Anordnung über Mitteilungen in Zivilsachen
 Modellprogramm Psychiatrie, s. psychiatrische Daten
 Museum für Verkehr und Technik 121
 Nachrichtendienstliches Informationssystem (NADIS) 35
 Nebentätigkeit 1986/11
 Neue Medien 32, 37, 45, 49, 59, 67, 75, 91, 100; 1984/12, 28, 30; 1985/31; 1986/12
 Neue Medien, Grundsätze 64, 67; 1984/30
 Notare 87
 Novellierung des Bundesdatenschutzgesetzes, s. Bundesdatenschutzgesetz
 OECD 28, 46
 Öffentlichkeit 1986/19
 on-line-Anschlüsse 39, 49, 78, 84, 115
 Ordnungsmäßigkeit der Datenverarbeitung 114
 Ordnungsmerkmal 53, 77; 1985/6
 Ordnungsverwaltung 1986/5
 Organleihe 44
 Orwell 99
 Öffentliche Lebensversicherung 1984/16
 öffentliche Wirtschaftsunternehmen 1984/16
 Öffentlichkeitsarbeit 33, 50, 89, 121; 1984/29
 Paß 126; 1986/4
 Pay – TV 102; 1985/15
 Personalakten 26, 40, 67; 1984/18; 1985/18; 1986/20, 23
 Personalausweis 26, 31, 42, 55, 87, 106, 120, 126; 1985/6; 1986/5
 Personalausweisgesetz 44, 100, 106; 1984/4; 1986/3
 Personalbezügedatei 1984/24
 Personalcomputer 1985/4, 32; 1986/3, 7, 14, 17
 Personaldaten 25, 32, 40, 45, 49, 56, 66, 67; 1984/9, 18; 1985/5, 18; 1986/3, 15, 20, 28
 Personalfragebogen 1984/19
 Personalrat 1985/19; 1986/21
 Personalverzeichnis 41
 Personenbeförderungsgesetz 62
 Personenkennzeichen 53; 1984/4
 Persönlichkeitsprofil 39, 67, 68
 Persönlichkeitsrecht 59, 73
 Petitionsausschuß 1984/26; 1985/24; 1986/29
 Pflugschaft 54
 Planung 51, 52, 59, 73; 1985/11
 Polizei, Ordnungsaufgaben, s. Allgemeines Sicherheits- und Ordnungsgesetz, Ausländerbehörde, Melderegister, Paß, Personalausweis
 Polizei, Strafverfolgung, s. Fahndung, Informationssystem, Verbrechensbekämpfung, INPOL-System, KAN, KpS-Richtlinien, Strafverfolgung, Strafprozeßordnung
 Polizeiliche Beobachtung 1984/11; 1985/7

- Polizeiliche Kriminalstatistik 1986/9
 Postverkehr 43; 1986/25
 Presse 1986/19
 private Computernutzung 1984/18; 1986/24, 35
 private EDV-Unternehmen 84
 Programmdokumentation 106, 114
 Programmtests 86, 113
 Protokollisten 116
 Prozeßordnungen 1984/25; 1985/22
 psychiatrische Daten 53, 66; 1984/8; 1985/20
 psychiatrische Gutachten 41
 Quellabzugsverfahren 57
 Rasterfahndung 33, 35, 43; 1984/11
 Rechenzentrum 62, 114; 1986/27
 Rechenzentrum, Datenträgerarchiv 86
 Rechenzentrum, Funktionentrennung 114
 regelmäßige Übermittlungen 1986/6, 39
 Reichsversicherungsordnung 72
 Religionsgemeinschaften 24, 27, 32, 45, 64
 remote station 62, 84
 Rundfunkgebühren 81, 88
 Rückkanal 102
 Sanierung 74
 Satellitenfernsehen 37
 Schadensersatz 24, 28, 32
 Schlüssel, Aufbewahrung 117
 Schufa 61; 1984/7; 1985/3; 1986/4, 5, 27
 Schuldnerverzeichnis 61; 1984/28
 Schule 25, 32, 36, 41, 50, 57, 87, 118, 120; 1984/28;
 1985/5, 24; 1986/3
 Schülerunterlagen 1986/3, 23
 Schulfragebogen 36
 Schulpsychologischer Dienst 118
 Schutzgemeinschaft für allgemeine Kreditsicherung s. Schufa
 Schweiz 65
 Schwerbehinderte 1984/26
 Selbsthilfeeinrichtungen 57
 Sender Freies Berlin 24, 45
 Seriennummer, s. Personalausweis
 Sicherheitsgesetze 1986/30
 Sozialbericht 64
 Sozialdaten, s. Sozialgesetzbuch X
 Sozialgeheimnis, s. Sozialgesetzbuch X
 Sozialgesetzbuch I, Mitwirkung (§ 60) 26; 1985/22
 Sozialgesetzbuch X 25, 26, 27, 31, 44, 50, 58, 64, 72, 81, 109; 1984/2;
 1985/22; 1986/25
 Sozialgesetzbuch X, Aktenführung 1984/25, 34; 1986/25
 Sozialgesetzbuch X, Ausländer 100, 111
 Sozialgesetzbuch X, Datenschutzbeauftragte 112
 Sozialgesetzbuch X, Offenbarung für Forschung und Planung 59, 82
 Sozialgesetzbuch X, Offenbarung für Strafverfahren 82, 100, 111; 1984
 Sozialgesetzbuch X, Zweckbindung 83
 Sozialgesetzbuch X, 3. Kapitel 83, 100
 Sozialhilfe, Ausländer 58, 82
 Sozialhilfe, 58, 87
 Sozialhilfestatistik 64; 1986/28
 Sozialleistungsträger 1984/16
 Sozialwissenschaftliche Untersuchungen 33
 Sparkasse der Stadt Berlin West 1984/16
 speichernde Stelle 62, 109; 1986/24, 38
 Sperrung 1984/22; 1985/6
 Spezialgesetze s. bereichsspezifische Regelungen
 Spurendokumentationssysteme 1984/12; 1986/17
 Staatsanwaltschaft 60, 64, 115; 1984/28
 stand-alone-Rechner 63
 Statistik 31, 59, 64, 102, 104; 1984/23; 1985/11; 1986/3
 Statistisches Informationssystem 1986/9
 Städtebauförderungsgesetz 74
 Sterilisation 1986/10
 Steuerfahndung 88
 Steuerverwaltung 88
 Strafgesetzbuch, § 200 81
 Strafprozeßordnung 1984/10; 1986/4, 42
 Strafverfolgung 37, 79; 1984/10
 Strafvollzug, s. Justizvollzugsanstalten
 Studentendaten s. Hochschulen
 Synchronknoten 1986/15
 Taxifahrer 62; 1984/28; 1986/27
 Technische Prüfstellen für den Kraftfahrzeugverkehr 64
 Telebus 1984/26
 Telefon, Benutzung 42
 Telefonaufzeichnung 1986/5
 Telefondatenerfassung 63, 87, 120; 1986/5
 Telekommunikationsordnung 1986/14, 32
 Teletex 37, 38
 Testdaten 86, 113; 1984/18
 Textverarbeitung 84, 85; 1985/5
 Todesursachenstatistik 104
 Transparenz der Datenverarbeitung 30, 86, 104, 114
 Transportkontrolle 86
 Umwandlung von Mietwohnungen 73
 Umweltschutz 1986/26
 unbeschränkte Auskunft, s. Bundeszentralregister
 UNESCO 46
 Universitätsklinikum Steglitz 112
 Unterhaltsansprüche 58; 1984/26
 Unterricht 1986/24
 Unterschriftenliste 55
 USA 1984/6
 Übermittlung an nichtöffentliche Stellen 26, 31, 65, 121
 Übermittlung nichtöffentlicher Stellen an Behörden 31
 Überweisungsträger 58, 81, 120
 Verfahrensdokumentation 114
 Verfahrensentwicklung 113
 Verfassungsschutz 25, 35, 108, 120; 1984/3
 Verfassungsschutzgesetz 1985/3, 8, 26, 29; 1986/30
 Verkehrszählung 1985/11; 1986/9
 Vermessungsamt 1985/6
 Vernichtung von Datenträgern 63, 115
 Veröffentlichung von Verurteilungen 81
 Versand von Schriftstücken s. Postverkehr
 Vertraulichkeit 111; 1984/9; 1985/23; 1986/27
 Verurteilungen, Veröffentlichung 81
 Verwaltungsprozeßordnung 90
 Verwechslungen 61
 Verwertungsverbot 66
 Videoaufzeichnungen 1986/11
 Videotext 37; 1986/13
 Vieh- und Schlachthof Spandau 105
 Volksbegehren 55
 Volkszählung 1983 99, 100, 103, 120; 1984/3, 23
 Volkszählung 1987 1984/23; 1985/11; 1986/7
 Vordrucke 53, 87; 1986/25
 Wahlen 54, 55, 59, 68; 1985/17
 Warnkartei 40
 Wählerliste, s. Wahlen
 Werbung 28
 Wettbewerbsunternehmen, Krankenhäuser 112
 Wirtschaftskriminalität 77; 1984/6; 1986/4
 Wohnung 100
 Wohnungsbau-Kreditanstalt 1985/16
 Wohnungsbau-Rechenzentrum 85, 120; 1984/17
 Zentrale Vormundschaftskasse / Unterhaltsvorschußkasse 85
 Zugriffsberechtigung 55
 Zugriffskontrolle 86; 1985/8
 Zustimmung, s. Einwilligung
 Zweckbindung 66